* DORIN LELEA *
DORIN.LELEA@UPT.RO
LOCAL 25.07.2025 11:16
20.01.2025 20:28 - 20.01.2028 20:28
UNIVERSITATEA POLITEHNICA DIN TIMISOARA
Angajat UPT
20110420940401bd89332de2924a2697

Ensuring Cybersecurity Standards Compliance by Integration of Multiple Standards in the Context of Automotive Software Development Projects

A Thesis Submitted for obtaining
the Scientific Title of PhD in Engineering
from
Politehnica University Timișoara
in the Field of Engineering Management
by

Eng. Darius Barmayoun, PhD Candidate

PhD Supervisor:
Prof. eng. dr. ec. Marian Mocan

Committee Chair:
Prof.univ.dr.eng Anca Drăghici

Committee Members:
Prof.univ.dr.eng. Stelian Brad
Prof.univ.dr.eng George Căruțașu
Prof.univ.dr.eng Gabriela Ioana Prostean

Date of the Doctoral Thesis Defense:
11.07.2025

∴

BUPT

PhD Thesis
Ensuring Cybersecurity Standards Compliance by Integration of Multiple Standards in the Context of Automotive Software Development Projects

Darius Barmayoun[1,2]

[1] Politechnica University of Timisoara, Timisoara, Romania
[2] SynSpace Group GmbH, Freiburg, Germany

Abstract. In the contemporary digital landscape, the integration of robust cybersecurity measures within the automotive industry is essential to ensure the security and integrity of increasingly complex automotive systems. This thesis addresses the critical need for compliance with key industry standards, specifically ISO/SAE 21434 and the ASPICE for Cybersecurity framework, through a dual approach comprising a theoretical analysis and a practical implementation. The first part of the thesis offers a detailed theoretical foundation for a novel strategy aimed at aligning these two frameworks within automotive projects. It also includes an examination of the UNECE WP.29 regulations, particularly R155 (Cybersecurity and Cybersecurity Management) and R156 (Software Update Management Systems), and their interrelation with ISO/SAE 21434 and ASPICE for Cybersecurity. This section provides a comprehensive analysis of the structure, challenges, and implementation intricacies of these standards, laying the groundwork for a strategic integration of multiple cybersecurity standards in automotive projects. The second part of the thesis focuses on the practical application of the theoretical foundation, introducing a compliance matrix designed to map and integrate the requirements of ASPICE for Cybersecurity with ISO/SAE 21434. This compliance matrix serves as a tool to streamline the compliance process by clearly defining how the requirements of both standards interrelate, facilitating their concurrent implementation. To support this matrix, a web-based tool was developed, allowing for real-time tracking, gap analysis, and reporting, which significantly enhances usability and efficiency in managing compliance assessments. The practical application of the compliance matrix, supported by the web tool, reduces the resources required for audits and assessments, including time, costs, and manpower. Through this dual approach, the thesis not only provides a comprehensive theoretical understanding of the integration of ASPICE for Cybersecurity and ISO/SAE 21434 but also delivers a practical solution that bridges the gap between theory and industry practice. Ultimately, this research offers a valuable contribution to both industry practice and academic knowledge, advancing the understanding and application of integrated compliance frameworks within the automotive sector.

Keywords: Cybersecurity, ASPICE, ISO/SAE 21434, UNECE R155, UNECE R156, Automotive, Compliance, Software Development, Process Improvement.

BUPT

Foreword

In an era where cybersecurity is paramount to the safe operation of modern vehicles, ensuring that automotive systems meet stringent compliance standards is more important than ever. With the growing sophistication of automotive software and the integration of digital technologies in vehicles, the risk of cybersecurity breaches has increased exponentially. As a result, the automotive industry must adhere to robust cybersecurity frameworks and standards to ensure that the vehicles of tomorrow are not only functional but also secure.

This thesis addresses a critical gap in the automotive industry's approach to managing cybersecurity standards and their compliance. By focusing on the integration of ISO/SAE 21434, a standard specifically designed for cybersecurity in the automotive domain, with ASPICE for Cybersecurity, which ensures that cybersecurity is embedded within automotive software development processes, this research presents an innovative solution for improving compliance and efficiency. The work aims to streamline the otherwise complex process of aligning and meeting these critical cybersecurity standards in automotive projects.

The approach outlined in this thesis centers on the creation of a compliance matrix and the development of a web-based tool to support it. The matrix serves as a guide for aligning the requirements of ASPICE for Cybersecurity and ISO/SAE 21434, providing a clear, structured path for compliance. By utilizing this matrix in conjunction with the web-based tool, organizations can reduce the time, cost, and resources typically required to complete assessments and audits while improving the accuracy and efficiency of their compliance efforts.

This work not only explores the theoretical underpinnings of cybersecurity standards in the automotive industry but also presents a tangible, practical solution to a real-world challenge faced by organizations in this domain. The practical implementation of the compliance matrix, coupled with the accompanying tool, demonstrates the feasibility and benefits of integrating multiple standards into a cohesive compliance framework.

In writing this thesis, I aim to contribute to the growing body of knowledge in the field of automotive cybersecurity and offer solutions that can be readily adopted by practitioners and researchers alike. This work draws upon extensive research into existing standards and frameworks, industry best practices, and a deep understanding of the challenges faced by automotive organizations in managing cybersecurity compliance. It is my hope that this thesis will serve as a practical reference for those in the automotive industry looking to streamline compliance processes and improve cybersecurity management. Additionally, I aspire for this work to inspire further research and innovation in the area of integrated compliance solutions, contributing to the development of more secure and resilient automotive systems in the future.

BUPT

Acknowledgements

I would like to express my deepest gratitude to all those who have supported and guided me throughout the process of writing this thesis. Without their expertise, encouragement, and unwavering support, this research would not have been possible.

First and foremost, I am sincerely grateful to my scientific advisor, Prof. eng. dr. ec. Marian Mocan, for his exceptional guidance, valuable insights, and constant encouragement throughout my research. His expertise and critical feedback have been instrumental in shaping the direction and quality of this thesis.

I would also like to extend my thanks to the esteemed members of my advisory committee: Prof. dr. habil. eng. Bogdan Groza, Assoc. Prof. dr. eng. Răzvan Bogdan, and Prof. dr. habil. eng. Larisa Ivașcu, for their invaluable advice, constructive criticism, and unwavering support throughout my doctoral journey. Their contributions were essential in refining my ideas and improving the overall quality of my work.

A special thank to Martin Kemeter, for his support and collaboration, which greatly enriched the practical aspects of my research. His insights and the opportunity to work closely with professionals in the field made a significant impact on my academic development.

Finally, I would like to express my heartfelt appreciation to my family. Their constant love, patience, and understanding were my greatest sources of strength during this challenging and rewarding journey.

Thank you all for your invaluable support and for being a part of this achievement.

BUPT

Contents

Foreword 3
Acknowledgements 4

A. Theoretical Aspects 14
1 Introduction 14
2 Cybersecurity in the Automotive Industry 16
2.1 Evolution of Cybersecurity Threats in the Automotive Industry 18
Multifaceted landscape of attack. motivations. 19
Cybersecurity threats. 20
Conclusion. 25
2.2 Development of Regulatory Standards 25
Technological Advancements vs. Regulatory Developments. 26
Escalating Cyber Threats and Regulatory Response. 27
Interaction between various standards and regulations. 27
2.3 Impact of Cybersecurity Standards on the Automotive Industry 29
Enhanced Collaboration for Cybersecurity Compliance. 29
Acceptance of UNECE WP.29 and ISO/SAE 21434. 30
2.4 Regulatory Future for Cybersecurity in the Automotive Sector 31
Expanding Scope of Cybersecurity Regulations. 32
Integration Challenges and Industry Response. 33
Knowledge-Sharing and Cybersecurity Management 34
Future Directions and Research Framework. 35
3 International Regulations – UNECE WP.29 37
3.1 R155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system 39
Establishing a Cyber Security Management System. 39
3.2 Impact of UNECE R155 and R156 in the automotive industry 41
3.3 From Regulations to Standards 42
4 ISO/SAE 21434 and its Integration 45
4.1 The purpose of ISO/SAE 21434: 46

BUPT

4.2 Relation to UNECE: 47
4.3 The Role of implementing ISO 21434 in Organizations..... 49
Core Element: The Integral Role of a Cybersecurity Management System (CSMS). 50
Conducting Comprehensive Threat Analysis and Risk Assessment (TARA). 51
Cybersecurity in the Concept Phase. 53
Continuous Cybersecurity Activities: A Lifecycle Approach. 54
Ensuring Cybersecurity During Production. 56
Decommissioning with Security in Mind 57
Conclusion. 58
4.4 ISO/SAE 21434 Overview 59
Clause 4: General Considerations. 60
Clause 5: Organizational Cybersecurity Management. 60
Clause 6: Project Dependent Cybersecurity Management. 62
Clause 7: Distributed Cybersecurity Activities. 64
Clause 8: Continual Cybersecurity Activities. 65
Clause 9: Concept Phase. 66
Clause 10: Product Development. 68
Clause 11: Cybersecurity Validation. 69
Clause 12: Production. 71
Clause 14: End of Cybersecurity Support and Decommissioning. 73
Clause 15: Threat Analysis and Risk Assessment Methods. 74
4.5 Conclusion 75
5 ASPICE for Cybersecurity and its Integration 77
5.1 Connection to ISO/SAE 21434. 79
Structure and content. 80
Process Capability Assessment. 81
Process reference model. 81
Process assessment model. 82
Process capability levels and process attributes. 82
5.2 Cybersecurity Relevant Process Groups and Processes 83
Newly introduced process groups and processes. 84

BUPT

5.3 Conclusion. 90
6 Conclusion of Theoretical Aspects 91
6.1 Theoretical Aspects Summary 91
6.2 Following Practical Application Report 92

B. Practical Aspects 93
1 Introduction 93
2 Compliance Matrix Development 95
2.1 Selection of ISO 21434 Clauses for Mapping 96
Clause 7: Distributed Cybersecurity Activities. 97
Clause 9: Concept. 97
Clause 10: Product Development. 97
Clause 11: Cybersecurity Validation. 97
Clause 15: Threat Analysis and Risk Assessment Methods. 97
2.2 Rationale for Selecting These Clauses 98
3 Mapping between ISO 21434 and ASPICE for Cybersecurity 99
3.1 Mapping of Clause 7 99
Supplier Capability (7.4.1). 100
Request for Quotation (7.4.2) 102
Alignment of Responsibilities (7.4.3) 105
3.2 Mapping of Clause 9 112
Item Definition (9.3) 113
Cybersecurity Goals (9.4) 115
Cybersecurity Concept (9.5) 121
3.3 Mapping of Clause 10 127
Design (10.4.1) 129
Integration and Verification (10.4.2) 140
3.4 Mapping of Clause 11 148
Cybersecurity Validation 148
3.5 Mapping of Clause 15 151
Asset Identification (15.3) 152
Threat Scenario Identification (15.4) 154

BUPT

Impact rating (15.5) 156
Attack path analysis (15.6) 160
Attack feasibility rating (15.7) 163
Risk value determination (15.8) 164
Risk Treatment decision (15.9) 166
4 Web Application 169
4.1 Development and Features of the Web Application 170
User Registration and Account Management 170
Project Creation and Management 171
Dual Compliance Views: ISO-ASPICE and ASPICE-ISO 172
Observations and Compliance Rating 172
Data Synchronization and Consistency 173
User Interface and Experience 173
Collaborative Features 174
4.2 Conclusion 174

C. Case Studies and Financial Analysis 176
1 Case Study - A 176
1.1 Case Study Introduction 176
1.2 Identified non-conformances 177
1.3 Cost Reduction through the Use of the Compliance Matrix 180
2 Case Study – B 184
2.1 Case Study Introduction 184
2.2 Identified non-conformances 185
2.3 Cost Reduction through the Use of the Compliance Matrix 187
3 Financial Analysis 191
3.1 Introduction 191
3.2 Methodological Approach 192
Theoretical Framework of CBA. 193
Data Sources and Collection Methods. 195
3.3 Identification of Costs 196
Subscription Costs 196

BUPT

Hourly Rates of Employees and Assessors 197
Rationale for Hourly Rate Transparency 198
3.4 Assessment Efforts and Costs 198
ISO/SAE 21434 Assessment Efforts and Costs. 199
ASPICE for Cybersecurity Planned Assessment Efforts and Costs. 203
3.5 ASPICE for Cybersecurity Assessment Effort and Cost Improvement 207
Comparison of Actual Efforts vs. Planned Efforts 208
Comparison of Actual Costs vs. Planned Costs 209
Summary of Improvements 210
3.6 Identification of Benefits 212
Operational Benefits 213
Financial Benefits 213
Intangible Benefits 214
Conclusion 215
3.7 Aggregation of Costs and Benefits for the ASPICE Assessment 217
Total Cost Savings and Benefits 218
Net Present Value (NPV) 218
Benefit-Cost Ratio (BCR) 219
Return on Investment (ROI) 220
Conclusion of Financial Analysis 220
3.8 Risks of Cost Estimation 221
Impact of Location on Cost Estimation 221
Impact of Experience and Team Expertise 222
Discrepancies Between Planned and Actual Costs 222
The Role of Experience in Planning 223
3.9 Financial Analysis Conclusion 223

D. Scientific Contribution 225
1 Development of a Compliance Matrix for ASPICE for Cybersecurity and ISO/SAE 21434 226
1.1 Addressing the Need for Integration 226

BUPT

1.2 Key Features of the Compliance Matrix 227
1.3 Theoretical and Practical Implications 228
1.4 Limitations and Areas for Future Research 228
2 Development of a Web-Based Tool to Support the Compliance Matrix 229
2.1 Addressing the Need for Digital Transformation in Compliance 229
2.2 Key Features and Functionalities 230
2.3 Streamlining Compliance Tasks 230
2.4 Benefits of the Web-Based Tool 231
3 Contribution to Industry Practice and Academia 231
3.1 Contribution to Industry Practice 232
3.2 Contribution to Academia 233
4 Scientific Contribution Summary 236

E. Final Conclusions 238
1 Conclusion 238
1.1 Web Application Summary 240
1.2 Case Studies Summary 242
1.3 Financial Analysis Summary 245

References 247

BUPT

Table of Figures

Fig. 1. The primary components of UNECE WP.29 [4] 17
Fig. 2. Black-Hat vs. White-Hat attacks in 2021 [8] 22
Fig. 3. Physical vs. Remote-Access Attacks 2021 vs.2022 [8][5] 23
Fig. 4. Short vs. Long-Range Attacks 2021 vs. 2022 [8][5] 24
Fig. 5. Relation between regulations, standards, and frameworks 28
Fig. 6. Relation between UNECE regulations and ISO standards 43
Fig. 7. ISO/SAE 21434, R155, and R156 in practice [4] 44
Fig. 8. ISO/SAE 21434 and WP.29 collaborate to safeguard vehicles [5] 48
Fig. 9. High-level TARA Steps [50] 53
Fig. 10. Overview of ISO/SAE 21434 clauses [6] 60
Fig. 11. How Cybersecurity Policy is enforced, enabled, and ensured 61
Fig. 12. Distributed Cybersecurity Activities [6] 64
Fig. 13. V-Cycle development (ISO/SAE 21434, 2021) 69
Fig. 14. Overview of ASPICE and ASPICE for Cybersecurity Process Reference Model (PRM) [52] 78
Fig. 15. Relationship overview within the Process Assessment Model [65] 81
Fig. 16. Mapping of ISO 21434 Requirements RQ-07-01, RQ-07-02 101
Fig. 17. Mapping of ISO 21434 Requirement RQ-07-03 103
Fig. 18. Mapping of ISO 21434 Requirements RQ-07-04, RQ-07-05 106
Fig. 19. Mapping of ISO 21434 Requirement RQ-07-06 109
Fig. 20. Mapping of ISO 21434 Requirement RQ-07-08 111
Fig. 21. Mapping of ISO 21434 Requirements RQ-09-01, RQ-09-02 115
Fig. 22. Mapping of ISO 21434 Requirement RQ-09-03 116
Fig. 23. Mapping of ISO 21434 Requirements RQ-09-04, RQ-09-05, RQ-09-06 118
Fig. 24. Mapping of ISO 21434 Requirement RQ-09-07 120
Fig. 25. Mapping of ISO 21434 Requirement RQ-09-08 121
Fig. 26. Mapping of ISO 21434 Requirement RQ-09-09 123
Fig. 27. Mapping of ISO 21434 Requirement RQ-09-10 125
Fig. 28. Mapping of ISO 21434 Requirement RQ-09-11 127
Fig. 29. V-Cycle Product Development Activities [6] 128
Fig. 30. Mapping of ISO 21434 Requirement RQ-10-01 129
Fig. 31. Mapping of ISO 21434 Requirement RQ-10-02 131
Fig. 32. Mapping of ISO 21434 Requirement RQ-10-03 133
Fig. 33. Mapping of ISO 21434 Requirement RQ-10-04 135
Fig. 34. Mapping of ISO 21434 Requirements RQ-10-05, RC-10-06 136
Fig. 35. Mapping of ISO 21434 Requirement RQ-10-07 138
Fig. 36. Mapping of ISO 21434 Requirement RQ-10-08 139
Fig. 37. Mapping of ISO 21434 Requirements RQ-10-09, RQ-10-10 141
Fig. 38. Mapping of ISO 21434 Requirement RQ-10-11 143
Fig. 39. Mapping of ISO 21434 Requirement RQ-10-12 146
Fig. 40. Mapping of ISO 21434 Requirement RQ-10-13 147
Fig. 41. Mapping of ISO 21434 Requirement RQ-11-01 149
Fig. 42. Mapping of ISO 21434 Requirement RQ-11-02 151

BUPT

Fig. 43. Mapping of ISO 21434 Requirements RQ-15-01, RQ-15-02 153
Fig. 44. Mapping of ISO 21434 Requirement RQ-15-03 155
Fig. 45. Mapping of ISO 21434 Requirement RQ-15-04 157
Fig. 46. Mapping of ISO 21434 Requirements RQ-15-05, RQ-15-06, PM-15-07 159
Fig. 47. Mapping of ISO 21434 Requirements RQ-15-08, RQ-15-09 162
Fig. 48. Mapping of ISO 21434 Requirements RQ-15-15, RQ-15-16 165
Fig. 49. Mapping of ISO 21434 Requirement RQ-15-17 167
Fig. 50. Web Application User Registration 171
Fig. 51. Web Application Project Creation 171
Fig. 52. Web Application Project List 172
Fig. 53. Web Application ISO-ASPICE mapping 173
Fig. 54. Web Application Observations 174
Fig. 55. ISO/SAE 21434 Assessments Total Costs 202
Fig. 56. Planned ASPICE for Cybersecurity Assessments Costs 206
Fig. 57. Actual ASPICE for Cybersecurity Assessments Costs 209
Fig. 58. Planned vs. Actual effort in hours 211
Fig. 59. Planned vs. Actual costs in EURO 212
Fig. 60. Overall Planned Costs 216
Fig. 61. Overall Actual Costs 217

BUPT

Table of Tables

Table 1. Vehicle categories impacted by R155 & R156 [8] 39
Table 2. CAL determination example [6] 67
Table 3. Process attributes [65] 83
Table 4. Template of each process description [65] 84
Table 5. Efforts reduction in case an ISO/SAE Audit was already conducted (Values expressed as Number of involved Employees x Number of Days) 181
Table 6. Efforts reduction in case an ASPICE Assessment was already conducted (Values expressed as Number of involved Employees x Number of Days) 188
Table 7. Hourly Rates of all Roles involved in project assessments 197
Table 8. Hourly Rates of Assessors 198
Table 9. ISO/SAE 21434 Assessments Efforts and Costs based on Phases 200
Table 10. ISO/SAE 21434 Assessments Efforts and Costs based on Phases 203
Table 11. Planned ASPICE for Cybersecurity Assessments Efforts and Costs based on Phases 204
Table 12. Planned ASPICE for Cybersecurity Assessments Efforts and Costs based on Phases 207
Table 13. Actual ASPICE for Cybersecurity Assessments Efforts and Costs based on Phases 209
Table 14. Summary of Improvements 210
Table 15. Overall Planned Costs and Efforts 216
Table 16. Overall Actual Costs and Efforts 217

BUPT

A. Theoretical Aspects

1 Introduction

In an era defined by rapid technological advancements and increasing interconnected systems, the automotive industry stands at the peak of the digital revolution. This current transformation is not solely relying on the introduction of new technologies but represents a fundamental shift of the basic principles of automotive design, development, production, and operation. The increasing presence of connected vehicles is anticipated to amplify the impact of cyberspace's growing influence on our daily lives, thereby significantly heightening society's vulnerability to cyberattacks in a negative manner [1]. Vehicles today are not only regarded as means of transportation; they are complex, interconnected systems that integrate a large variety of complex technologies, from autonomous driving capabilities to IoT-enabled devices. This digital transformation of unprecedented technologies and innovations also brings with it a critical challenge: cybersecurity. Therefore, cybersecurity is becoming an increasingly critical concern due to the heightened likelihood and severity of attacks [2].

The importance of cybersecurity assurance in the automotive industry cannot be anymore underrated. As vehicles become more connected and autonomous, the cybersecurity landscape evolves from a minor to a major concern. Modern cars are currently undergoing a significant technological transformation. The electrical/electronic (E/E) systems within vehicles, specifically the in-vehicle networks, are evolving. Emerging technologies like automotive Ethernet are beginning to replace or supplement traditional systems like the Controller Area Network (CAN) bus[3]. Therefore, becoming a central pillar for assuring automotive safety and reliability. The integration of digital technologies has expanded the attack vectors, making vehicles and their associated systems vulnerable to a wide range of cybersecurity attacks and threats. These threats not only compromise the privacy and safety of vehicle users but also pose a significant threat for OEM and their Suppliers. In this context, ensuring robust cybersecurity measures is not just a technical necessity but a must.

The evolution of the automotive industry, marked by the rapid increase in innovation and technological breakthroughs, needs a deep reevaluation of traditional cybersecurity strategies implied by other industries. This reevaluation is driven by the unique characteristics of the automotive sector, including the complex supply chains, the long lifecycle of vehicles, and the critical nature of safety-related systems. Thus, cybersecurity encompassing a broad spectrum of considerations, from the protection of vehicle-to-everything (V2X) communications to the security of cloud-based services and the integrity of electronic control units (ECUs). V2X attacks are still in their early stages, yet they are anticipated to become much more common in the upcoming years [4].

Recognizing the importance of cybersecurity, the industry has driven the development and implementation of extensive standards and frameworks aimed at mitigating

BUPT

cyber risks. As vehicles increasingly become targets for hacking, regulators are continuously broadening the scope of cybersecurity protections and measures [5]. Among these, ISO/SAE 21434 and ASPICE for Cybersecurity stand out as essential standards providing structured approaches to assuring cybersecurity compliance of the automotive systems. The UNECE regulations and the ISO/SAE 21434 standard have gained significant traction and are transforming operations globally. With the expansion set for July 2024, all new vehicles will fall under the governance of R155 [4]. These standards not only highlight the best practices for cybersecurity management but also establish a common language and framework for industry stakeholders to address together cybersecurity challenges.

ISO/SAE 21434 represents a core foundation stone in the automotive cybersecurity spectrum, offering a holistic approach to the management of cybersecurity risks throughout the whole lifecycle of automotive systems. It consists of various aspects of cybersecurity, from risk assessment and management to incident response and recovery, providing a comprehensive framework for the industry to stay safe against cyber threats [6]. Similarly, ASPICE for Cybersecurity adapts the Automotive SPICE framework to the specific needs of the automotive industry in assuring cybersecurity compliance, offering guidelines for the development and assessment of cybersecurity-related projects [7].

However, the implementation of these standards presents its own set of challenges, particularly for Tier 1 suppliers who play a crucial role in the automotive supply chain. These suppliers are tasked with integrating cybersecurity measures into their products and services, a resource consuming task given the complex horizon of cybersecurity threats. The compliance challenges faced by these suppliers highlight the need for a novel approach to ease the compliance process, reducing the resources required for audit and assessment preparation. To tackle these cyber threats through a cohesive strategy, automotive OEMs along with Tier-1 and Tier-2 suppliers are adopting the UNECE's WP.29 R155 & R156 regulations, as well as the ISO/SAE 21434 standard [8]. The R155 and R156 regulations, enacted by the UNECE - World Forum for Harmonization of Vehicle Regulations at the start of 2021 and applicable to all vehicles produced from July 2024, necessitate a reevaluation of development processes [9].

This part, therefore, presents a detailed examination of the theoretical foundations necessary to understand the cybersecurity landscape in the automotive industry. It highlights the rapid evolution of the industry, led by technological advancements and innovations. Through a comprehensive review of UNECE R155 & R156, ISO/SAE 21434 and ASPICE for Cybersecurity, the theoretical parts explores the application of these standards, setting the stage for a deeper investigation into how they can be harmonized to simplify and accelerate compliance efforts. In doing so, it not only contributes to the academic discourse on automotive cybersecurity but also offers practical insights for industry practitioners, paving the way for a more secure and resilient automotive future.

BUPT

2 Cybersecurity in the Automotive Industry

The concept of cybersecurity within the automotive industry has undergone a profound evolution, emerging as a pivotal concern relatively late in the industry's history. A significant gap exists between cybersecurity practices and their implementation in small to medium-sized organizations which are part of the Industry 4.0 [10]. Unlike sectors such as finance, healthcare, and information technology, where cybersecurity has been a cornerstone due to early digital adoption and the high stakes of data breaches, the automotive sector historically concentrated on functional safety. This focus prioritized physical integrity and reliability, safeguarding against mechanical failures and human errors that could lead to immediate physical harm. As vehicles were primarily mechanical in nature, the notion of 'safety' was largely confined to the physical domain, with standards and regulations meticulously crafted to mitigate risks of accidents and malfunctions. Relying solely on the automotive system design approach that adheres to functional safety standards (ISO 26262) is insufficient to safeguard the vehicle's critical functions from various cyber-attacks [11]. This traditional approach remained largely unchallenged until recently when the automotive industry began to embrace a new paradigm characterized by digital integration and connectivity. In response to the technological advancements within the automotive sector, such as CASE (Connected, Automated/Autonomous, Shared/Service, and Electrification), communication functions, autonomous driving, mobility services like MaaS (Mobility as a Service), and increasing electrification, experts from various countries have collaborated to develop systematic approaches aimed at enhancing vehicle system safety [12]. As these technologies evolve, there is a growing need for concerted efforts to establish robust cybersecurity measures that can protect these increasingly interconnected and automated systems. This adaptation is crucial to safeguarding against the rising potential for cybersecurity threats as vehicle systems become more technologically integrated and exposed to digital risks. Furthermore, as the automotive industry advances towards greater connectivity and automation, the exposure of vehicles to potential cybersecurity attacks increases, making them more vulnerable to digital threats [13]. The advent of connected and autonomous vehicles has dramatically altered the landscape, embedding complex digital technologies, including the Internet of Things (IoT), advanced telematics, and autonomous driving systems, into the automotive infrastructure. These advancements, while transformative, introduced a new array of vulnerabilities and potential threats that extended beyond physical safety to encompass data security and privacy. Although autonomous vehicles offer numerous potential benefits that have led to their development, they also pose significant risks to future travel ecosystems due to their susceptibility to cyber threats [14]. Despite these emerging threats, the automotive industry's response to cybersecurity concerns remained tepid compared to the proactive approaches observed in other technologically intensive sectors. The delay in prioritizing cybersecurity can be attributed to several factors, including the industry's entrenched focus on physical safety, the gradual pace of digital adoption compared to other sectors, and a lack of early regulatory pressure concerning cybersecurity measures.

However, this landscape began to shift significantly as the implications of cybersecurity breaches became more apparent, underscored by high-profile incidents that

BUPT

exposed the vulnerabilities in automotive systems. These incidents not only highlighted the potential for remote exploitation of vehicle controls but also demonstrated the possible compromise of personal and operational data, thereby catalyzing a reevaluation of cybersecurity's role within the automotive safety paradigm. The critical turning point came with the introduction of the UNECE WP.29 regulations. Developed by the United Nations Economic Commission for Europe, these regulations represent a landmark in automotive cybersecurity, establishing robust standards for vehicle cybersecurity protections. UNECE WP.29 not only mandates measures to protect against cyber-attacks but also requires manufacturers to implement systems ensuring the continual safety and privacy of automotive software throughout the vehicle's life cycle [5]. This regulatory milestone marked a definitive acknowledgment of the integral role cybersecurity plays in modern automotive safety. It established a framework that compelled the automotive industry to align its safety and security strategies, integrating cybersecurity into the very fabric of automotive design and development processes. The introduction of UNECE WP.29 has necessitated a shift in the industry's outlook, moving from a reactive posture to a proactive, holistic security strategy that encompasses both cybersecurity and physical safety.



Fig. 1. The primary components of UNECE WP.29 [4]

This chapter delves into several key dimensions of cybersecurity within the automotive industry, tracing the evolution of cyber threats, the development of regulatory standards, their impact on the industry, and other broader implications. Each section provides a detailed analysis, aimed at understanding how these factors converge to shape the current and future landscape of automotive cybersecurity. The analysis begins by examining the evolution of cybersecurity threats specific to the automotive sector. It charts the progression from early, rudimentary hacks to more sophisticated and systemic cyber-attacks that exploit the interconnected nature of modern vehicles. The discussion includes case studies of notable cybersecurity breaches that have highlighted vulnerabilities in vehicular communications systems, telematics, and onboard software. This historical perspective provides a backdrop for understanding the complex nature of current threats and the necessity for robust cybersecurity measures.

Attention then shifts to the development of regulatory standards that have been implemented to safeguard automotive systems against these evolving threats. A significant portion of this discussion is dedicated to the role of international standards, such as UNECE WP.29 and ISO/SAE 21434, which have been pivotal in establishing cybersecurity guidelines. The evolution of these standards is contextualized within the

BUPT

broader regulatory landscape, noting how shifts in policy reflect changing priorities in automotive cybersecurity and the increasing emphasis on continuous risk assessment and mitigation.

The impact of these cybersecurity standards on the automotive industry is analyzed next. This examination assesses how compliance with these standards is reshaping everything from vehicle design and manufacturing processes to post-market services and customer interactions. This section also evaluates the operational, financial, and strategic challenges faced by automotive companies as they integrate these cybersecurity standards into their existing frameworks. The discussion includes insights into how companies are leveraging these standards to not only enhance security but also gain a competitive advantage.

Finally, the broader implications of enhanced cybersecurity measures in the automotive sector are explored. This includes the impact on consumer trust and market dynamics, the legal ramifications of data breaches, and the potential for cybersecurity to become a key differentiator in brand value and consumer loyalty. Additionally, the future outlook of automotive cybersecurity is discussed, speculating on emerging technologies such as artificial intelligence and blockchain, and their potential to further transform the cybersecurity landscape in the automotive industry.

Through these discussions, the chapter aims to provide a comprehensive overview of the multifaceted role of cybersecurity in modern automotive systems, illustrating how it has become an indispensable element of automotive safety and integrity in the digital age.

2.1 Evolution of Cybersecurity Threats in the Automotive Industry

This section sets the stage by acknowledging the transition from mechanically dominant vehicles to those heavily integrated with digital technologies. In the realm of the Industrial Internet of Things (IIoT), where a myriad of smart devices connected to machines, computers, and people are networked to communicate with one another, cybersecurity emerges as a primary challenge for companies [15]. This new reality means that modern vehicles are not just susceptible to traditional physical theft or sabotage, but also to sophisticated cyber threats that can compromise vehicle functionality, driver safety, and data privacy. The initial concerns regarding automotive cybersecurity were relatively modest, focusing primarily on preventing the unauthorized use of diagnostic ports which, historically, were used for maintenance and repair. However, as vehicles began to incorporate more digital components and internet connectivity, these concerns expanded. Early incidents typically involved the manipulation of software through these ports, but were limited in scope and scale, affecting individual vehicles rather than entire fleets. As the connectivity of vehicles increased, so did the potential for cyber threats. The introduction of features like GPS tracking, remote control functions, and Wi-Fi, while enhancing user experience and vehicle functionality, also opened new avenues for cyber-attacks. Hackers could potentially gain remote access to a vehicle's control systems, leading to scenarios where critical functions such as braking, steering, and engine control could be manipulated. This period marked the beginning of serious considerations regarding the need for robust vehicle cybersecurity measures.

BUPT

The advent of autonomous and electric vehicles has introduced a new layer of complexity to automotive cybersecurity. Autonomous vehicles, reliant on sensors and real-time data processing for navigation and decision-making, present unique challenges. Cyber-attacks could involve spoofing sensor data to misguide the vehicle or disabling safety features, posing serious risks to passenger safety. Electric vehicles, with their connected charging networks and battery management systems, offer new targets for cyber-attacks that could lead to disruption in power management or even sabotage. Likewise, Hataba et al. [16] highlighted the potential privacy concerns, security risks, and cyber threats associated with autonomous vehicles. For example, the 2015 Jeep Cherokee hack demonstrated the real-world implications of cybersecurity vulnerabilities. In this case, researchers remotely accessed the vehicle's entertainment system via the cellular network, subsequently taking control of the vehicle's physical functions [17]. This incident not only showcased the potential dangers of cyber threats but also prompted significant responses from both manufacturers and regulators. As highlighted by Muhammad Z. et. Al. [18], the growing integration of sensors in electric vehicles (EVs) is leading to cyber threats and privacy concerns because of the sensitive nature of the data they gather and store. These sensors amass a range of information, such as the identities of drivers and passengers, location details, and vehicle performance statistics, all of which could be exploited for harmful intentions [19]. Furthermore, attackers can leverage software vulnerabilities to infiltrate vehicle systems and potentially seize control of the vehicle [20].

Multifaceted landscape of attack. motivations.
The Upstream Cybersecurity report of 2022 sheds light on the multifaceted landscape of cybersecurity threats within the automotive industry, highlighting various actors and motives behind these threats.

State-Sponsored Hacking. The realm of cybersecurity in the automotive industry is increasingly threatened by state-sponsored hacking groups. These groups are notorious for their elusive operations, often targeting public systems that significantly impact the daily lives of citizens. As highlighted in the Upstream Cybersecurity report 2022[8], the difficulty in pinpointing the exact locations or confirming any official government sanction of these actions does not diminish their focus on similar targets or their disruptive impact. This type of cybersecurity threat poses a unique challenge due to the sophistication and resources available to state-backed actors, making them a formidable force against automotive cybersecurity measures.

Black-Hat Actors for Profit. Financial gain remains a primary motivator for many cybercriminals, particularly those targeting the automotive sector. According to the same Upstream report, the advent of relatively affordable hacking technology and increased idle time during periods such as the COVID-19 furloughs have spurred a significant rise in vehicle thefts. For instance, the first half of 2021 witnessed 124 vehicle thefts in Oakville, Canada—a city with only 211,000 residents [8]. Remarkably, sixty-six of these incidents exploited keyless entry systems or involved the use of programming technology, with 42 thefts occurring within just four weeks. These thefts are not only

BUPT

becoming more frequent but also more audacious, often occurring in broad daylight. Criminals can now identify, compromise, and abscond with luxury vehicles in under a minute, demonstrating the escalating threat to automotive security [8].

Hacking for Personal Gain. The intrinsic curiosity and desire to tinker with vehicle systems have historically led to various innovations and even cultural phenomena, such as the creation of NASCAR from the legacy of bootleggers outrunning law enforcement. However, during the COVID-19 lockdowns, this tendency took a darker turn as individuals had more opportunities to manipulate their vehicle systems at home. This meddling often involved altering both software and hardware components of vehicles, posing serious risks not only to the individual's vehicle but also potentially compromising the safety, privacy, and reliability of entire vehicle networks. For example, software obtained from forums on the internet might contain vulnerabilities that hackers could exploit to steal data, manipulate vehicle functionality, or launch broader cyberattacks [8].

The rising trend of vehicle tampering has also captured the attention of insurance companies, which are increasingly turning to vehicle telematics and related technologies to gain a better understanding of these attacks and trends. This not only helps in assessing the risks and impacts of such intrusions but also aids in developing more robust defense mechanisms against potential future threats.

These evolving challenges underscore the necessity for continuous enhancement of cybersecurity measures in the automotive industry. The sophistication and variety of these threats demand a multi-faceted approach that includes technological innovation, regulatory oversight, and international cooperation to safeguard against the ever-growing landscape of automotive cyber threats.

The 2024 report indicates a significant shift in the scale and potential impact of cybersecurity threats. Unlike previous years where attacks might have been more localized or targeted individual OEMs (Original Equipment Manufacturers), recent data shows that nearly half of the activities by the most active threat actors are targeting multiple OEMs or automotive suppliers simultaneously. This broad targeting is complemented by a startling 37% of activities having the potential to impact mobility assets globally, affecting stakeholders across the automotive industry [4]. This represents a stark escalation from the trends observed in 2022, suggesting not only an increase in the capability of these threat actors but also a shift towards intentions that could cause widespread disruption.

Cybersecurity threats.

Continuing the exploration of cybersecurity threats in the automotive industry, the 2022 Upstream Cybersecurity report highlights a notable increase in sophisticated attacks throughout 2021, posing significant challenges to both the automotive ecosystem and local authorities tasked with bolstering defenses against these threats.

Escalation of Cybersecurity Threats in 2021. The year 2021 was marked by an uptick in advanced cyber attacks, challenging automotive manufacturers, cybersecurity

BUPT

professionals, and regulatory bodies. As standards and regulations from bodies such as UNECE, ISO, and SAE continue to evolve, there remains an ongoing debate about whether these measures will deter malicious activities or inadvertently push black-hat actors towards developing more intricate methods of exploitation [8]. The majority of these attacks were attributed to black-hat actors, who not only seek to exploit vulnerabilities for financial gain but also increasingly outpace efforts by white-hat hackers who aim to fortify systems through ethical hacking practices. According to the report, 56.9% of cyber attacks in 2021 were carried out by black-hat actors, a significant increase from 49.3% in 2020. This statistic underscores the persistent threat posed by these malicious actors and highlights the continuous cat-and-mouse game between cybercriminals and cybersecurity defenders.

The 2023 Upstream Cybersecurity Report adds further context to the evolving landscape of cyber threats in the automotive industry, particularly focusing on the roles and activities of different types of hackers. The report from 2023 highlights that most attacks in 2022 were perpetrated by black hat actors, who accounted for 63% of incidents [5]. This aligns with the trend observed in the 2022 and 2024 reports, where black hat activities continue to dominate due to their malicious intentions and sophisticated organizational structures. These hackers are part of extensive networks, capable of launching coordinated attacks across multiple companies globally, contrasting sharply with the more research-focused white hat hackers.

The 2024 report also sheds light on the activities within the deep and dark web, areas often obscured from typical cybersecurity analyses. In 2023, it was found that nearly 65% of cyber activities on these hidden segments of the internet had the potential to impact thousands to millions of mobility assets, underscoring a significant rise in the scale of potential damages compared to previous years [4]. This vast scope of impact reflects a troubling advancement in the technical capabilities and strategic ambitions of cybercriminals.

Delving deeper into the specific areas of interest for black hat hackers and fraud operators, the 2024 report reveals that 67% of malicious activities are classified as having a "High" or "Massive" impact—this is a notable increase from 45% across all actors as noted in the 2022 report. Furthermore, 58% of these malicious activities involve multiple OEMs or have a global reach, highlighting a concerted effort to maximize disruption across the automotive sector.

When examining the specific focuses of these threat actors, it is found that:

- 13% of activities are aimed at developing or distributing vehicle manipulation tools.
- 12% are focused on gaining access to sensitive data and Personally Identifiable Information (PII).
- Nearly 50% are centered around exploiting vulnerabilities within automotive systems.

BUPT

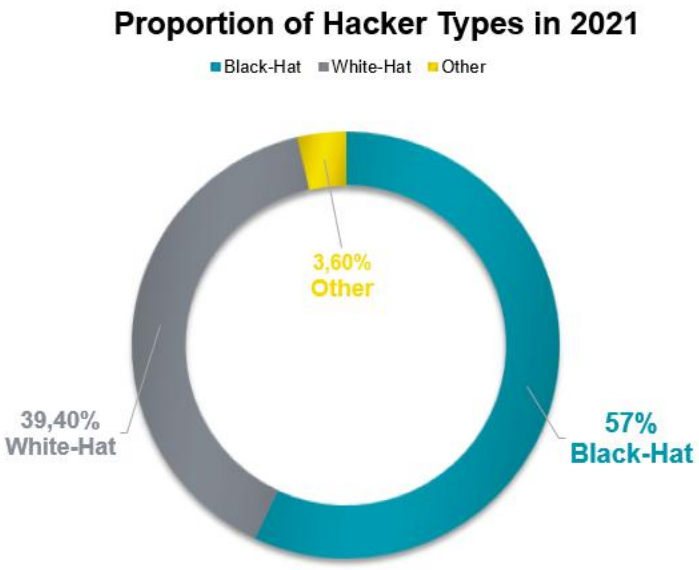


Fig. 2. Black-Hat vs. White-Hat attacks in 2021 [8]

Categories of Cybersecurity Incidents. The report [8] classifies cybersecurity incidents into two primary categories:

- Physical Attacks: These require the attacker to have physical access to the vehicle, such as through direct interaction with the car's hardware or systems.
- Remote Attacks: These can be executed from a distance, allowing hackers to breach vehicle systems without needing physical contact.

A striking example provided in the report describes a January 2021 incident where a researcher exploited a vulnerability in an Asian OEM's infotainment system. By simply plugging a USB device into the system, the researcher gained root shell access, demonstrating how seemingly innocuous interfaces can serve as gateways for significant security breaches [8]. Another notable incident occurred in the UK in July 2021, where thieves exploited a remote keyless entry system to steal a European-made vehicle right outside the owner's home. This short-range attack involved a relay attack device that intercepted and mimicked the signal from the key fob to unlock and start the vehicle[8].

The 2022 report highlights a concerning trend: between 2010 and 2021, 84.5% of reported attacks were remote, indicating a shift towards less need for physical access as vehicles become more interconnected [8]. This trend is facilitated by the increased reliability of long-range accessibility through cellular networks and other wireless communications, which are becoming more prevalent in modern vehicles. As vehicles continue to incorporate more connected components, the vector for remote attacks expands, underscoring the need for robust cybersecurity measures that can address both current

BUPT

and emerging threats. The automotive industry, along with regulatory bodies, must continue to innovate and implement comprehensive security strategies to protect against both physical and remote cyber threats, ensuring the safety and integrity of automotive systems in an increasingly connected world.

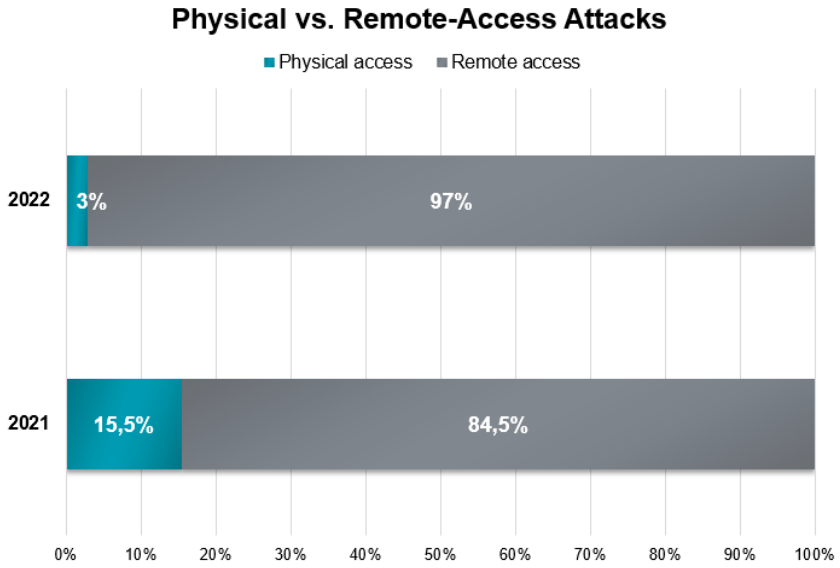


Fig. 3. Physical vs. Remote-Access Attacks 2021 vs.2022 [8][5]

The 2023 report from Upstream Cybersecurity provides a comprehensive update on the nature of automotive cyber-attacks, placing a strong emphasis on the dominance of remote attacks over physical ones in the most recent years. This development contrasts somewhat with the observations from the 2022 report, which still recognized a significant number of physical attacks alongside remote threats. In the 2022 report, attacks were broadly categorized into those requiring physical access to the vehicle and those executed remotely, noting the growing trend towards remote attacks as vehicles became increasingly connected. This trend was evident in the examples provided, which included both short-range actions exploiting keyless entry systems and long-range activities that utilized network vulnerabilities.

The 2023 report, however, indicates a pronounced shift, revealing that nearly all automotive cyber-attacks in 2022 were remote, making up 97% of all incidents [5]. This shift underscores a significant evolution in automotive cyber threats. The report distinguishes between short-range and long-range remote attacks. Short-range attacks often take advantage of local connectivity technologies such as Bluetooth, exemplified by an incident involving the exploitation of the phone-as-a-key technology. On the other

BUPT

hand, long-range attacks, which have grown in prevalence, exploit broader network infrastructures, including APIs and internet connectivity. This leads to more extensive impacts, such as the ransomware attack on a Japanese automotive supplier or the cyber attack that disrupted Denmark's largest train company by targeting IT providers that manage essential assets for transportation infrastructure [5].

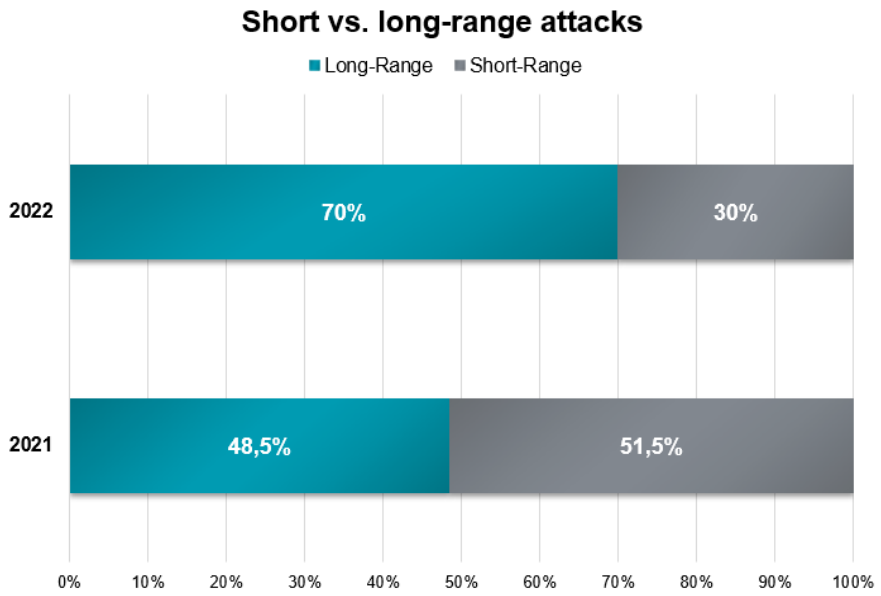


Fig. 4. Short vs. Long-Range Attacks 2021 vs. 2022 [8][5]

This change highlights that over two-thirds of remote attacks in 2022 were long-range, pointing to a growing sophistication of cyber threats and the ability of attackers to impact larger systems, potentially causing widespread disruption. The increased proportion of remote attacks necessitates enhanced security measures focused on network security, secure API design, and robust encryption practices for wireless communications. It also suggests that the automotive industry's approach to cybersecurity needs to be increasingly preemptive and comprehensive, securing not only endpoints but ensuring that third-party services and supply chain interactions are integral to the overall cybersecurity strategy. Overall, the shift towards nearly all attacks being remote also reflects the broadening attack surface due to the connectivity features that both enhance vehicle functionality and user experience. The evolution in attack patterns documented across the reports highlights the dynamic and escalating nature of cyber threats in the automotive sector, necessitating advanced technological defenses and a strategic, holistic approach to cybersecurity.

BUPT

Conclusion.
In conclusion, the evolution of cybersecurity threats in the automotive industry, as detailed throughout this subchapter, reflects a rapidly changing landscape where the stakes are increasingly high. Over the past few years, there has been a pronounced shift from a mix of physical and remote threats to a predominance of sophisticated remote attacks, with an alarming trend toward attacks that not only exploit short-range technologies like Bluetooth but also leverage long-range network vulnerabilities. The analysis from successive reports—2022, 2023, and 2024—illustrates how cyber threats have grown not just in frequency but in sophistication and potential impact. Initially, the industry contended with hackers who targeted individual systems or components. Today, the threat spectrum includes highly organized black-hat operations capable of launching coordinated attacks across multiple automotive companies and suppliers worldwide. These actors exploit the interconnectedness of modern vehicles, using the deep and dark web to coordinate and magnify their attacks, impacting everything from individual consumer safety to broader operational technology infrastructure.

The reports highlight an urgent need for the automotive industry to adapt its cybersecurity measures to keep pace with these evolving threats. This adaptation involves not only enhancing traditional cybersecurity defenses but also integrating comprehensive strategies that include advanced network security, secure API integrations, and robust encryption practices. Additionally, as the industry moves forward, fostering collaborative efforts among OEMs, suppliers, cybersecurity experts, and regulatory bodies will ensure that security measures are comprehensive and up to date.

As the industry looks to the future, the continuous innovation in automotive technologies—such as autonomous driving and increased vehicle connectivity—will likely introduce new cybersecurity challenges. Addressing these challenges will require ongoing vigilance, innovative thinking, and proactive approaches to cybersecurity. The evolution of cybersecurity threats in the automotive industry underscores a critical juncture at which the industry must not only anticipate future threats but also implement forward-thinking strategies to mitigate them effectively. This proactive stance will be essential in safeguarding the next generation of automotive technologies, ensuring that security evolves in tandem with technological advancements and remains a cornerstone of the automotive industry's commitment to safety and reliability.

To further understand how the industry is responding to these challenges, the next subchapter will explore the regulatory frameworks that are being established to guide and enforce the necessary cybersecurity measures across the global automotive sector.

2.2 Development of Regulatory Standards

In response to the escalating complexity and frequency of cybersecurity threats highlighted in the previous sections, the automotive industry has seen a concerted push towards establishing robust regulatory frameworks and standards. This chapter, entitled "Development of Regulatory Standards," will delve into the evolution and implementation of key regulatory measures that aim to safeguard automotive systems against cyber threats. The introduction of regulatory standards such as UNECE WP 29 R155 and R156, ISO/SAE 21434, and ASPICE for Cybersecurity marks a pivotal shift in the

BUPT

automotive sector's approach to cybersecurity. These frameworks are not merely guidelines but are enforceable mandates that define how cybersecurity measures are to be integrated throughout the lifecycle of automotive products. From design and development to production and post-production, these standards provide a comprehensive blueprint for securing automotive systems.

UNECE WP 29 R155 and R156, for instance, are instrumental in setting a global benchmark for cybersecurity practices in vehicles. They mandate that manufacturers not only address cybersecurity pre-market but also ensure ongoing protection throughout the vehicle's operational life [21]. Similarly, ISO/SAE 21434 focuses on establishing cybersecurity guidelines at all stages of engineering, emphasizing risk assessment processes and the management of cybersecurity information. Furthermore, ASPICE for Cybersecurity extends beyond conventional approaches by integrating cybersecurity into automotive software development processes. It aligns cybersecurity practices with overall system and software development, ensuring that cybersecurity considerations are embedded in the automotive development lifecycle from the outset.

While these standards and frameworks will be discussed in detail in the subsequent chapters, it is important to recognize their significance in the current automotive landscape. They represent a collaborative effort among regulatory bodies, industry leaders, and cybersecurity experts to standardize responses to cyber threats and enforce a rigorous cybersecurity regime that keeps pace with technological advancements and emerging cyber threats. This chapter aims to outline the foundational aspects of these regulatory standards, setting the stage for a deeper exploration of each framework in later discussions. By understanding these regulatory developments, stakeholders across the automotive industry can better navigate the complexities of implementing effective cybersecurity measures, ensuring not only compliance but also proactive protection against potential cyber threats.

The evolution of cybersecurity regulations within the automotive industry, as detailed in the Upstream Security Global Automotive Cybersecurity Reports from 2021 and 2022, reveals a dynamic landscape where technological advancements often outpace regulatory frameworks. This phenomenon, not unique to the automotive sector, has significant implications for cybersecurity in connected vehicles.

Technological Advancements vs. Regulatory Developments.
In the 2021 report, it is noted that technology advances too quickly for regulatory bodies to keep pace, a challenge seen previously with the introduction of the General Data Protection Regulation (GDPR) and other privacy laws, which were established well after the widespread adoption of technologies that exploit user data [21]. Similarly, the automotive industry has seen a lag in the development of cybersecurity regulations relative to the speed at which connected vehicle technologies have been deployed. This gap highlights the critical need for updated regulatory measures to address emerging cyber threats.

Recognizing the urgency, the industry saw significant developments in 2020 with the adoption of the UNECE WP.29 cybersecurity regulations and the drafting of the ISO/SAE 21434 standard. These frameworks mandate that OEMs (Original Equipment Manufacturers) not only ensure cybersecurity throughout the vehicle lifecycle—

BUPT

including development, production, and post-production—but also maintain the capability to deploy over-the-air (OTA) software security updates to vehicles already in use. As stated in a UNECE press release dated June 25, 2020, these regulations cover comprehensive aspects: managing vehicle cyber risks, securing vehicles by design, detecting and responding to security incidents, and safely updating vehicle software.

Escalating Cyber Threats and Regulatory Response.
The 2022 report expands on these themes by discussing the sharp increase in cyberattacks targeting the automotive industry, attributed to the growing number of connected vehicles and the proliferation of hacking tools and knowledge. This escalation of threats coincides with the automotive industry's push towards enhancing driving experiences and vehicle functionalities through connectivity, inadvertently expanding the attack surface accessible to cybercriminals [8]. This report emphasizes that the implementation of UNECE's WP.29 R155 and R156 regulations, along with the ISO/SAE 21434 standard, is crucial not just for mitigating these threats but also for establishing a unified cybersecurity approach across the automotive industry. These standards are designed to allow manufacturers flexibility in delivering innovative cybersecurity measures while ensuring that safety and security remain paramount.

The two reports underscore a clear trajectory from recognizing the lag in regulatory measures to implementing comprehensive standards aimed at mitigating an increasingly sophisticated and prevalent threat landscape. The 2021 report sets the stage by highlighting the initial regulatory efforts and the need for such measures, while the 2022 report observes these regulations in action, responding to an uptick in cyber threats driven by increased vehicle connectivity. Both reports collectively emphasize the necessity of a paradigm shift in the automotive industry's approach to cybersecurity. This shift involves moving from reactive security measures to proactive and integrated strategies that encompass the entire ecosystem of vehicle production and operation, thus ensuring the safety and security of connected vehicles against current and future cyber threats. This ongoing evolution in cybersecurity regulations is critical not only for protecting against malicious attacks but also for maintaining consumer trust and the automotive industry's credibility in the face of evolving digital challenges.

Interaction between various standards and regulations.
The UN Economic Commission for Europe (UNECE) introduced regulations WP.29 R155 and R156 in June 2020. R155 mandates the establishment of a Cybersecurity Management System (CSMS) covering the entire lifecycle of vehicles, from development to production and post-production [22]. It places accountability on Original Equipment Manufacturers (OEMs) to ensure that suppliers adhere to specified security measures. On the other hand, R156 focuses on post-production software aspects, including software approval and over-the-air (OTA) procedures [23]. Any modifications affecting technical performance require reapplication for approval under R155.

ISO/SAE 21434 provides a comprehensive methodology to support UNECE regulations R155 and R156. Unlike the UNECE regulations, ISO/SAE 21434 offers a detailed approach for calculating risk scores and prioritizing vulnerability urgency. It

BUPT

establishes cybersecurity as an integral component of engineering throughout the vehicle lifecycle, from conceptualization to decommissioning. ISO/SAE 21434 stands as a landmark achievement in the automotive industry's concerted effort to fortify cybersecurity practices. Developed collaboratively by SAE International and the International Organization for Standardization (ISO), this standard represents a comprehensive framework designed to meticulously manage cybersecurity risks across the entire lifecycle of automotive systems. Its significance lies in its ability to provide a structured and systematic approach to assessing and mitigating cybersecurity vulnerabilities, thereby empowering Original Equipment Manufacturers (OEMs) and suppliers alike to implement robust cybersecurity measures. By offering a detailed methodology for calculating risk scores and prioritizing vulnerability urgency, ISO/SAE 21434 equips stakeholders with the tools needed to effectively safeguard vehicles against cyber threats. From the initial conceptualization phase through to decommissioning, this standard serves as a guiding beacon, ensuring that cybersecurity remains a fundamental consideration at every stage of vehicle development and operation[4]. In an era where connectivity and digitalization are transforming the automotive landscape, ISO/SAE 21434 emerges as a cornerstone, reaffirming the industry's commitment to prioritizing safety and security in an ever-evolving technological landscape.

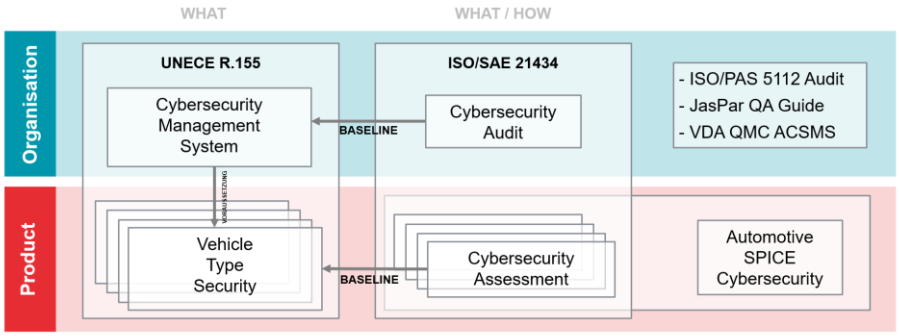


Fig. 5. Relation between regulations, standards, and frameworks

The Automotive SPICE (ASPICE) framework complements UNECE regulations and ISO/SAE standards by integrating cybersecurity into the software development process. ASPICE defines processes and capabilities required for developing automotive software, ensuring that cybersecurity considerations are systematically incorporated from the early stages of development. By aligning with ASPICE, automotive manufacturers can streamline cybersecurity practices and achieve compliance with regulatory requirements. Recognizing the critical importance of cybersecurity in modern vehicles, ASPICE has evolved to incorporate cybersecurity considerations into its framework. This integration ensures that cybersecurity is systematically addressed throughout the software development lifecycle, from requirements engineering to testing and validation. By aligning cybersecurity practices with ASPICE, automotive manufacturers can

BUPT

establish robust processes for identifying, assessing, and mitigating cybersecurity risks at every stage of software development.

In subsequent chapters, a deeper exploration of the regulations, standards, and frameworks discussed, including UNECE R155/R156, ISO/SAE 21434, and ASPICE for cybersecurity, will be undertaken. These chapters will delve into the intricacies of each regulation, standard, and framework, elucidating their individual requirements, methodologies, and implications for the automotive industry. Furthermore, the interplay and relationships between these regulatory measures will be thoroughly examined, highlighting how they complement and interact with one another to establish comprehensive cybersecurity practices in the automotive sector. Through detailed analysis and discussion, readers will gain a comprehensive understanding of the regulatory landscape and its impact on cybersecurity in connected vehicles.

2.3 Impact of Cybersecurity Standards on the Automotive Industry

As cyber threats become increasingly sophisticated, the automotive industry faces heightened risks that can compromise both vehicle safety and data integrity. In response, the industry has embraced significant cybersecurity standards, such as UNECE WP.29 R155 and ISO/SAE 21434 [5]. These standards are critical in shaping the security frameworks for automotive systems and enhancing the overall cybersecurity posture of the industry. The adoption of UNECE WP.29 R155 and ISO/SAE 21434 marks a significant shift in the automotive industry's approach to cybersecurity. WP.29 R155 introduces mandatory regulations for a Cyber Security Management System (CSMS) and necessitates type approval for vehicle security systems. ISO/SAE 21434 extends the focus to include detailed guidance on the cybersecurity aspects of engineering road vehicles throughout their lifecycle. The implementation of cybersecurity standards has reshaped the design and development phases of automotive production. Engineers and designers now incorporate cybersecurity considerations from the earliest stages of vehicle design. Moreover, Cybersecurity standards impose new requirements on the production process and the broader automotive supply chain. Manufacturers and suppliers are adapting to ensure that cybersecurity measures are embedded throughout the manufacturing process. At the same time maintaining cybersecurity throughout the operational life of vehicles is crucial after they leave the production line. Manufacturers are required to manage software updates and patches effectively through ongoing risk assessments.

Enhanced Collaboration for Cybersecurity Compliance.
Under the UNECE WP.29 R155 regulation, Original Equipment Manufacturers (OEMs) are mandated to conduct thorough threat analysis and risk assessments (TARA) across all stages of the vehicle lifecycle. This requirement extends beyond the OEMs themselves, compelling them to forge processes that address and mitigate potential future cyber attacks in collaboration with their Tier-1 and Tier-2 suppliers [5]. Although R155 primarily targets OEMs, its stipulations necessitate that the Cyber Security Management System (CSMS) encompasses the entire value chain, significantly

BUPT

broadening the regulation's scope to include suppliers. This regulation is applicable to OEMs operating within the 54 countries that are signatories to the 1958 UNECE Transportation Agreements and Conventions. The collaboration between OEMs and suppliers under R155 facilitates a more robust capability to identify and respond to security risks[5]. These risks are increasingly prevalent with new and emerging vehicle architectures, mobility services, and the connected vehicle ecosystem. R155 particularly focuses on several critical areas, including:

- Security of back-end servers that interact with vehicles in the field
- Protection of vehicles' communication channels
- Safeguarding of vehicles' software update procedures
- Mitigation of risks due to unintended human actions that could facilitate a cyber attack
- Security concerning vehicles' external connectivity and connections
- Integrity and protection of vehicle data and software code.

R155 is distinctive in its practical approach to automotive cybersecurity, providing concrete examples of threats and specified mitigation strategies. It incorporates a holistic approach that covers process and governance as well as IT, product, operational technology (OT), and Internet of Things (IoT) perspectives. This comprehensive coverage ensures that all potential vulnerabilities are addressed, from governance structures to the technical details of vehicle systems. The year 2022 marked a significant advance in how decision-making among OEMs at the global level supports cybersecurity compliance [5]. The adoption of UNECE regulations and the ISO/SAE 21434 standard has reached a critical mass, altering operations worldwide. OEMs now routinely collaborate with suppliers and cybersecurity firms to support industry-wide compliance and certification efforts. Together, they establish robust cybersecurity governance structures and develop rigorous testing processes that reinforce the security of the entire automotive ecosystem [5].

The cooperation between OEMs and suppliers in adhering to R155 and other relevant cybersecurity standards is pivotal in enhancing the overall cybersecurity posture of the automotive industry. This collaborative approach not only ensures compliance with international regulations but also fosters a proactive stance against cyber threats, safeguarding the future of automotive innovation and consumer safety. As these relationships deepen and standards evolve, the automotive sector is better positioned to tackle the complex challenges posed by an interconnected digital landscape.

Acceptance of UNECE WP.29 and ISO/SAE 21434.

In 2023, the automotive industry significantly enhanced its approach to cybersecurity through the further implementation of the R155 standard for Cyber Security Management System (CSMS) and Type Approval, alongside WP.29 R156 for Software Update Management System (SUMS). These efforts are part of a larger global initiative aimed at creating a unified defense against cyber threats, aligned with the ISO/SAE 21434 standard. The increasing importance of R155 is highlighted by the fact that its requirements will become mandatory for all new vehicle models beginning production in July

BUPT

2024. This upcoming requirement has prompted some OEMs to discontinue models that would face compliance challenges with the new regulatory milestones [4].

The ISO/SAE 21434 standard, in particular, differentiates itself by providing OEMs and their suppliers with a comprehensive process for calculating asset risk, offering methods for scoring and prioritizing the urgency of vulnerabilities. This standard establishes a structured cybersecurity framework, integrating cybersecurity as a fundamental aspect of engineering throughout the entire lifecycle of a vehicle, from the conceptual phase to decommissioning. In line with the ISO/SAE 21434 standard and the R155 CSMS requirements, OEMs are encouraged to establish and maintain a virtual Security Operations Center (vSOC) to enforce continuous monitoring for over a decade after vehicles roll off the assembly line [4]. Amid these regulatory advancements, several organizations, including the US National Highway Traffic Safety Administration (NHTSA), the European Union Agency for Cybersecurity (ENISA), and the Auto-ISAC trade association, have updated their cybersecurity guidelines and best practices. These updates are informed by recent research and the ongoing evolution of industry standards, underscoring a proactive approach to adapting and strengthening cybersecurity measures [4].

Both the R155 and ISO/SAE 21434 standards are renowned for their approach to cybersecurity, focusing on the necessity of high-level cybersecurity analysis rather than prescribing specific solutions or detailed processes. They emphasize ongoing risk assessment and response planning, highlighting the need for continuous attention to cybersecurity threats and vulnerabilities throughout the development, production, and post-production phases. This strategic focus is designed to equip the automotive industry with the tools and processes necessary to address and mitigate the dynamic and complex landscape of cyber threats effectively.

2.4 Regulatory Future for Cybersecurity in the Automotive Sector

As the automotive industry continues to evolve with the integration of advanced connectivity and autonomous technologies, the focus on cybersecurity has intensified. The future of automotive cybersecurity is poised to be shaped by an expanding regulatory framework that aims to address the complex challenges posed by the next generation of vehicles. This ongoing transformation is driven by the need to protect increasingly sophisticated vehicular networks and systems from potential cyber threats that could compromise vehicle safety and data privacy. Looking ahead, regulatory bodies worldwide are actively updating and extending cybersecurity regulations to cover a broader spectrum of automotive applications. For instance, the significant expansion of the R155 standard to include all new vehicles by July 2024 marks a proactive approach to standardizing cybersecurity measures across the industry [4]. This extension signifies a critical milestone in regulatory efforts, setting a precedent for comprehensive cybersecurity mandates that could soon encompass motorcycles and agricultural equipment as well. Furthermore, new legislative developments, such as the European Cyber Resilience Act (CRA), are indicative of a shifting focus towards ensuring that all digital components within vehicles are secure from cyber threats. Updated in December 2023, the CRA represents a pivotal move towards horizontal legislation that not only

BUPT

safeguards vehicles but also extends to protect a wide array of consumer-connected devices [4].

These regulatory changes underscore a future where cybersecurity is not just an afterthought but a fundamental aspect of the automotive design and manufacturing process. By anticipating the needs of tomorrow's vehicles, policymakers are laying the groundwork for a cybersecurity framework that not only meets current demands but is also adaptable to the future technological landscape. This forward-looking approach is essential for maintaining consumer confidence and ensuring the safety and reliability of the next generation of automotive technology.

Expanding Scope of Cybersecurity Regulations.
As the automotive industry continues to advance technologically, the scope of regulatory frameworks overseeing cybersecurity is undergoing substantial expansion to address the evolving landscape. This broadening of regulations is a strategic move to keep pace with the rapid developments in vehicle technology, particularly with the advent of connected and autonomous vehicles, which introduce new layers of complexity and potential vulnerabilities.

The extension of the R155 standard is a primary example of how regulatory bodies are adapting to these changes. By July 2024, this standard will enforce cybersecurity requirements across all new vehicle models, reflecting a significant shift towards a more rigorous and inclusive regulatory environment [4]. This expansion is not limited to passenger vehicles but extends to include motorcycles and agricultural equipment, demonstrating a comprehensive approach to securing all facets of vehicular technology against cyber threats. In addition to R155, the implementation of the European Cyber Resilience Act (CRA) marks another critical development in the regulatory landscape. Updated in December 2023, the CRA introduces a broad spectrum of cybersecurity requirements that apply to all products with digital components. This horizontal legislation is particularly consumer-focused, aiming to safeguard users across a diverse range of connected devices. By encompassing everything from smartwatches to sophisticated automotive systems, the CRA is setting a new standard in consumer protection, ensuring that cybersecurity measures are embedded in the product design and development stages [4].

These regulatory expansions are indicative of a global recognition of the increasing risks associated with cyber-physical systems in vehicles. As vehicles become more integrated with digital technologies and the internet, the potential for cyber-attacks grows, prompting a proactive response from regulators. The goal is to create a robust framework that not only addresses current cybersecurity challenges but is also flexible enough to adapt to future technological advancements. Moreover, the legislative changes are increasingly emphasizing collaboration among international regulatory bodies, automotive manufacturers, and technology providers to establish common standards that ensure safety and security across borders. This collaborative approach is crucial for creating a unified global response to cybersecurity threats in the automotive sector. The expanding scope of these regulations reflects a concerted effort to address the complex cybersecurity challenges of today's automotive industry, as outlined in the [4].

BUPT

Integration Challenges and Industry Response.
The integration of robust cybersecurity measures within the automotive industry presents a myriad of challenges, compounded by the evolving nature of vehicle technologies and the complex network of stakeholders involved. As the industry transitions towards more connected and autonomous vehicles (CAVs), the need for an integrated and holistic approach to cybersecurity becomes paramount.

The literature underscores a notable deficiency in a unified visualization of the role played by Intelligent Transportation Systems (ITS) stakeholders in establishing comprehensive cybersecurity regulatory frameworks (CRF). S.K. Khan et al. emphasize the necessity of a thorough analysis within the realm of cybersecurity regulation to fully leverage the benefits of CAV technology. Their study meticulously evaluates the roles of pertinent ITS stakeholders, including road operators, automakers, service providers, consumers, repairers, and the public, in fortifying the cybersecurity landscape of CAVs (Khan et al.). Recognizing potential unintended consequences of the CRF, such as privacy or legal implications, is crucial for delineating each stakeholder's rights, privileges, and responsibilities within the regulatory framework [24]. This delineation is essential to mitigate adverse impacts, foster positive outcomes, and reduce uncertainties and disconnections among stakeholders during the deployment of CAVs. Furthermore, D. Moris et al. highlight the shifting dynamics within the automotive supply chain, where new forms of industry players and integrators exert significant influence on the industry's ability to manage cybersecurity threats effectively. These shifts, driven by the integration of increasingly complex electronic control systems and software into vehicles, challenge traditional component integration strategies that are often ill-equipped to address modern cybersecurity vulnerabilities [25].

To address these challenges, Khan et al. propose the establishment of the CAV's Network Operations Center (NOC), which would play a pivotal role in regulating the flow of CAV data. This includes overseeing crucial aspects such as data accessibility, ownership, trans-border flow, privacy, and security. The study also emphasizes the importance of reinforcing compliance among ITS infrastructure providers to establish a robust framework for the smooth implementation of the CRF. Key regulatory measures should also ensure fair and equitable benefits derived from CAV data, treating it as a valuable asset for areas including operations, design, manufacturing, sales, marketing, and urban planning [24]. Moreover, the integration of trust layers into CAV products, grading cybersecurity schemes, and effective management of software lifecycle security are critical. The right to repair in instances of software malfunction and the standardization of CAV insurance regulations to promptly determine liability in the event of crashes or accidents are also highlighted as necessary regulatory measures [24]. The challenges of integrating cybersecurity measures in the automotive industry are further complicated by a lack of economic incentives for knowledge sharing among OEMs and suppliers, as well as the effectiveness of the information being shared, which promotes a lack of participation [25]. This situation necessitates a more collaborative and transparent approach to knowledge sharing, particularly in the development and maintenance of cybersecurity measures within the industry.

Addressing these integration challenges requires a concerted effort from all stakeholders to develop and implement a unified regulatory framework that not only

BUPT

addresses the current cybersecurity challenges but is also adaptable to future advancements in vehicle technology. The insights provided by Khan et al. and Moris et al. are invaluable in guiding these efforts, offering a detailed pathway for future research and policy development to ensure a secure transition to the next generation of automotive technology.

Knowledge-Sharing and Cybersecurity Management

As the automotive industry continues to evolve with the proliferation of connected and autonomous vehicles, the imperative for robust cybersecurity management through effective knowledge-sharing becomes more critical. The integration of advanced technologies and the expansion of network capabilities increase the potential for cyberattacks, which could have severe implications for both consumer safety and societal stability. Nikolaos Argyropoulos et al. highlight the emerging challenges posed by next-generation mobility, which includes autonomous cars, connected vehicles, and electromobility. The introduction of technologies such as 5G, LiDAR, novel in-vehicle and roadside sensors, and smart charging systems creates new vulnerabilities and attack surfaces [26]. Addressing these cybersecurity challenges requires a proactive, multi-faceted approach that spans various ICT domains. The CARAMEL H2020 project, as discussed by Argyropoulos et al., embodies this approach by aiming to develop an anti-hacking platform that leverages advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques for risk detection and mitigation, demonstrating the critical role of collaborative knowledge-sharing in enhancing cybersecurity measures.

In the context of industry-wide collaboration, D. Moris et al. point out that the structural shifts in the automotive supply chain have necessitated a reevaluation of traditional knowledge-sharing mechanisms. The introduction of complex electronic systems and software into vehicles has rendered old strategies inadequate for addressing modern cybersecurity challenges [25]. The transition requires a revamped approach to knowledge exchange that not only facilitates the sharing of cybersecurity best practices but also integrates insights from new industry players, including those from ICT and software sectors. Moreover, the effective management of cybersecurity in the automotive industry is further complicated by a lack of economic incentives and the effectiveness of shared information, which fosters a lack of participation [25]. This situation underscores the need for a more strategic, incentivized approach to knowledge-sharing that promotes active engagement from all stakeholders, including OEMs, suppliers, and new industry entrants. Enhancing trust and transparency among these players is essential for fostering an environment where cybersecurity information and strategies are freely exchanged. The CARAMEL project, as outlined by Argyropoulos et al., provides a comprehensive example of how multi-domain cooperation and advanced technological applications can lead to significant advancements in cybersecurity. The project's emphasis on AI and ML for anomaly detection and the classification of cyber threats exemplifies the potential of integrated technological solutions to address cybersecurity risks effectively. Furthermore, the project's planned activities, including live simulations and real-life demonstrations, highlight the importance of practical, hands-on approaches to validating and refining cybersecurity measures (Argyropoulos et al., 2021).

BUPT

As the industry moves forward, it is crucial to build on these foundations by continuing to evolve knowledge-sharing practices. The integration of cutting-edge technologies and methodologies should be accompanied by an equally dynamic approach to collaboration and information exchange. Ensuring that all stakeholders have access to up-to-date, relevant, and actionable cybersecurity knowledge will be key to mitigating risks and enhancing the overall security posture of the automotive industry.

Future Directions and Research Framework.
As the automotive industry navigates the complexities of integrating cutting-edge technologies and managing evolving cybersecurity threats, the necessity for innovative research and development approaches becomes increasingly apparent. The future research framework in the realm of automotive cybersecurity needs to be expansive, incorporating advanced artificial intelligence (AI) techniques, ensuring robust knowledge sharing, and fostering collaboration among all stakeholders. R. Kaur et al. emphasize the importance of adopting more sophisticated AI techniques to fully harness the potential of various data sources and application areas in cybersecurity. Key innovations such as multiple data source analysis, explainable AI (XAI), and augmented intelligence highlight the need for a more integrated and holistic approach in AI research [27]. For instance, multiple data source analysis can address the current shortcomings in cybersecurity AI, where isolated dataset usage fails to provide a comprehensive security posture. By integrating diverse datasets, AI can achieve a deeper understanding and enhanced predictive capabilities, significantly improving vulnerability assessments and risk management. Explainable AI is another critical area of focus, as it brings transparency to AI decision-making processes, which is vital for trust and reliability in cybersecurity applications. This transparency is essential for stakeholders to understand, trust, and effectively implement AI-driven cybersecurity solutions.

Augmented intelligence, which combines human expertise with AI capabilities, represents a promising frontier. This approach facilitates superior decision-making by incorporating the intuitive and contextual strengths of human analysts with the processing power of AI. This synergy is crucial for handling complex cybersecurity tasks where human judgment is indispensable.

As highlighted by Nikolaos Argyropoulos et al., the integration of emerging technologies such as 5G, LiDAR, and smart charging systems in vehicles introduces new cybersecurity challenges. The CARAMEL H2020 project illustrates a proactive approach to these challenges, utilizing AI and ML for anomaly detection and risk mitigation in the evolving landscape of next-generation mobility [26]. Such projects underscore the importance of a structured, multi-domain approach to cybersecurity, ensuring that all technological advancements are accompanied by adequate security measures. Furthermore, the project brings attention to the need for a balanced regulatory framework that addresses privacy and legal implications, particularly in the deployment of connected and autonomous vehicles (CAVs). Establishing clear rights, privileges, and responsibilities for all ITS stakeholders is crucial in mitigating risks and fostering a secure environment for the adoption of new technologies.

Drawing from the insights provided by M. Lezzi et al., the future of cybersecurity research should also focus on creating a reference framework that incorporates the

BUPT

complex interactions and roles of ITS stakeholders as observed in Industry 4.0 scenarios [28]. This framework should address the four critical areas of cybersecurity: defining vulnerabilities, assessing cyber threats, exploring countermeasures, and developing structured solutions that can be easily integrated into the managerial practices of automotive cybersecurity. This comprehensive approach to cybersecurity, which Lezzi et al. define, offers a valuable blueprint for addressing the specific needs and challenges within the automotive sector. By synthesizing the most cited evidence across different areas of analysis, this framework can guide both future research and the development of new organizational practices that enhance cybersecurity across the entire lifecycle of automotive products. The necessity for collaborative and networked approaches in cybersecurity is evident, as described by both Kaur et al. and Argyropoulos et al. Developing flexible, adaptable, and interconnected threat intelligence platforms at national and international levels can significantly enhance the sharing of threat information. Such platforms are essential for improving situational awareness and facilitating effective, risk-informed decision-making, ultimately enhancing the security and dependability of critical infrastructure.

To address the identified gaps and advance the field, future research should focus on creating and supporting new infrastructures that enhance AI capabilities in cybersecurity. This includes the development of new real-time datasets and the establishment of platforms that enable comprehensive evaluations and validations across diverse scenarios. Moreover, interdisciplinary research that integrates insights from psychology, cognitive science, and human-computer interaction is needed to optimize the design and functionality of human-AI interfaces in cybersecurity tasks. The ongoing evolution of AI in cybersecurity, as studied by R. Kaur et al., necessitates continuous attention to the acquisition, representation, and utilization of data. Future directions should also emphasize the practical application of AI techniques, ensuring that they are adaptable to the rapidly changing landscape of cybersecurity threats and are capable of delivering real-world benefits to organizations of all sizes and sectors [27].

By embracing these future directions and building on the current research frameworks, the automotive industry can effectively navigate the challenges of cybersecurity and ensure the safe, secure adoption of emerging technologies. The future of the regulatory cybersecurity landscape in the automotive industry is characterized by an increasing complexity and a greater need for comprehensive and integrated approaches to manage cybersecurity risks. The evolution of regulations such as R155 and the CRA, along with industry-led initiatives and research, are pivotal in shaping a more resilient automotive ecosystem. As these standards and practices continue to develop, the emphasis will increasingly be on creating open, trust-based models that not only comply with evolving regulations but also foster innovation and enhance overall cyber resilience.

BUPT

3 International Regulations – UNECE WP.29

The landscape of automotive cybersecurity is rapidly evolving, paralleled by an increasing integration of connected technologies within vehicles. This surge in connectivity not only enhances vehicular capabilities and consumer experience but also escalates the potential cyber risks associated with automotive systems. In response to these emerging threats, in order to reduce the risk that vehicles or components get attacked, regulatory bodies worldwide are implementing rigorous standards to ensure vehicular safety and security [29]. A significant milestone in this regulatory evolution is the establishment of the UNECE WP.29 framework, specifically through Regulations R155 (Cybersecurity and Cybersecurity Management) and R156 (Software Updates and Software Updates Management Systems). The regulatory frameworks established by UNECE WP.29 are applicable to its 54 member countries, which include the European Union, the United Kingdom, Japan, and South Korea. Additionally, various regions and countries may mandate compliance with UN R155 and other WP.29 regulations as a prerequisite for manufacturers (OEMs) before permitting their products to enter these markets [30]. This chapter provides a comprehensive exploration of these regulations, underscoring their development, implications, and the challenges they pose for automotive manufacturers.

The United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (WP.29) is a pivotal global body responsible for standardizing automotive regulations. WP.29 facilitates international cooperation and alignment in vehicle regulations, which encompasses safety, environmental protection, energy efficiency, and anti-theft measures[31]. The forum's initiatives are critical in shaping the regulatory landscape for automotive systems, making it a central figure in the advancement of vehicle safety and sustainability standards worldwide [31].

Regulation R155 represents a groundbreaking step in automotive cybersecurity, marking a significant shift from recommendations to mandatory compliance for vehicle manufacturers. Adopted in June 2020, R155 establishes comprehensive measures for managing vehicle cybersecurity risks. The regulation mandates the establishment of a Cybersecurity Management System (CSMS), requiring manufacturers to continuously identify, evaluate, and manage cybersecurity threats throughout the lifecycle of automotive products [32]. This involves rigorous assessment processes, documentation requirements, and regular audits to ensure compliance. R155 not only aims to protect vehicles against cyber-attacks but also ensures that cybersecurity measures evolve with changing threat landscapes and technological advancements[22].

Simultaneously, Regulation R156 addresses the critical aspect of software management in vehicles. With the increasing reliance on software to control critical vehicle functions, managing software updates has become crucial for maintaining safety, security, and compliance with regulatory requirements. R156, also adopted in June 2020, mandates the implementation of a Software Update Management System (SUMS) [33]. This system ensures that software updates are managed systematically and securely, minimizing risks associated with software faults and vulnerabilities. The regulation covers the entire process from the development and testing of updates to their deployment and post-deployment monitoring.

BUPT

As also depicted in Table 1, the following vehicles categories are impacted by the UNECE WP.29 Regulations R155 and R156 [4]:

- L6: Described as a vehicle with four wheels weighing under 350kg (approximately 770lbs), with an engine capacity not exceeding 50 cubic centimeters and designed for a maximum speed of 45 km/h (around 28mph), is subject to R155 if it is equipped with level-3 functionalities or above.
- L7: Defined as a vehicle with four wheels weighing under 400kg (about 880lbs), with a continuous rated power not exceeding 15kW, also falls under R155 if it possesses level-3 functionalities or higher.
- M: This category includes vehicles with at least four wheels meant to carry passengers, and these are affected by both R155 and R156 regulations.
- N: Represents automobiles with at least four wheels designed to carry goods, and they are also subject to both R155 and R156.
- O: Covers trailers that have at least one Electronic Control Unit (ECU) and are impacted by R155 and R156 as well.
- R: Agricultural Trailers are mentioned, which are under the purview of R156.
- S: Interchangeable towed agricultural or forestry equipment, which is governed by R156.
- T: Encompasses any motorized, wheeled, or tracked agricultural equipment with two axles, intended to travel at speeds greater than 6km/h (approximately 3.5mph), and is affected by R156.

However, the Working Party on Automated/Autonomous and Connected Vehicles under the UNECE has recently resolved to expand the coverage of UN Regulation No. 155 concerning cybersecurity and cybersecurity management to encompass motorcycles, scooters, and electric bicycles capable of speeds over 25 km/h [34].

The introduction of R155 and R156 poses several challenges for automotive manufacturers. These include the integration of robust cybersecurity and software management practices into the existing development processes, aligning with the regulatory expectations without compromising on innovation and market demands. Manufacturers must navigate these challenges while ensuring transparency with regulatory bodies and maintaining consumer trust in vehicle safety and security [30]. For the effective execution of the issued regulation, collaboration, and concerted efforts from all involved parties—including car manufacturers, suppliers, and government bodies—are essential. The initial step is to classify these potential attack vectors by their anticipated threat severity, allowing stakeholders to prioritize and methodically address the mitigation of these threats [35].

BUPT

Table 1. Vehicle categories impacted by R155 & R156 [8]

Vehicle Category	Definition	Applicable Regulation
L6	Vehicle with four wheels weighing under 350kg (~770lb.) whose engine does not exceed 50 cubic cm. and whose maximum speed is designed for 45 km/h (~28mph)	R155 if equipped with level-3 functionalities and above
L7	Vehicle with four wheels weighing under 400kg (~880lb.) and whose continuous rated power does not exceed 15kW	R155 if equipped with level-3 functionalities and above
M	A vehicle with at least four wheels and meant to carry passengers	R155 & R156
N	An automobile with at least four wheels meant to carry goods	R155 & R156
O	Trailers that have at least one ECU	R155 & R156
R	Agricultural Trailer	R156
S	Interchangeable towed agricultural or forestry equipment	R156
T	Any motorized, wheeled, or tacked agricultural equipment that has two axles and is meant to travel at speeds greater than 6km/h (~3.5mph)	R156

3.1 R155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

The introduction of the United Nations Economic Commission for Europe (UNECE) Regulation R155 marks an important regulatory moment in automotive regulatory history. This regulatory framework guides in a new chapter for the industry, focusing on the critical need for robust cybersecurity measures in the face of increasingly connected and sophisticated vehicle technologies. Central to Regulation R155 is the mandate for a Cybersecurity Management System (CSMS), which serves as the starting point for manufacturers to secure vehicles against cyber threats systematically. In their pursuit of a cohesive strategy to safeguard against cyber threats, numerous automotive Original Equipment Manufacturers (OEMs) and their suppliers have started to adopt the WP.29 R155 regulation, which focuses on the Cyber Security Management System (CSMS) and Type Approval [5].

Establishing a Cyber Security Management System.
The Cyber Security Management System (CSMS), as delineated by the United Nations Regulation No. 155 (UN R155) [32], is more than just a set of requirements; it is an extensive process landscape embedded within organizations to seamlessly integrate cybersecurity into vehicle development. The CSMS establishes a full spectrum of

BUPT

processes within an organization, ensuring that cybersecurity is not an afterthought but a fundamental aspect of vehicle development [36]. This holistic incorporation demands a multi-faceted approach:

- Risk Identification: At the core of the CSMS is the assessment, categorization, and management of risks, forming the basis for a robust cybersecurity posture.
- Continuous Monitoring: A proactive surveillance system is crucial, enabling the detection of and response to cybersecurity threats in real time.
- Value Chain Collaboration: The CSMS extends beyond the confines of the OEM, necessitating a concerted effort throughout the entire supply chain, including all suppliers involved.
- Lifecycle Consideration: The regulation mandates that cybersecurity be considered throughout the entire product lifecycle of a vehicle, from the early phases of development to the post-production stage.

The Certificate of Compliance (CoC) serves as evidence of an organization's adherence to the CSMS requirements. However, the type approval procedures necessitate concrete proof of the CSMS's practical application during the development phase. This includes the submission of technical documents, proofs, and evidence demonstrating the CSMS's active role in development processes [36]. While the onus of compliance primarily lies with the OEM, there is a clear responsibility outlined for the management of the downstream supply chain. This is particularly important as OEMs begin to explicitly convey their cybersecurity requirements to suppliers. In practice, the implementation of UN Regulation No. 155 and the application of the CSMS at the supplier level often culminate in queries regarding the exact requirements to be met. As OEMs relay their specific needs down the supply chain, suppliers are compelled to evaluate and adapt their processes to align with the stringent standards set forth by the regulation. While regulatory mandates for compliance rest with the Original Equipment Manufacturers (OEMs), there is a discernible market movement wherein the stipulations for a Cyber Security Management System (CSMS) are cascaded virtually verbatim from the OEMs to their suppliers. Suppliers frequently perceive it as an obligation—a prerequisite for conducting business—to establish management systems and fulfill cybersecurity obligations that are closely aligned with the standards upheld by the OEMs [32]. This trickle-down effect of cybersecurity requirements ensures that every component and system within a vehicle is developed with security in mind.

The enactment of UN R155 and the establishment of a CSMS represent a shift in the automotive industry toward a process-led approach to cybersecurity. As previously outlined, this approach is comprehensive, extending from risk management to the verification of security measures across the product's lifecycle and throughout the supply chain [36]. For OEMs and suppliers alike, the CSMS is not just a regulatory hurdle but a fundamental component of modern vehicle development, embedding cybersecurity into the DNA of automotive design and manufacturing.

BUPT

3.2 Impact of UNECE R155 and R156 in the automotive industry

In a historical move responding to regulatory shifts, Porsche ceased production of the gasoline-powered Macan SUV in December 2023 [37]. The decision was largely driven by the financial burdens imposed by the new cybersecurity regulations, which would prevent the model from being registered after July 2024. These regulations, specifically UNECE Regulation No. 155, necessitate that manufacturers maintain a robust, fully operational Cyber Security Management System (CSMS) to ensure the cybersecurity of their vehicle fleets [9]. Coupled with the requirements of UNECE Regulation R.156 on Software Update Management Systems, the landscape of vehicle development is being reshaped, demanding swift and strategic responses from car manufacturers. Porsche's discontinuation of the Macan SUV underscores the significant repercussions that such regulations have on the automotive industry, which is currently undergoing rapid transformation.

The publication of UNECE Regulations R155 and R156 has inaugurated a transformative phase in the automotive industry, fundamentally altering the approach to cybersecurity and software management. These regulations not only set new benchmarks for vehicle safety and data integrity but also impose a comprehensive compliance framework that automotive manufacturers and suppliers must navigate[38]. The enforcement of R155 requires automotive firms to adopt stringent cybersecurity measures through a mandated Cyber Security Management System (CSMS)[22]. This shift signifies the transition to a proactive cybersecurity posture, demanding continuous monitoring and defense against evolving cyber threats. Alongside, R156 calls for a robust Software Update Management System (SUMS)[23], ensuring that the software governing vehicle functions is consistently updated and secured against vulnerabilities. These changes underscore a commitment to enhancing the safety and performance of the modern vehicle through improved digital resilience.

As seen in the previous example, compliance with R155 and R156 brings substantial financial implications. Automotive companies are compelled to invest in new technologies, workforce training, and the restructuring of internal processes to meet the regulations' stringent demands. The heightened administrative burden, due to the extensive documentation required to demonstrate compliance, can affect the agility of companies, potentially delaying the market entry of new vehicle models. Therefore, leading OEMs like Porsche to discontinue a famous car model as the costs would be too high to bring its platform to the newest standards[37].

The year of 2022 marked the beginning the implementation of the UNECE WP.29 R155 standards. Concurrently, there was a significant surge in the development and use of mobility applications, services, and the broadening of mobility assets. As the number of connected vehicles on the streets grows, the incidence and complexity of cyber-attacks are escalating, paralleled by the advancement of hacking tools and techniques[5]. Starting in 2022, the regulations set forth by the United Nations harmonization body for the European Economic Area have become a mandatory prerequisite for the approval and homologation of new vehicle types and platforms. There is a transition period in place until 2024. These regulations, under the General Safety Regulation, are being enacted into European law; they require manufacturers to establish management

BUPT

systems for cybersecurity (R.155) and software updates (R.156), which must be certified by independent auditors. Without the appropriate evidence, no manufacturer will receive type approval from national licensing authorities. Therefore, meeting cybersecurity requirements becomes a critical factor in whether a vehicle is even allowed to be sold. Flexibility is an essential component of WP.29 R155 and ISO/SAE 21434, providing clear directives while maintaining manufacturers' capacity to introduce new technologies into the market [4].

3.3 From Regulations to Standards

In examining the nuanced dynamics between ISO/SAE 21434 standards and UNECE Regulation No. 155, it is crucial to delineate the distinctions between 'standards' and 'regulations' within the context of the automotive industry.

Standards, such as those set forth by the International Standards Organization (ISO), are crafted by industry stakeholders and serve as benchmarks of state-of-the-art practices. They are not prescriptive but rather provide an abstract framework for guiding industry practices [32]. ISO/SAE 21434, titled "Road Vehicles – Cybersecurity Engineering," exemplifies this by offering a structured approach to cybersecurity within the automotive sector without dictating specific solutions. Instead, it underscores the significance of engineering vehicles with robust cybersecurity defenses in mind. In a legal sense, adherence to such a standard can be instrumental in demonstrating that a product has been developed in alignment with contemporary industry methodologies and best practices.

Regulations, on the other hand, are mandates imposed by authoritative entities and carry legal weight, often backed by government or intergovernmental bodies [32]. They set forth compulsory requirements that industries must comply with to achieve regulatory approval and access to markets. In the realm of automotive cybersecurity, UNECE Regulation No. 155 stands out as a pivotal regulatory directive. Compliance with this regulation is non-negotiable for manufacturers seeking type approval and the legal distribution of vehicles within and across the jurisdictions of over 60 countries that have adopted the regulation. The stakes are high: non-compliance could result in a prohibition of sales within these regions.

The relationship between ISO/SAE 21434 and UNECE Regulation No. 155 will be further analyzed during the following chapters. ISO/SAE 21434 distinguishes itself from WP.29 R155 / R156 by offering a detailed methodology for OEMs and Tier suppliers to assess the risk score of an asset and to determine the priority of addressing vulnerabilities. This standard lays out a comprehensive framework for cybersecurity, embedding it as a crucial component of the engineering process across the entire lifespan of a vehicle, from the initial concept to its eventual decommissioning[4]. In practice, this means automotive industry players must strategically navigate both the standard's framework and the regulation's legal mandates to ensure compliance and market access. The CSMS, as defined by ISO/SAE 21434, encapsulates the lifecycle management of cybersecurity risks and is foundational to complying with UNECE Regulation No. 155. It encompasses the organizational processes necessary for managing

BUPT

cybersecurity risks and establishes the expectation for independent assessments to confirm conformity to the standard—and by extension, to the UNECE regulation.

Similarly, the SUMS, rooted in ISO 24089 standards, lays down the principles for managing software updates, a process intricately tied to both the cybersecurity and operational efficacy of modern vehicles. The implementation of these systems, as mandated by UNECE Regulation R156, requires that neutral inspectors verify the adherence to the regulatory requirements, thus completing the compliance loop.

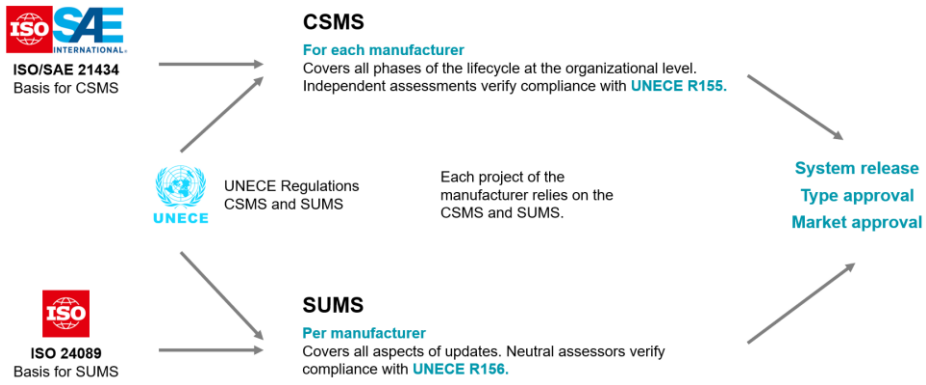


Fig. 6. Relation between UNECE regulations and ISO standards

The journey towards integrating these standards and regulations is not merely about fulfilling legal obligations but about embedding a culture of cybersecurity excellence [32]. It demands a forward-thinking approach where manufacturers and suppliers harmoniously align their operations with the dual pillars of ISO/SAE 21434 and UNECE R155 and R156, ensuring that the vehicles they produce are not only innovative but also secure and compliant in an ever-changing technological and regulatory landscape.

As we conclude this exploration into the interplay between ISO/SAE 21434 and UNECE Regulations R155 and R156, it is evident that these frameworks collectively forge a comprehensive strategy for cybersecurity in the automotive sector, as depicted in Figure 7. The 'Security by design' philosophy, rooted in the ISO/SAE 21434 standard, insists on a proactive forecast and mitigation of security flaws that may emerge during the vehicle's lifetime. This forward-thinking approach signifies a transformative shift in vehicle design philosophy, embedding cybersecurity at the foundational level. The Cyber Security Management System (CSMS) introduced by R155 amplifies this approach, extending vigilant monitoring for vulnerabilities beyond production, ensuring the protection of the vehicle through its entire lifecycle. This ongoing oversight process aligns with the dynamic nature of cybersecurity threats in an era where vehicles are continually connected to a broader digital ecosystem [8]. Furthermore, the TARA process emerges as a critical analytical framework, assigning risk scores and enabling manufacturers to prioritize responses to the most pressing vulnerabilities [8]. This risk-based prioritization facilitates strategic resource allocation and ensures that

BUPT

manufacturers can swiftly neutralize potential threats. The early detection and rapid response mechanism, which R155 advocates, enables manufacturers to quickly rectify cybersecurity issues, upholding the regulation's rigorous standards for timely and effective threat management.

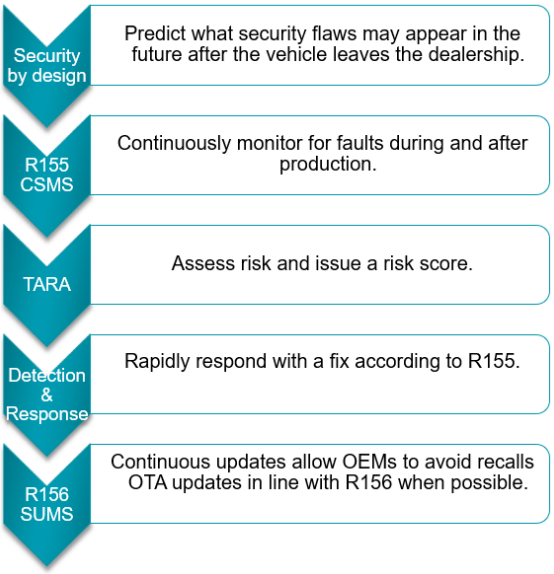


Fig. 7. ISO/SAE 21434, R155, and R156 in practice [4]

Complementing these preventative and evaluative measures, R156's emphasis on the Software Update Management System (SUMS) empowers manufacturers to deliver continuous software updates over-the-air (OTA), reducing the reliance on physical recalls. This capability is crucial for maintaining software integrity and ensuring the ongoing operational safety of the vehicle.

In conclusion, the confluence of ISO/SAE 21434 and UNECE Regulations R155 and R156 maps out a robust cybersecurity governance model that spans the entire vehicle lifecycle. This collaborative framework not only addresses current cybersecurity needs but also sets a clear trajectory for future automotive innovations. As the automotive industry advances, the adoption and implementation of these standards and regulations will remain pivotal, guiding the industry towards a future where vehicle safety is synonymous with cybersecurity, thereby ensuring the trust and safety of consumers worldwide.

BUPT

4 ISO/SAE 21434 and its Integration

The ISO/SAE 21434 standard, titled "Road vehicles — Cybersecurity engineering," is a pivotal standard in the automotive industry, marking a significant evolution in the approach towards cybersecurity within the context of automotive software development projects. Its introduction and widespread adoption highlight the increasing recognition of cybersecurity as a critical component of automotive safety and reliability. As automotive systems have advanced in functionality and convenience, they have also become more systematized and interconnected, thereby elevating the risk of cyberattacks [12]. The standard aims to establish a comprehensive set of guidelines for managing cybersecurity risks across the entire lifecycle of automotive systems, from the initial concept phase through design, production, operation, maintenance, and decommissioning. If encompasses the concept phase, which is marked by collaboration among a variety of high-level stakeholders from different disciplines, departments, and potentially various companies [39]. The imperative for such a standard arises from the evolving landscape of automotive technologies, where vehicles are no longer standalone mechanical entities, but complex, interconnected systems embedded within broader digital ecosystems. The integration of advanced functionalities, such as autonomous driving, connectivity, and the Internet of Things (IoT), has exponentially increased the attack surface, making vehicles and their associated infrastructure more susceptible to cyber threats. These developments necessitate a paradigm shift in how cybersecurity measures are integrated into automotive systems, moving beyond traditional project-based defenses towards a more holistic, organization-wide approach to cybersecurity. ISO/SAE 21434 responds to this need by providing a structured framework for identifying and managing cybersecurity risks in automotive systems. It emphasizes the importance of integrating cybersecurity considerations into the automotive design process from the concept phase, ensuring that security measures are built into the architecture of automotive systems rather than being appended as an afterthought. Moreover, from the perspective of automotive manufacturers, collaboration within the automotive sector also involves working with multiple suppliers and subsidiaries [40]. This preemptive approach is crucial for mitigating the potential impact of cyber threats on vehicle safety, privacy, and functionality. Furthermore, the standard recognizes the dynamic nature of cyber threats and the need for continuous monitoring and adaptation of cybersecurity measures throughout the lifecycle of automotive systems. It advocates for a lifecycle management approach to cybersecurity, encompassing continuous risk assessment, threat analysis, and incident response mechanisms. This approach ensures that cybersecurity measures remain effective and relevant in the face of evolving cyber threats and technological advancements. Unlike SAE J3061, ISO/SAE 21434 presents a non-sequential list of activities for cybersecurity risk management. The standard provides objectives for each activity and includes informative examples that illustrate various methods for implementing these activities [41].

The implementation of ISO/SAE 21434 also has significant implications for regulatory compliance and industry best practices. As governments and regulatory bodies around the world increasingly recognize the importance of cybersecurity in the automotive sector, compliance with ISO/SAE 21434 is becoming a critical factor for market

BUPT

access and competitive advantage. Additionally, by establishing a common language and set of practices for cybersecurity in the automotive industry, ISO/SAE 21434 facilitates collaboration and knowledge sharing among stakeholders, enhancing the overall cybersecurity posture of the industry. Therefore, the introduction of ISO/SAE 21434 marks a crucial step forward in the integration of cybersecurity standards within the automotive industry. Although ISO/SAE 21434 serves as a security engineering standard for the domain, there is a lack of frameworks and tools for cybersecurity training and testing of concepts [42]. However, by providing a comprehensive framework for managing cybersecurity risks throughout the lifecycle of automotive systems, it addresses the unique challenges posed by the increasing complexity and connectivity of modern vehicles. The adoption and effective implementation of ISO/SAE 21434 are essential for ensuring the safety, reliability, and trustworthiness of automotive systems in the digital age.

4.1 The purpose of ISO/SAE 21434:

The core objective of ISO/SAE 21434 is to integrate cybersecurity considerations into the engineering processes of electrical and electronic (E/E) systems within road vehicles [6]. This standard is pivotal in guiding automotive manufacturers and suppliers through the complexities of cybersecurity in modern vehicle design and functionality. Recognizing the dynamic nature of technology and the sophistication of potential cyber threats, ISO/SAE 21434 is designed to ensure that the engineering of E/E systems not only keeps pace with cutting-edge advancements but also incorporates robust measures to defend against evolving cyber-attack methodologies. ISO/SAE 21434, which extends the ISO 26262 Road Vehicles – Functional Safety standard, mandates that automotive OEMs and suppliers integrate cybersecurity across the entire vehicle lifecycle [4].

ISO/SAE 21434 serves as a comprehensive framework, offering an extensive vocabulary, setting clear objectives, stipulating precise requirements, and providing practical guidelines focused on the sphere of cybersecurity engineering. This foundational guidance is instrumental in fostering a uniform understanding of cybersecurity across the automotive supply chain, facilitating a cohesive approach to tackling cyber threats in the industry. By laying down these standardized principles, the document empowers organizations within the automotive sector to:

- Develop and Implement Cybersecurity Policies and Processes: It guides organizations in defining their own cybersecurity policies and procedures that are aligned with industry best practices and regulatory requirements. This includes the adoption of strategies that ensure the confidentiality, integrity, and availability of automotive systems and data.
- Manage Cybersecurity Risks Effectively: ISO/SAE 21434 emphasizes a structured approach to identifying, assessing, and mitigating cybersecurity risks associated with E/E systems. This risk management process is crucial for prioritizing security efforts and allocating resources efficiently to address vulnerabilities and threats in a timely manner.

BUPT

- Cultivate a Strong Cybersecurity Culture: The document underscores the importance of fostering a cybersecurity culture within organizations. This involves raising awareness about cyber threats, training employees on cybersecurity best practices, and encouraging proactive engagement with cybersecurity initiatives. Creating an environment where cybersecurity is a shared responsibility helps in reinforcing the organization's defense against cyber incidents.

Furthermore, ISO/SAE 21434 can be leveraged to establish a comprehensive cybersecurity management system (CSMS), encompassing all aspects of cybersecurity risk management. This includes the formulation of strategies for continuous monitoring, incident response planning, and the implementation of cybersecurity controls throughout the lifecycle of E/E systems. The adoption of a CSMS as guided by ISO/SAE 21434 ensures a systematic and consistent approach to cybersecurity, enabling organizations to respond adeptly to both current and future cybersecurity challenges.

ISO PAS 5112, released in 2022, targets the evaluation of cybersecurity processes at the organizational level. Its framework and structure are derived from ISO 19011:2018, which provides guidelines for auditing management systems, and have been tailored to fit the context of automotive cybersecurity and ISO/SAE 21434. ISO PAS 5112 offers guidance on conducting audits for a cybersecurity management system that is developed in accordance with ISO/SAE 21434 [43].

4.2 Relation to UNECE:

The evolution of automotive technology towards increasingly interconnected and software-intensive systems has elevated the stakes in automotive cybersecurity. The collaborative emergence of ISO/SAE 21434: "Road Vehicles — Cybersecurity Engineering" and UNECE Regulation No. 155 (R155) embodies a strategic pivot towards standardized cybersecurity practices and regulatory oversight. The United Nations Regulation No. 155 (UN R155) explicitly references ISO/SAE 21434 [22]. This essential standard outlines a comprehensive set of engineering requirements dedicated to the cybersecurity risk management of electrical and electronic (E/E) systems integrated into road vehicles[6]. It meticulously addresses the entire lifecycle of these systems, starting from the initial concept phase through to the development of products, their production, operational period, maintenance routines, and finally, their decommissioning. ISO/SAE 21434 serves as a foundational guideline for ensuring the cybersecurity integrity of not only the primary E/E systems themselves but also their individual components and the interfaces that facilitate their interaction within the vehicular environment. By establishing stringent criteria, this standard aims to fortify the resilience of road vehicles against potential cybersecurity threats and vulnerabilities that can arise at any point during their lifecycle. It emphasizes a proactive approach to cybersecurity, advocating for the early integration of security measures within the design and development processes, thereby ensuring that vehicles are equipped to protect against and withstand cyber threats from the outset and throughout their operational life. A notable distinction between ISO/SAE 21434 and R155 is that the ISO/SAE standard offers OEMs and their

BUPT

suppliers a detailed methodology for assessing asset risk, including suggested techniques for scoring and prioritizing the urgency of vulnerabilities [4].

As ISO/SAE 21434 gains recognition as the global industry standard for automotive cybersecurity practices, its role in facilitating compliance with UNECE R155 becomes increasingly significant. The standard not only offers a structured framework for cybersecurity engineering but also sets a benchmark for legislative compliance across different jurisdictions. The focus on continuous improvement and adaptability within these standards underscores the dynamic nature of automotive cybersecurity, requiring ongoing vigilance and responsiveness to emerging threats. The inclusion of ISO/SAE 21434 within UN R155 underscores the global automotive industry's commitment to adopting uniform and effective cybersecurity practices. This alignment between regulatory requirements and industry standards highlights the critical importance of cybersecurity in the modern vehicular ecosystem, where the proliferation of connected and increasingly autonomous vehicles presents new and complex cybersecurity challenges. Through the application of ISO/SAE 21434's guidelines, manufacturers, suppliers, and stakeholders are equipped with a strategic framework for addressing these challenges, ensuring that vehicles are not only safe and reliable but also secure from cyber threats in an evolving digital landscape.

The foundational link between ISO/SAE 21434 and UNECE R155 is their shared aim of reinforcing the cybersecurity integrity of automotive systems. ISO/SAE 21434 provides an exhaustive framework for cybersecurity engineering and management, setting the stage for a proactive and structured approach to cybersecurity risk management [41]. In parallel, UNECE R155 introduces regulatory mandates for the establishment of a CSMS and the execution of comprehensive cyber risk assessments, essential for vehicle type approval [5]. This regulatory scope extends beyond vehicle manufacturers to an expansive network of suppliers and service providers, integral to the automotive ecosystem.

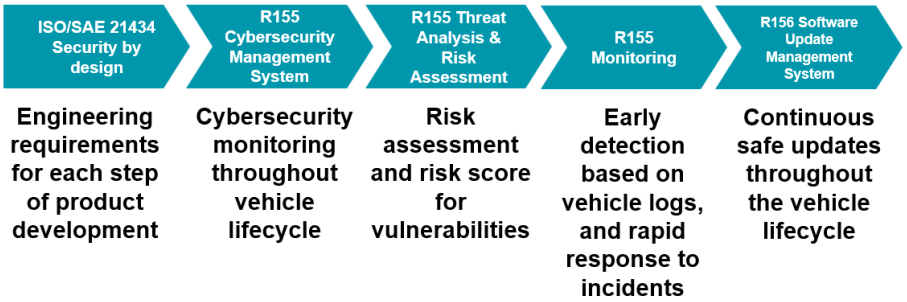


Fig. 8. ISO/SAE 21434 and WP.29 collaborate to safeguard vehicles [5]

UNECE R155's directive for manufacturers to conduct detailed cyber risk assessments, incorporating a CSMS, represents a cornerstone of contemporary automotive

BUPT

cybersecurity strategy. This mandate ensures a systematic approach to identifying, evaluating, and mitigating cybersecurity risks. ISO/SAE 21434 complements this by offering in-depth guidance on CSMS development and maintenance, fostering a unified and consistent understanding across the automotive sector. This harmonized perspective is crucial for maintaining the integrity and resilience of automotive systems against cyber threats. The automotive industry's reliance on a complex network of suppliers for critical components and systems necessitates an extension of cybersecurity responsibilities. Suppliers are required to demonstrate the efficacy of their CSMS to contribute to the overarching cybersecurity posture of the vehicles. This requirement highlights the interconnected nature of automotive cybersecurity, where the security measures adopted by individual entities within the supply chain collectively contribute to the vehicle's overall cybersecurity resilience. ISO/SAE 21434 serves as a blueprint for suppliers to implement robust cybersecurity processes, aligning with R155's objectives and bolstering the security fabric of the automotive supply chain. ISO/SAE 21434 emphasizes the importance of TARA methodologies in identifying and mitigating cybersecurity risks associated with critical items throughout their lifecycle. A central aspect of the newly released cybersecurity standard, ISO/SAE 21434, focuses on conducting threat analysis and risk assessment (TARA) [44]. This emphasis aligns with R155's focus on comprehensive cyber risk assessments, ensuring a cohesive strategy for addressing potential vulnerabilities. Through TARA, both standards advocate for a meticulous evaluation of cybersecurity threats, facilitating the development of targeted protective measures and enhancing the CSMS's efficacy.

As discussed in the previous chapter regarding UNECE R156, the standard ISO 21434-Road Vehicles-Cybersecurity Engineering primarily addresses the fundamental requirements for updating in-vehicle ECUs. Meanwhile, a second standard was developed based on UNECE R156, focusing on over the air updates[45].

The strategic alignment between ISO/SAE 21434 and UNECE R155 epitomizes a comprehensive and collaborative approach to automotive cybersecurity. By establishing a harmonized framework for cybersecurity management, extending cybersecurity responsibilities across the supply chain, prioritizing rigorous risk assessment methodologies, and recognizing the critical role of software updates, these standards and regulations lay the groundwork for a secure automotive future[5]. As the industry continues to evolve amidst the challenges of digital transformation, the synergy between ISO/SAE 21434 and UNECE R155 will be instrumental in shaping resilient and robust automotive cybersecurity landscapes globally.

4.3 The Role of implementing ISO 21434 in Organizations

In the current landscape of the automotive industry, characterized by rapid technological advancements and increasing cyber threats, the implementation of ISO/SAE 21434, "Road Vehicles — Cybersecurity Engineering," has emerged as a critical measure for organizations aiming to safeguard their products and services. The foundation of implementing ISO/SAE 21434 in any organization begins with the establishment of a Cybersecurity Management System (CSMS).

BUPT

Core Element: The Integral Role of a Cybersecurity Management System (CSMS).
At the heart of ISO/SAE 21434's comprehensive approach to bolstering automotive cybersecurity is the implementation of a Cybersecurity Management System (CSMS). The establishment of a CSMS within an organization is not merely a recommendation but a fundamental requirement for adhering to the guidelines set forth by R155 [46]. This system is designed to take a systematic and structured approach to the identification, mitigation, and management of cybersecurity risks, ensuring that security considerations are seamlessly integrated into the fabric of organizational processes and the vehicle lifecycle.

A CSMS serves as the operational backbone of an organization's cybersecurity strategy, embedding security principles into the core of vehicle development processes—from the initial concept and design stages through to production, operation, and eventual decommissioning. The UNECE issued regulation R155, mandates a Cybersecurity Management System (CSMS) certification for vehicles from SAE Level 3 and above [47]. This holistic integration ensures that cybersecurity is not perceived as an auxiliary or afterthought but as an essential component of the organization's DNA, ingrained in every activity and decision. A CSMS can be envisaged as a comprehensive shield that fortifies an organization against the multitude of cyber threats that pervade the digital landscape. This system is characterized by several key features:

- Structured Risk Management: At its core, a CSMS establishes a structured framework for the ongoing assessment and management of cybersecurity risks. This involves the continuous monitoring of the threat environment, assessing the vulnerabilities of vehicle systems, and implementing strategies to mitigate identified risks.
- Definition of Roles and Responsibilities: A well-defined CSMS clearly outlines the cybersecurity roles and responsibilities of team members across the organization. By delineating these roles, everyone from top management to operational staff understands their part in maintaining and enhancing the organization's cybersecurity posture.
- Standardized Procedures for Vulnerability Management: The system prescribes standardized procedures for the identification, assessment, and remediation of vulnerabilities within automotive systems. This includes the adoption of best practices for secure coding, regular penetration testing, and the application of security patches to address known vulnerabilities.
- Incident Response and Management: A CSMS encompasses procedures for the timely detection, reporting, and management of cybersecurity incidents. This ensures that potential security breaches are addressed swiftly and effectively, minimizing their impact on the organization and its stakeholders.
- Effective Communication and Training: Fundamental to a CSMS is the facilitation of effective communication about cybersecurity matters within the organization. This includes the provision of regular training and awareness programs for employees to understand the latest cyber threats and how to prevent them, fostering a culture of cybersecurity awareness.

BUPT

- Legal and Regulatory Compliance: Implementing a CSMS also involves ensuring compliance with relevant legal, regulatory, and contractual obligations related to cybersecurity. This includes adhering to international standards such as ISO/SAE 21434, as well as national and regional regulations governing automotive cybersecurity.
- Continual Improvement Process: A CSMS is not static; it embodies a philosophy of continuous improvement. Through regular reviews and audits of the cybersecurity management practices, organizations can adapt and evolve their CSMS to meet emerging threats and incorporate new technological advancements.

In essence, the adoption of a CSMS as mandated by ISO/SAE 21434 is a strategic investment in the future security and resilience of automotive products and services. It signifies an organization's commitment to implementing a proactive and comprehensive approach to cybersecurity management, ensuring the protection of vehicles from conception through to decommissioning. The CSMS stands as a testament to the organization's dedication to safeguarding not only its tangible assets but also the trust and safety of its customers in an increasingly connected and digitalized automotive landscape. Moreover, with the introduction of regulations R155 and R156, the UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) has made CSMS certification compulsory in Europe for all new types of vehicles beginning in June 2022, and for all vehicles starting in 2024 [48].

Conducting Comprehensive Threat Analysis and Risk Assessment (TARA).
The implementation of ISO/SAE 21434 within organizations necessitates a rigorous and comprehensive approach to Threat Analysis and Risk Assessment (TARA). This process is pivotal in enabling organizations to meticulously identify, scrutinize, and appraise potential cybersecurity threats and the risks they pose to their automotive systems. In TARA, damage scenarios for the vehicle/components under development need to be identified [39]. TARA serves as a cornerstone for understanding the intricate landscape of cyber threats and formulating robust countermeasures to mitigate these risks effectively. Its importance in the cybersecurity framework cannot be overstated, as it provides a systematic methodology for addressing potential vulnerabilities within automotive systems.

TARA is envisioned not merely as an isolated activity but as a dynamic, ongoing process that adapts in tandem with the evolving cyber threat environment. This adaptability ensures that the cybersecurity measures implemented are not static but evolve to counter new and emerging threats effectively. This engineering process necessitates conducting a thorough Threat Analysis and Risk Assessment (TARA), which includes calculating relative values for impact and attack feasibility to determine the associated risk [49]. The continuous nature of TARA is essential for maintaining a state of vigilance and preparedness within organizations, allowing them to respond proactively to changes in the threat landscape. Through the process of TARA, organizations embark on a multi-stage journey of cybersecurity assessment:

BUPT

- Identification of Potential Threats: This initial stage involves mapping out the cybersecurity landscape to pinpoint potential threats that could exploit vulnerabilities within automotive systems. This step is crucial for establishing a baseline understanding of the types of cyber threats that exist and which systems or components are most at risk.
- Analysis of Threat Capabilities: Following the identification of potential threats, the next step involves analyzing the capabilities of these threats. This analysis considers the methods, techniques, and resources available to potential attackers, providing insights into how a threat might be executed and the likelihood of its occurrence.
- Evaluation of System Vulnerabilities: Concurrent with threat analysis, organizations must assess the vulnerabilities within their automotive systems. This involves a detailed examination of system architectures, software components, and network interfaces to identify weaknesses that could be exploited by cyber threats.
- Risk Assessment: With an understanding of both the threats and vulnerabilities, organizations can then assess the risk level. This involves evaluating the potential impact of each identified threat exploiting a given vulnerability, considering factors such as the severity of impact on vehicle operation, safety, and data privacy.
- Development of Countermeasures and Mitigation Strategies: Armed with a comprehensive understanding of threats, vulnerabilities, and associated risks, organizations can then develop targeted countermeasures and mitigation strategies. This stage focuses on designing and implementing controls to reduce risk to an acceptable level, whether through technical solutions, process changes, or a combination of both.
- Prioritization of Cybersecurity Efforts: An essential aspect of TARA is the prioritization of cybersecurity efforts. Given the resource constraints that most organizations face, it becomes critical to allocate resources effectively, focusing on mitigating the most significant threats and vulnerabilities first.
- Continuous Monitoring and Review: Finally, TARA mandates continuous monitoring and review of the threat environment and the effectiveness of implemented countermeasures. This ongoing evaluation ensures that the organization's cybersecurity posture remains robust over time, adapting to new threats and emerging technologies.

BUPT

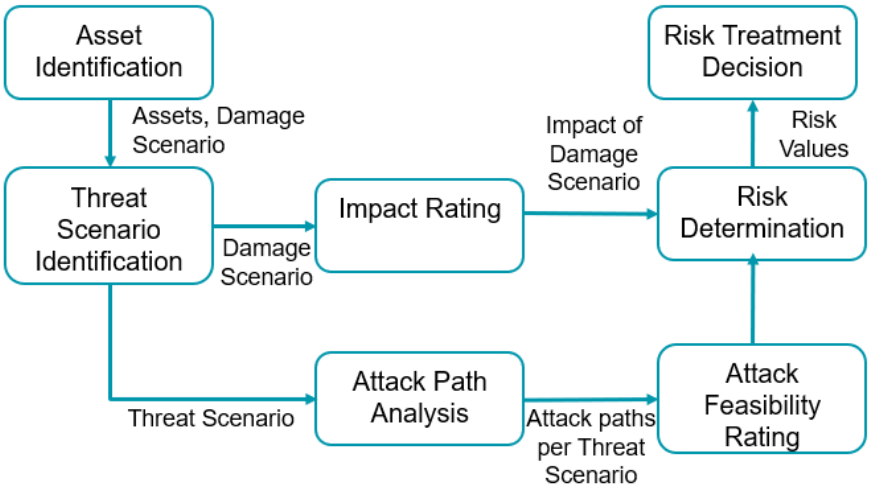


Fig. 9. High-level TARA Steps [50]

The implementation of TARA within the ISO/SAE 21434 framework empowers organizations to create a proactive and resilient cybersecurity strategy. By systematically identifying, analyzing, evaluating, and mitigating cybersecurity threats and risks, organizations can ensure the safety, reliability, and integrity of their automotive products. This continuous, iterative process not only enhances the security of automotive systems but also fosters a culture of cybersecurity awareness and vigilance within organizations, ultimately contributing to the safety and security of the automotive industry as a whole. Concluding, TARA is a crucial component of the automotive cybersecurity engineering process. Essential to determining risk is the identification of the attack surface, along with a detailed assessment of the feasibility of potential attacks on each asset of a modern vehicle, for which a generic reference architecture has been established [3].

Cybersecurity in the Concept Phase.
The concept phase stands as a pivotal juncture in the lifecycle of automotive products, marking the stage where fundamental decisions regarding design, functionality, and overarching development strategies are solidified. The standard establishes a structured cybersecurity framework that integrates cybersecurity as a fundamental aspect of engineering across the entire lifecycle of a vehicle, from the conceptual phase through to decommissioning [4]. At this early stage, the groundwork for the future of the automotive product is laid, setting the trajectory for its development, production, and operational phases. The implementation of ISO/SAE 21434 standards from the very beginning of this phase is not merely advantageous but essential, ensuring that cybersecurity is not an adjunct but a core component of the design and development process. This early-stage integration of cybersecurity measures, as advocated by ISO/SAE 21434, facilitates a holistic approach towards identifying and addressing potential

BUPT

cybersecurity vulnerabilities and threats [6]. By weaving cybersecurity considerations into the fabric of the design process, organizations are equipped to preemptively recognize and mitigate cybersecurity challenges. This forward-looking strategy encompasses the evaluation of potential threat vectors, the assessment of risk levels associated with various design choices, and the proactive incorporation of security features and protocols that are robust against such threats [6].

The benefits of prioritizing cybersecurity during the concept phase are manifold. Firstly, it enables the seamless embedding of necessary security features into the automotive product from the ground up. This foundational integration of security measures ensures that cybersecurity is an intrinsic attribute of the product, rather than a supplementary layer added in response to subsequent vulnerability discoveries. Such an approach not only enhances the security efficacy of these measures but also optimizes the product's overall design for security resilience. Furthermore, by addressing cybersecurity at the outset, organizations can sidestep the pitfalls of costly redesigns and retrofitting efforts. Retrofitting security features into an already developed product not only incurs significant financial burdens but also extends development timelines, potentially compromising the product's market competitiveness and regulatory compliance. Early integration, conversely, streamlines the development process, ensuring that products are engineered with a robust cybersecurity posture from the onset. Focusing on cybersecurity during the concept phase affords organizations the opportunity to align their products with evolving regulatory standards and consumer expectations regarding data protection and privacy. This alignment is crucial in today’s increasingly security-conscious market, where consumer trust can significantly influence product success. By proactively embedding advanced cybersecurity features, organizations can differentiate their products, enhance their brand reputation, and foster consumer trust. Moreover, this proactive approach to cybersecurity encourages a culture of security awareness and innovation within organizations. It prompts cross-functional teams to collaborate closely from the earliest stages of product development, fostering an organizational ethos where cybersecurity is a shared responsibility and integral to the product innovation process. This collaborative environment not only enriches the product design with comprehensive security considerations but also catalyzes the development of innovative security solutions that can set new industry standards.

Continuous Cybersecurity Activities: A Lifecycle Approach.

ISO/SAE 21434 sets a benchmark in the automotive industry for integrating continuous cybersecurity activities as a fundamental aspect of the lifecycle of automotive products. This standard advocates for a holistic approach, emphasizing that cybersecurity should permeate every phase of a vehicle's lifecycle—from the initial concept and design stages, through development and production, to operation, maintenance, and ultimately, decommissioning [5]. This lifecycle approach to cybersecurity transcends the notion of security as a mere checkpoint or afterthought in the development process. Instead, it positions cybersecurity as a continuous, proactive, and integral component of automotive product development and maintenance.

The lifecycle approach outlined in ISO/SAE 21434 encompasses a comprehensive suite of continuous cybersecurity activities. Each activity plays a pivotal role in

BUPT

maintaining and enhancing the cybersecurity posture of automotive products over their entire lifespan. These activities include, but are not limited to, the following key areas [6]:

- Ongoing Risk Assessments: Regular and systematic risk assessments are crucial for identifying and evaluating potential cybersecurity threats throughout the lifecycle of automotive products. These assessments provide the foundation for understanding the evolving threat landscape and the specific vulnerabilities that may affect automotive systems at different stages of their lifecycle.
- Development and Implementation of Security Measures: Based on the outcomes of risk assessments, appropriate security measures are developed and implemented. This includes the integration of secure design principles in the concept phase, the application of secure coding practices during development, and the incorporation of robust security mechanisms in production.
- Regular Updates and Patch Management: The dynamic nature of cybersecurity threats necessitates regular updates and the application of patches to automotive software and systems. This activity involves the timely identification of new vulnerabilities, the development of patches or updates to address these vulnerabilities, and the efficient distribution and installation of these patches across the fleet of vehicles.
- Constant Monitoring of Cybersecurity Incidents: Continuous monitoring for potential cybersecurity incidents is essential for early detection and response. This involves the implementation of advanced monitoring systems and procedures to detect anomalies or unauthorized activities that could indicate a cybersecurity breach.
- Swift Response to Emerging Threats: The capability to respond swiftly to emerging threats is critical for minimizing the potential impacts on vehicle safety and consumer privacy. This requires the establishment of a dedicated incident response team, equipped with the necessary tools and procedures to quickly assess and mitigate the impact of cybersecurity incidents.
- Feedback Loops and Continuous Improvement: A key aspect of continuous cybersecurity activities is the establishment of feedback loops that facilitate the collection and analysis of data on cybersecurity incidents and the effectiveness of implemented security measures. This data is invaluable for driving continuous improvement in cybersecurity practices, ensuring that they remain effective against evolving threats.
- Security Considerations in Decommissioning: The lifecycle approach also extends to the decommissioning phase, where vehicles are retired from service. Proper security measures must be implemented to ensure that sensitive data is securely erased and that decommissioned vehicles do not pose a cybersecurity risk.
- Stakeholder Communication and Collaboration: Continuous cybersecurity activities also involve regular communication and collaboration with stakeholders, including suppliers, regulatory bodies, and consumers. This ensures that all parties are informed about potential cybersecurity risks and the measures taken to mitigate them.

By embracing this lifecycle approach to cybersecurity, as advocated by ISO/SAE 21434, organizations in the automotive industry can ensure that cybersecurity is an integral and continuous part of their product development and maintenance processes. This proactive stance not only enhances the security and resilience of automotive

BUPT

products but also fosters trust among consumers and stakeholders, reinforcing the commitment to safeguarding vehicle safety and privacy in an increasingly connected and digital world.

Ensuring Cybersecurity During Production.
Ensuring cybersecurity during the production phase of automotive products is a critical concern that requires meticulous attention and rigorous implementation of ISO/SAE 21434 guidelines. The standard delineates the process and specifies targets for risk analysis and response, highlighting the importance of addressing ongoing cybersecurity threats and vulnerabilities throughout the development, production, and post-production stages [4]. As products transition from the conceptual and design stages into production, the landscape of cybersecurity challenges evolves. The manufacturing process introduces a new set of risks and vulnerabilities, making it imperative to enforce robust cybersecurity measures to safeguard against potential threats. This phase is crucial for embedding security into the very fabric of the product, ensuring that both software and hardware components are imbued with resilience against cyber threats.

Securing the Supply Chain. A secure supply chain is fundamental to maintaining cybersecurity during production. The complexity of modern automotive supply chains, often spanning multiple countries and involving numerous suppliers, can introduce multiple points of vulnerability. Ensuring the integrity of every component, from the smallest sensor to complex software systems, requires a comprehensive approach. Implementing ISO/SAE 21434 involves conducting thorough security assessments of suppliers, establishing secure communication protocols, and requiring suppliers to adhere to stringent cybersecurity standards. By securing the supply chain, organizations can significantly reduce the risk of introducing vulnerabilities into automotive products during the manufacturing process.

Protecting Production Data. The protection of production data is another critical aspect of ensuring cybersecurity during the manufacturing phase. This encompasses all data related to manufacturing processes, including software code, design specifications, and testing protocols. Unauthorized access to or manipulation of this data could compromise the security of the manufacturing process and, by extension, the final product. As ransom attacks throughout the supply chain could significantly disrupt operational availability and production [4]. Implementing robust data encryption, access control measures, and continuous monitoring of data flows are essential steps in safeguarding production data. These measures ensure that sensitive information remains confidential and integral, thereby upholding the integrity of the production process.

Ensuring Component Integrity. Ensuring that software and hardware components are free from vulnerabilities is a cornerstone of cybersecurity during the production phase. This involves rigorous testing and validation procedures to identify and rectify any security vulnerabilities before the components are integrated into the final product. Regular software updates and patches are critical to addressing vulnerabilities that may be discovered in software components. Similarly, hardware components require thorough inspection and testing to ensure they are not susceptible to tampering or other forms of cyber threats. Establishing a protocol for continuous vulnerability assessment and management throughout the production process is vital to maintaining the security

BUPT

integrity of components. Automotive cyber-attacks can lead to both direct and indirect financial consequences, many of which are substantial. Direct costs include expenses related to recalls and production shutdowns [5].

Preventing the Introduction of Cyber Threats: The production phase is particularly vulnerable to the introduction of cyber threats through manufacturing processes. This can occur through compromised software updates, malicious insiders, or insecure production environments. Implementing stringent security protocols, such as secure boot mechanisms, code signing, and access controls, can mitigate these risks. Additionally, employee training and awareness programs are essential to ensure that all personnel involved in the production process are aware of potential cybersecurity threats and the importance of maintaining security protocols.

Adherence to Cybersecurity Standards: Ensuring that the final product adheres to the highest standards of cybersecurity is the ultimate goal of implementing ISO/SAE 21434 during the production phase. This requires a holistic approach to security, encompassing every aspect of the production process, from supplier selection to component testing and data protection. Regular audits and compliance checks are necessary to ensure that all elements of the production process meet or exceed the standards set forth in ISO/SAE 21434 [8]. By doing so, organizations can assure customers and stakeholders that their products are not only functional and high-quality but also secure against cyber threats.

Decommissioning with Security in Mind.

The decommissioning phase, the final chapter in the lifecycle of automotive products, represents a critical juncture where the principles of cybersecurity must be meticulously applied, yet it is a phase that often does not receive the attention it duly merits. As automotive products reach the culmination of their operational life, the imperative to decommission them securely becomes paramount. This necessity is underscored by the potential risks associated with the improper handling of data and hardware, which can lead to the unintended exposure of sensitive information. The implementation of ISO/SAE 21434 provides a comprehensive framework for organizations, guiding them through the process of decommissioning with an emphasis on security, thereby ensuring the protection of data integrity and the prevention of information leakage. This standard addresses cybersecurity management within organizations and individual projects, covering cybersecurity engineering throughout the project lifecycle, including production, operation, and decommissioning phases [51].

Ensuring Secure Data Erasure. One of the foremost considerations during the decommissioning phase is the secure erasure of stored data. Automotive products, particularly those embedded with advanced technologies and connectivity features, are repositories of a vast array of data, from personal user information to proprietary organizational data. Secure data erasure involves the systematic deletion of this data in a manner that renders it irretrievable. ISO/SAE 21434 outlines methodologies for secure data deletion, recommending the use of standards-based data sanitization processes to ensure that data, once erased, cannot be recovered or reconstructed. This process is vital in mitigating the risks of data breaches and protecting user privacy post-decommissioning.

BUPT

Managing the Disposal of Hardware. The disposal of hardware components presents another significant challenge during the decommissioning phase. The physical components of decommissioned products, if not disposed of securely, can become sources of security vulnerabilities. For instance, memory devices and other storage media can contain residual data even after attempts at erasure. ISO/SAE 21434 guides organizations in the secure disposal of hardware, emphasizing the importance of physical destruction methods or specialized recycling processes that ensure the complete destruction of data-bearing components. By adhering to these guidelines, organizations can prevent the inadvertent leakage of sensitive information through discarded hardware.

Establishing Decommissioning Protocols. The development and implementation of formal decommissioning protocols are critical components of ISO/SAE 21434's guidance. These protocols delineate the steps and procedures to be followed during the decommissioning process, ensuring a consistent and secure approach across all decommissioned products. This includes the documentation of decommissioning activities, the assignment of responsibilities to designated personnel, and the establishment of audit trails to verify the completeness and security of the decommissioning process. Through these structured protocols, organizations can ensure that decommissioning activities are conducted systematically and securely.

Assessing and Mitigating Residual Risks. Even with stringent decommissioning processes in place, the potential for residual risks remains. ISO/SAE 21434 encourages organizations to conduct thorough risk assessments as part of the decommissioning process, identifying any remaining vulnerabilities and implementing measures to mitigate these risks. This might involve additional security controls for particularly sensitive data or enhanced physical security measures for the storage and transportation of decommissioned hardware. By assessing and addressing these residual risks, organizations can further secure the decommissioning process against potential security threats.

Training and Awareness. Finally, the importance of training and awareness cannot be overstated in ensuring the security of the decommissioning process. Personnel involved in decommissioning activities must be adequately trained in secure data erasure techniques, hardware disposal methods, and the handling of sensitive information. Additionally, raising awareness about the importance of security during decommissioning can foster a culture of security mindfulness within the organization, ensuring that all stakeholders recognize their role in safeguarding data integrity and privacy throughout the decommissioning phase.

Conclusion.

The adoption and rigorous implementation of ISO/SAE 21434 within the automotive industry mark a significant advancement in the collective approach to cybersecurity. This standard does not merely introduce a set of guidelines but catalyzes a paradigm shift in how cybersecurity is perceived and integrated across the entire lifecycle of automotive products and services. By laying the foundation for a Cybersecurity Management System (CSMS), facilitating in-depth Threat Analysis and Risk Assessment (TARA), and promoting a culture of continuous cybersecurity vigilance, ISO/SAE 21434 equips organizations with the tools and methodologies necessary to navigate the complex cybersecurity landscape effectively [6]. The establishment of a CSMS under

BUPT

the auspices of ISO/SAE 21434 empowers organizations to adopt a structured and systematic approach to cybersecurity. This framework ensures that cybersecurity measures are not siloed but are seamlessly woven into the very essence of organizational operations, from strategic planning to daily operations. Through the CSMS, organizations can delineate clear roles and responsibilities, enforce consistent security policies and procedures, and foster an organizational culture that prioritizes cybersecurity as a fundamental operational imperative [6].

Conducting comprehensive TARA is another cornerstone of ISO/SAE 21434's approach to bolstering automotive cybersecurity. By systematically identifying, analyzing, and assessing potential cybersecurity threats and their associated risks, organizations can gain invaluable insights into the vulnerabilities within their systems and processes. TARA enables the prioritization of risks, ensuring that resources are allocated efficiently to address the most critical vulnerabilities first. This proactive stance towards threat identification and risk management is crucial for developing resilient automotive products that can withstand the evolving threats in the cybersecurity landscape. From the concept phase, where initial designs are imbued with security considerations, to the decommissioning phase, where the secure disposal of products safeguards against data leakage, ISO/SAE 21434 provides a holistic framework for integrating cybersecurity into the fabric of automotive design and manufacturing [6]. This comprehensive framework ensures that every stage of the product lifecycle is underpinned by robust cybersecurity measures, thereby safeguarding the safety and privacy of users in an increasingly interconnected and digital world. Engaging in continuous cybersecurity activities further amplifies the effectiveness of ISO/SAE 21434's implementation. This ongoing commitment to cybersecurity vigilance ensures that organizations remain responsive to new threats, vulnerabilities, and technological advancements. Continuous monitoring, regular updates and patches, and the iterative improvement of cybersecurity practices ensure that the security measures in place evolve in tandem with the changing threat environment. This dynamic approach to cybersecurity underscores the importance of adaptability and resilience in securing automotive products and services throughout their lifecycle.

In conclusion, the implementation of ISO/SAE 21434 within organizations serves as a critical lever in enhancing the cybersecurity posture of automotive products and services. This standard not only addresses the current cybersecurity challenges facing the automotive industry but also anticipates future threats, ensuring that organizations are well-prepared to protect their products, services, and users. As the automotive industry continues to evolve, driven by innovations in connectivity and automation, the principles outlined in ISO/SAE 21434 will remain integral to the development of secure, reliable, and trustworthy automotive technologies, fostering a safer and more secure automotive future for all.

4.4 ISO/SAE 21434 Overview

This subchapter provides a comprehensive overview of the clauses within ISO/SAE 21434, elucidating the framework's scope, objectives, and the systematic methodology it proposes for integrating cybersecurity across the vehicle lifecycle.

BUPT

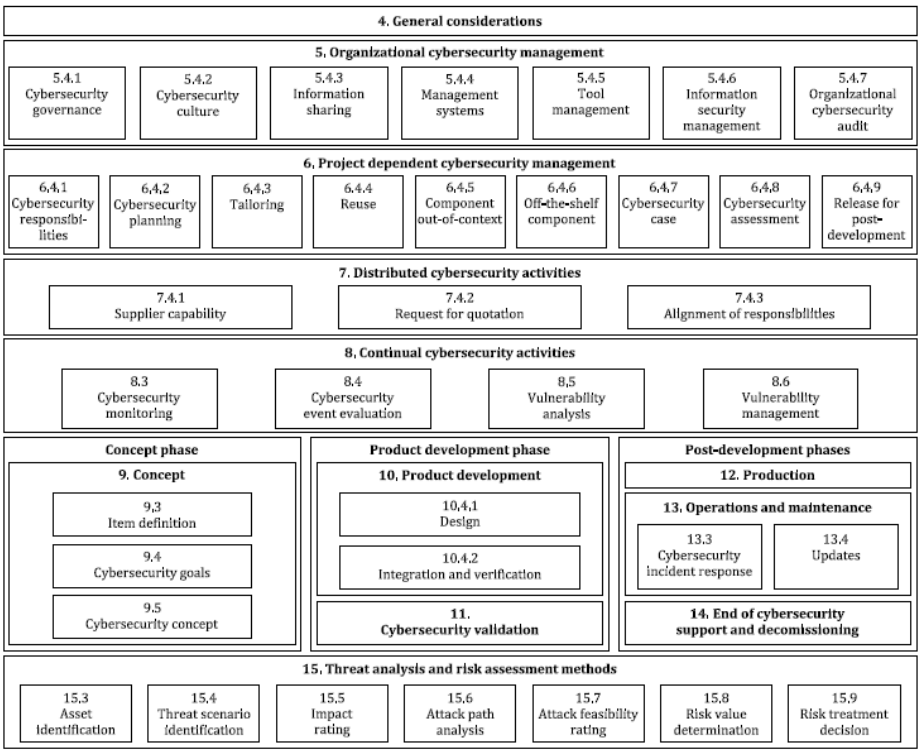


Fig. 10. Overview of ISO/SAE 21434 clauses [6]

Clause 4: General Considerations.
Clause 4 serves as the foundational bedrock of the standard, offering vital contextual information and perspectives on the approach to cybersecurity engineering in road vehicles [6]. It is informational in nature, setting the stage for the detailed cybersecurity management and engineering practices outlined in subsequent clauses. This clause ensures that readers grasp the underlying principles and rationale guiding the standard's approach to cybersecurity.

Clause 5: Organizational Cybersecurity Management.
At the heart of organizational cybersecurity management lies the establishment and maintenance of robust cybersecurity governance and culture. This foundational aspect underscores the importance of fostering an environment where cybersecurity is prioritized and integrated into the operational ethos of the organization. It involves the creation and enforcement of specific organizational rules and processes dedicated to cybersecurity, which are meticulously audited to ensure alignment with the objectives set forth in ISO/SAE 21434 [6]. Key to this endeavor is the development of a cybersecurity-aware culture, encompassing management of cybersecurity awareness and

BUPT

competencies, along with a commitment to continuous improvement. Organizations are tasked with specifying clear rules and processes that not only meet but exceed the benchmarks of cybersecurity excellence, undergoing independent audits to validate their adherence to the stringent requirements of this document. In support of cybersecurity engineering efforts, organizations are also encouraged to implement comprehensive management systems tailored to cybersecurity. This includes the effective management of cybersecurity tools and the integration of cybersecurity principles within existing quality management systems. By doing so, organizations can ensure a holistic approach to cybersecurity management, embedding security considerations seamlessly into every facet of their operations.

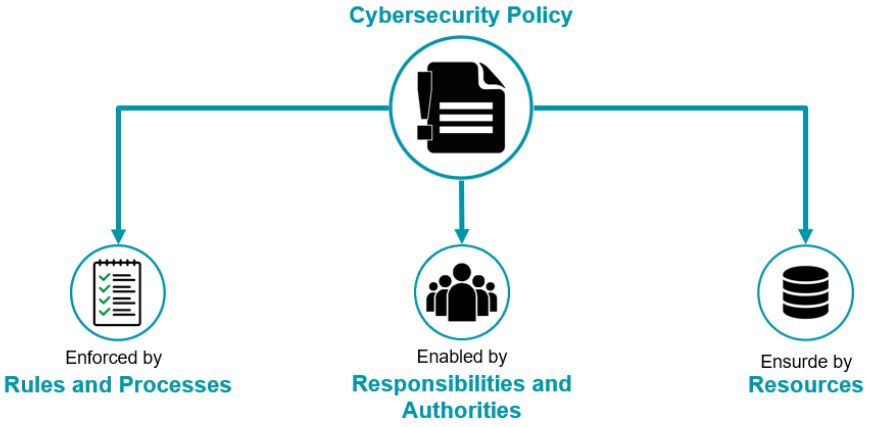


Fig. 11. How Cybersecurity Policy is enforced, enabled, and ensured

The objectives outlined in Clause 5 serve as guiding principles for organizations aiming to bolster their cybersecurity posture. These objectives include [6]:

- Cybersecurity Policy and Organizational Processes: Defining a clear cybersecurity policy alongside organizational rules and processes specifically tailored to cybersecurity. This framework serves as the backbone for cybersecurity management within the organization.
- Assignment of Responsibilities and Authorities: Clearly delineating the responsibilities and corresponding authorities essential for conducting cybersecurity activities. This ensures accountability and promotes an organized approach to cybersecurity
- Support for Cybersecurity Implementation: Facilitating the implementation of cybersecurity measures by providing necessary resources and managing the interactions between cybersecurity processes and related operational processes.
- Cybersecurity Risk Management: Actively managing cybersecurity risks through identification, assessment, and mitigation strategies to protect organizational assets and information.

BUPT

- Cultivation of a Cybersecurity Culture: Establishing and nurturing a culture that values cybersecurity, including the management of competencies, raising awareness among staff, and fostering an environment of continuous improvement.
- Sharing of Cybersecurity Information: Encouraging and managing the sharing of cybersecurity information within and possibly outside the organization to enhance collective security knowledge and practices.
- Maintenance of Cybersecurity Management Systems: Instituting and maintaining management systems that support and enhance the organization's ability to maintain robust cybersecurity measures.
- Tool Usage and Cybersecurity Impact: Providing evidence that the utilization of tools and technologies does not adversely impact the organization's cybersecurity posture.
- Organizational Cybersecurity Audit: Conducting thorough cybersecurity audits at the organizational level to assess compliance with established cybersecurity policies and practices.

Additionally, Clause 5 introduces a conceptual framework (illustrated in Figure 11) that illustrates the relationship between the overarching cybersecurity policy ([RQ-05-01]) and the specific organizational cybersecurity rules and processes ([RQ-05-02]), responsibilities ([RQ-05-03]), and resources ([RQ-05-04]) [6]. This visual representation serves as a roadmap for organizations, guiding the structured implementation of cybersecurity management practices in alignment with the strategic goals outlined in ISO/SAE 21434.

Therefore, Clause 5 of ISO/SAE 21434 lays the foundation for effective organizational cybersecurity management, providing a detailed blueprint for organizations to define, implement, and manage cybersecurity measures. By adhering to the objectives and guidelines set forth in this clause, organizations can ensure a comprehensive and proactive approach to cybersecurity, safeguarding their assets and information in an increasingly digital and connected world.

Clause 6: Project Dependent Cybersecurity Management.
Clause 6 of ISO/SAE 21434 dives into the nuanced requirements associated with managing cybersecurity within the context of specific projects. It emphasizes that cybersecurity management is not a one-size-fits-all process but requires careful consideration and adaptation to the unique characteristics and requirements of each project. This clause lays out a structured approach for integrating cybersecurity activities into project management, including the allocation of responsibilities and the planning of cybersecurity tasks tailored to the project's specific needs [6].

One of the key aspects covered in this clause is the concept of tailoring cybersecurity activities to fit the unique demands of a project. This flexibility is crucial for addressing the diverse nature of projects within the automotive sector, ranging from the development of entirely new systems to updates of existing components. Tailoring allows for adjustments to the standard cybersecurity activities based on rational justification, ensuring that the cybersecurity management approach remains both efficient and effective. Examples of scenarios where tailoring might be necessary include [6]:

BUPT

- Reuse of Components: Reusing items and components from previous projects or external sources can be an effective strategy for development. However, any modifications or changes in the operational environment might introduce new vulnerabilities. This clause highlights the importance of reassessing reused components for potential security risks, especially if the threat landscape has evolved since their initial development.
- Out-of-Context Development: Some components may be developed with an assumed usage context, without specific customer requirements in mind. These "out-of-context" components, such as microcontrollers, must be developed with generic security requirements that can later be tailored to fit specific projects.
- Utilization of Off-The-Shelf Components: The use of off-the-shelf components, including third-party software libraries or open-source software, is acknowledged. Given that these components may not have been developed following the guidelines of ISO/SAE 21434, the clause advises on considering their security implications carefully.
-

The objectives outlined in Clause 6 serve to guide organizations in effectively managing project-specific cybersecurity concerns [6]:

- Assignment of Responsibilities: Clearly defining who is responsible for various cybersecurity activities within the project ensures accountability and promotes effective management of cybersecurity tasks.
- Planning of Cybersecurity Activities: Establishing a comprehensive plan for cybersecurity activities, including tailored tasks, sets a clear roadmap for integrating security throughout the project lifecycle.
- Creation of a Cybersecurity Case: Developing a cybersecurity case helps document the rationale, activities, and assessments related to cybersecurity, serving as a record of the project's security considerations.
- Conducting Cybersecurity Assessments: If applicable, performing detailed cybersecurity assessments to evaluate the effectiveness of security measures and identify any remaining vulnerabilities.
- Release Decisions: Making informed decisions on whether an item or component can be released for post-development activities from a cybersecurity standpoint, ensuring that security risks have been adequately addressed.

Clause 6 of ISO/SAE 21434 underscores the importance of tailored, project-specific cybersecurity management within the automotive industry. By providing a framework for the flexible integration of cybersecurity activities into project management, this clause enables organizations to address the unique cybersecurity challenges of each project effectively. Through careful planning, tailored activity definition, and rigorous assessment, organizations can ensure that their projects not only meet but exceed the cybersecurity standards required for the safe and secure development of automotive components and systems.

BUPT

Clause 7: Distributed Cybersecurity Activities.
In the intricate ecosystem of automotive development, where components and systems often traverse organizational boundaries, the management of distributed cybersecurity activities becomes crucial. Clause 7 of ISO/SAE 21434 zeroes in on this complexity, addressing scenarios where responsibilities for cybersecurity are shared across different entities. This clause is pertinent in situations involving [6]:

- Distributed Development Activities: Items and components that are developed through collaborative efforts across multiple organizations or divisions.
- Customer-Supplier Interactions: The dynamic exchanges between customers and suppliers, where cybersecurity responsibilities are intertwined with the flow of components and information.
- Contractual Phases: Various stages of development and delivery where agreements dictate the cybersecurity obligations at the customer/supplier interface.

Notably, this clause underscores that internal suppliers should be managed with the same rigor as external entities, emphasizing the universal importance of cybersecurity regardless of the organizational relationship. The automotive industry's structure often sees organizations operating in dual roles – as both customers and suppliers – depending on the project context. For instance, a tier-1 organization might supply a component to an Original Equipment Manufacturer (OEM) while simultaneously acting as a customer to a tier-2 organization for another element of the same project. This dual role necessitates a clear understanding and management of distributed cybersecurity activities to ensure that all parties involved fulfill their cybersecurity responsibilities effectively.

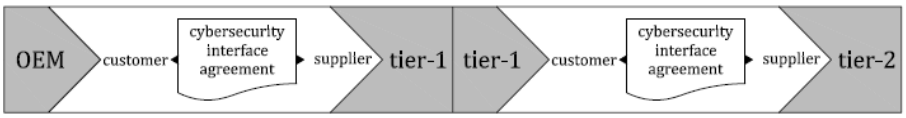


Fig. 12. Distributed Cybersecurity Activities [6]

The clause emphasizes the need for clear definitions of interactions, dependencies, and responsibilities among all parties engaged in the development, supply, and implementation of automotive components. This includes establishing clear communication channels, defining cybersecurity requirements and expectations, and ensuring that these are integrated into contractual agreements and project plans.

The core objective of this clause is to delineate the interactions, dependencies, and responsibilities associated with distributed cybersecurity activities between customers and suppliers. This involves [6]:

- Clarifying Roles and Responsibilities: Ensuring that each party involved in the distributed development and supply chain is fully aware of their cybersecurity responsibilities.

BUPT

- Defining Interactions: Establishing how organizations will interact concerning cybersecurity, including the mechanisms for reporting vulnerabilities, sharing threat intelligence, and conducting joint cybersecurity assessments.
- Managing Dependencies: Identifying and managing the cybersecurity dependencies that exist between components and systems being developed or supplied by different organizations.
- Integrating Cybersecurity into Agreements: Ensuring that cybersecurity considerations are explicitly included in agreements between customers and suppliers, with clear stipulations regarding cybersecurity standards, reporting obligations, and remediation responsibilities.

By addressing these aspects, Clause 7 provides a framework for managing the complexities associated with distributed cybersecurity activities in the automotive sector. It acknowledges the interconnected nature of modern automotive development and the critical need for a coordinated approach to cybersecurity across the industry's vast and varied supply chain.

Clause 8: Continual Cybersecurity Activities.
In the dynamic and evolving landscape of automotive cybersecurity, the need for vigilant and ongoing security practices cannot be overstated. Clause 8 of ISO/SAE 21434 emphasizes the importance of continuous cybersecurity activities that span the entire lifecycle of automotive products, transcending the boundaries of specific projects. This clause delineates a comprehensive approach to maintaining a robust cybersecurity posture through constant monitoring, evaluation, and management of cybersecurity threats and vulnerabilities [6].

A pivotal component of continual cybersecurity activities is the rigorous process of cybersecurity monitoring. This involves the systematic collection and analysis of cybersecurity information to detect potential threats and vulnerabilities. The process is designed to trigger triage based on predefined criteria, ensuring that cybersecurity events are promptly identified and assessed for their potential impact. Following the initial monitoring phase, cybersecurity event evaluation plays a critical role in determining whether a cybersecurity event poses a genuine risk to an item or component. This evaluation process scrutinizes the event to ascertain if it reveals any underlying weaknesses that could compromise the security integrity of the automotive product. Once a potential weakness is identified, vulnerability analysis is conducted to thoroughly examine the nature and severity of the weakness. This analysis assesses the feasibility of exploitation and the potential consequences, providing a foundation for informed decision-making regarding vulnerability mitigation strategies. Building on the insights gained from vulnerability analysis, vulnerability management encompasses the tracking and resolution of identified vulnerabilities. This crucial phase ensures that vulnerabilities are addressed systematically, from initial identification through to remediation or mitigation, up until the end of the product's cybersecurity support lifecycle.

BUPT

The overarching objectives of Clause 8 are designed to fortify the cybersecurity resilience of automotive products across their lifecycle. These objectives include [6]:

- Monitoring Cybersecurity Information: To proactively identify cybersecurity events through the continuous monitoring of relevant cybersecurity information.
- Evaluating Cybersecurity Events: To assess identified cybersecurity events for their potential to expose or exploit weaknesses within automotive items or components.
- Identifying Vulnerabilities from Weaknesses: To distinguish vulnerabilities that stem from identified weaknesses, enabling targeted cybersecurity interventions.
- Managing Identified Vulnerabilities: To implement effective vulnerability management practices, ensuring that vulnerabilities are addressed promptly and efficiently to maintain the security integrity of automotive products.

Clause 8 of ISO/SAE 21434 encapsulates the essence of continual cybersecurity activities within the automotive industry. By outlining a structured approach to cybersecurity monitoring, event evaluation, vulnerability analysis, and management, this clause provides organizations with a blueprint for sustaining a proactive and adaptive cybersecurity posture. The meticulous execution of these continual cybersecurity activities ensures that automotive products are not only secure upon release but remain resilient against emerging cybersecurity threats throughout their operational lifespan. This commitment to ongoing cybersecurity vigilance is crucial for protecting the safety and privacy of users in an increasingly connected automotive ecosystem.

Clause 9: Concept Phase.
The concept phase is a critical stage in the development lifecycle of automotive products, focusing on the integration of vehicle-level functionality within specific items. Clause 9 of ISO/SAE 21434 delves into the intricate process of shaping the cybersecurity framework at the very inception of a product's design. This foundational phase sets the stage for all subsequent cybersecurity efforts, emphasizing the importance of a well-defined item and its operational environment.

A key element of this phase is the "Item Definition", which meticulously identifies the item and its operational environment [6]. This definition serves as the cornerstone for all future activities, ensuring that cybersecurity considerations are aligned with the specific characteristics and requirements of the item in question. The item definition encapsulates the functionalities, interfaces, and interactions of the automotive component within its intended operational context, providing a clear blueprint for tailoring cybersecurity measures effectively. Subsequent to defining the item, Clause 9 outlines the establishment of cybersecurity goals, representing the pinnacle of cybersecurity requirements. These goals are formulated based on a thorough assessment of cybersecurity risks, utilizing the methodologies detailed in Clause 15 [6]. In addition to setting cybersecurity goals, this clause also introduces the concept of cybersecurity claims. These claims articulate the rationale behind decisions to retain or share risks, offering a transparent explanation of the adequacy of risk management strategies. Building upon the cybersecurity goals, the "Cybersecurity Concept" encompasses both the specific cybersecurity requirements for the item and the requisite conditions of its operational

BUPT

environment. This comprehensive concept is derived directly from the established cybersecurity goals, ensuring that all cybersecurity measures are firmly rooted in the overarching objectives. The cybersecurity concept represents a holistic view of the item, integrating cybersecurity seamlessly into its design and operational parameters.

The objectives outlined in Clause 9 are pivotal for setting a solid cybersecurity foundation during the concept phase. These objectives include [6]:

- Defining the Item and Its Operational Environment: Clearly delineating the item, its operational environment, and their interactions within a cybersecurity context to ensure a comprehensive understanding of potential vulnerabilities and threats.
- Specifying Cybersecurity Goals and Claims: Establishing high-level cybersecurity goals and articulating cybersecurity claims to guide the development of robust and effective cybersecurity measures.
- Specifying the Cybersecurity Concept: Detailing the cybersecurity concept to achieve the defined cybersecurity goals, encompassing both the cybersecurity requirements for the item and the operational environment conditions.

A Cybersecurity Assurance Level (CAL) can be designated to define a set of assurance requirements, which describe the degree of rigor or effort necessary to ensure that asset protection is sufficient. It is important to note that the CAL does not dictate specific technical measures for cybersecurity. Instead, it serves to guide the cybersecurity engineering process by providing a standardized[6] framework for articulating cybersecurity assurance requirements across different organizations involved. A CAL can be established early in the development cycle, during the concept phase, based on parameters expected to remain consistent through to the end of support. These parameters typically relate to the criticality and nature of the assets involved. Additionally, the determination of a CAL can take into account the threat scenarios that have been identified[6].

Table 2. CAL determination example [6]

		Attack Vector			
		Physical	**Local**	**Adjacent**	**Network**
Impact	Negligible	---[1]	---[1]	---[1]	---[1]
	Moderate	CAL1	CAL1	CAL2	CAL3
	Major	CAL1	CAL2	CAL3	CAL4
	Severe	CAL2	CAL3	CAL4	CAL4

Clause 9 of ISO/SAE 21434 plays an instrumental role in embedding cybersecurity considerations into the early stages of automotive product development. By rigorously defining the item and its operational environment, setting clear cybersecurity goals, and developing a comprehensive cybersecurity concept, organizations can ensure that cybersecurity is an integral part of their product design from the outset. This proactive approach not only enhances the security posture of automotive products but also aligns

BUPT

with the industry's commitment to safeguarding vehicles against emerging cyber threats, thereby ensuring the safety and privacy of users in our increasingly connected world.

Clause 10: Product Development.
Clause 10 of ISO/SAE 21434 delves into the critical phase of product development within the automotive industry, focusing on the meticulous specification of cybersecurity requirements and the architectural design of automotive products. This stage is pivotal in translating the cybersecurity concept developed in earlier phases into concrete, actionable specifications and designs that can be implemented and verified against established cybersecurity goals. In addition to outlining the requirements and design, Clause 10 also covers the essential activities of integration and verification, ensuring that cybersecurity measures are not only designed but also effectively incorporated and validated within the product [6]. These activities are iteratively performed to refine and perfect cybersecurity controls until they meet the predetermined standards of the cybersecurity concept, confirming the product's compliance through rigorous verification processes.

An illustrative example provided in Figure 13 demonstrates how these product development activities align with a V-model-based workflow, a common framework in systems engineering. In this model, the specification of cybersecurity requirements and architectural design is positioned on the left arm of the V, while integration and verification activities are placed on the right arm. This representation underscores the iterative and interconnected nature of designing and validating cybersecurity measures, from the highest level of item abstraction down to components and sub-components. Furthermore, Clause 10 acknowledges the diversity of development methodologies, stating that alternative approaches, such as agile software development, are equally viable for implementing the standards outlined in this clause. The Cybersecurity Assurance Level (CAL) is introduced as a means to scale the depth and rigor of the activities and methods employed, ensuring flexibility and adaptability to various project scopes and requirements.

The objectives specified in Clause 10 aim to establish a robust framework for the development of secure automotive products. These objectives include [6]:

- Defining Cybersecurity Specifications: The foundational goal of this phase is to articulate precise cybersecurity specifications that align with the overarching cybersecurity concept and architectural design. This may entail the specification of new cybersecurity-related components not previously included in the initial design.
- Verifying Specification Conformance: It is crucial to verify that the defined cybersecurity specifications are in accordance with higher-level architectural abstractions, ensuring consistency and coherence across all levels of product design.
- Identifying Component Weaknesses: A proactive objective is to uncover any weaknesses within components that could potentially be exploited, laying the groundwork for subsequent vulnerability analysis and management as outlined in Clause 8.
- Providing Implementation and Integration Evidence: Lastly, the clause emphasizes the importance of providing tangible evidence that the implementation and

BUPT

integration of components, whether at the component or sub-component level, conform to the defined cybersecurity specifications. This objective ensures that the product not only meets theoretical security standards but also demonstrates practical compliance through its development and integration processes.

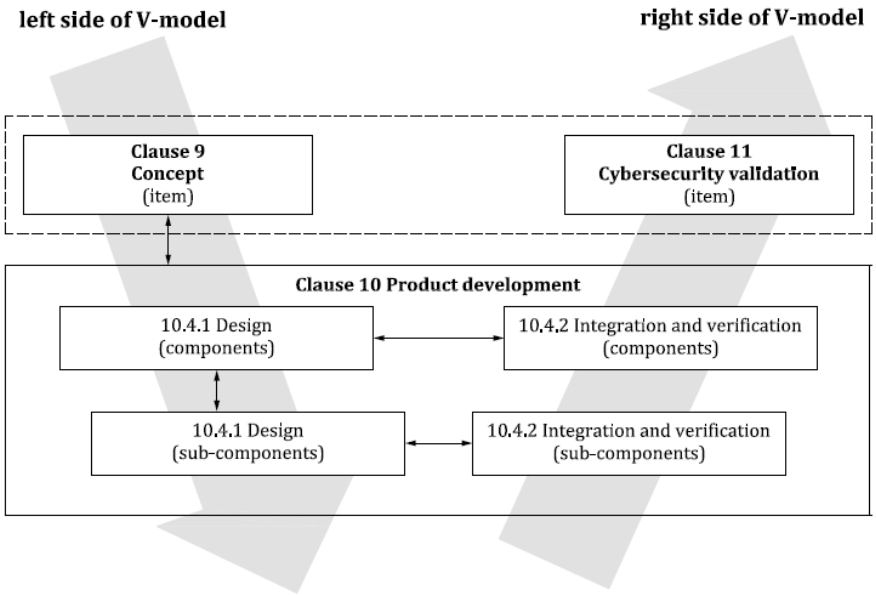


Fig. 13. V-Cycle development (ISO/SAE 21434, 2021)

Clause 10 of ISO/SAE 21434 encapsulates the essence of product development within the realm of automotive cybersecurity, providing a structured approach to defining, implementing, and verifying cybersecurity specifications [6]. By adhering to the objectives and guidelines outlined in this clause, organizations can navigate the complexities of product development, ensuring that their automotive products are designed with a strong cybersecurity posture from the ground up. This proactive and iterative approach to cybersecurity integration and verification is instrumental in safeguarding automotive systems against cyber threats, thereby protecting the safety and privacy of end-users in our increasingly connected automotive landscape.

Clause 11: Cybersecurity Validation.
Clause 11 of ISO/SAE 21434 zeroes in on the critical process of cybersecurity validation, specifically focusing on the vehicle level. This crucial phase is dedicated to ensuring that the cybersecurity measures designed and implemented in previous stages hold up under the scrutiny of real-world conditions and configurations intended for series

BUPT

production. It involves a comprehensive evaluation of the item, considering its integration within the operational environment of the vehicle. This holistic view ensures that the cybersecurity solutions are not only theoretically sound but also practically effective when deployed within the full context of the vehicle's operational environment.

The objectives laid out in Clause 11 serve as guiding principles for conducting thorough and effective cybersecurity validation, aiming to ensure that automotive products meet the highest standards of cybersecurity. These objectives include [6]:

- Validating Cybersecurity Goals and Claims: The primary aim is to rigorously validate the cybersecurity goals established in earlier phases, alongside the cybersecurity claims made. This involves assessing whether the cybersecurity measures in place effectively address the identified risks and threats, adhering to the cybersecurity goals set forth. The validation process scrutinizes the rationale behind risk retention or sharing strategies, ensuring they are justified and adequate.
- Confirming Achievement of Cybersecurity Goals: Beyond validating the goals and claims, it's imperative to confirm that the item indeed achieves the specified cybersecurity goals. This confirmation process evaluates the item's cybersecurity features and controls in action, ensuring they function as intended to protect the vehicle against cyber threats.
- Ensuring No Unreasonable Risks Remain: Lastly, this clause emphasizes the need to ensure that, following the implementation of cybersecurity measures, no unreasonable risks are left unaddressed. This objective underscores the importance of a thorough risk assessment and mitigation process, aiming for a level of cybersecurity where any remaining risks are at an acceptable level, ensuring the safety and security of the vehicle's operation.

The process of cybersecurity validation as described in Clause 11 is a vital step in the automotive product development lifecycle, providing a final checkpoint to ensure that all cybersecurity measures are not only in place but are effectively functioning within the vehicle's operational context. It necessitates a detailed examination of the item in its intended environment, testing and validating the cybersecurity features against real-world scenarios and threats. This validation process is integral to building confidence among manufacturers, stakeholders, and, ultimately, the end-users, ensuring that the vehicles they produce, sell, or drive are secure from cyber threats to the greatest extent possible. By methodically achieving the objectives of cybersecurity validation, organizations can demonstrate their commitment to cybersecurity, contributing to the overall safety and integrity of the automotive ecosystem.

Clause 11 of ISO/SAE 21434 underscores the significance of validating cybersecurity measures at the vehicle level, ensuring that the cybersecurity goals and claims are not only theoretically sound but also practically achievable. Through rigorous validation processes, organizations can confirm that their cybersecurity measures effectively mitigate risks, thereby safeguarding the vehicle against cyber threats throughout its operational life. This approach not only enhances the security posture of automotive products but also reinforces the industry's commitment to maintaining the highest standards of cybersecurity, ensuring the trust and safety of all users in the increasingly connected and digital automotive landscape.

BUPT

Clause 12: Production.
Clause 12 of ISO/SAE 21434 casts a spotlight on the production phase of automotive products, encompassing the manufacturing and assembly processes of items or components up to the vehicle level. This critical stage is where the theoretical designs and cybersecurity measures developed in previous stages come to life. The clause introduces the concept of a production control plan, a strategic blueprint designed to ensure that the cybersecurity requirements identified during the post-development phase are meticulously applied throughout the manufacturing and assembly processes. The primary aim is to maintain the integrity of cybersecurity measures and to safeguard against the introduction of any new vulnerabilities during production.

The objectives set forth in Clause 12 provide a focused framework for embedding cybersecurity considerations into the production environment. These objectives include [6]:

- Applying Cybersecurity Requirements for Post-Development: The first objective emphasizes the importance of carrying forward and applying the cybersecurity requirements established in the post-development phase into the production processes. This ensures that all cybersecurity measures, controls, and specifications are fully integrated and operationalized as items or components are manufactured and assembled. The continuity of cybersecurity requirements from development to production is crucial for maintaining a consistent cybersecurity posture.
- Preventing the Introduction of Vulnerabilities During Production: The second objective focuses on the critical goal of preventing new vulnerabilities from being introduced during the production phase. Given the complex nature of manufacturing and assembly processes, there are numerous opportunities for vulnerabilities to creep in, whether through software updates, configuration changes, or the integration of third-party components. Implementing stringent controls and checks as part of the production control plan is essential to mitigate these risks and ensure the cybersecurity integrity of the final product.

The creation and implementation of a production control plan are central to achieving the objectives of Clause 12. This plan outlines specific procedures, checks, and balances designed to ensure that cybersecurity requirements are systematically applied across all production activities; Monitor and control the manufacturing and assembly processes to identify and mitigate potential points of vulnerability introduction; Conduct regular audits and assessments of production processes to verify compliance with cybersecurity requirements and to identify areas for improvement.

Clause 12 of ISO/SAE 21434 highlights the pivotal role of the production phase in the automotive product lifecycle, underscoring the necessity of integrating cybersecurity measures into manufacturing and assembly processes. By establishing clear objectives and implementing a comprehensive production control plan, organizations can ensure that cybersecurity requirements are upheld and that new vulnerabilities are not introduced during production. This proactive approach to cybersecurity in production not only enhances the security of automotive products but also contributes to the overall resilience of the automotive industry against cyber threats, ensuring the safety and trust of end-users in our increasingly connected world.

BUPT

Clause 13: Operations and Maintenance.
Clause 13 of ISO/SAE 21434 turns the focus to the crucial stages of operations and maintenance, highlighting the ongoing efforts required to maintain and enhance cybersecurity for automotive products once they have been deployed in the field. This clause is pivotal in outlining the structured approach to managing cybersecurity incident responses and implementing updates for items or components after their initial development and production phases [6].

A key aspect of this clause is the detailed guidance on cybersecurity incident response and the process of issuing updates to address emerging threats, vulnerabilities, or to provide functional improvements to automotive products in use. Cybersecurity incident response is activated as part of an organization's broader vulnerability management strategy, indicating a systematic procedure for addressing identified vulnerabilities that could potentially impact the security of items or components in the field. Updates, on the other hand, represent changes or enhancements made to an item or component during its post-development phase. These can range from patches addressing specific security vulnerabilities to broader updates aimed at improving the functionality or safety of the product. Organizations may issue updates for a variety of reasons, with each update documented and managed as work products, integrating findings and requirements from across various clauses within the standard. It is important to note that modifications to items or components that are still in the concept, product development, or production phases fall under the purview of change management and are thus addressed separately from the operations and maintenance activities covered in this clause.

The objectives outlined in Clause 13 provide a clear roadmap for organizations to effectively manage cybersecurity aspects of automotive products throughout their operational life, ensuring continuous protection against cyber threats. These objectives include [6]:

- Determining and Implementing Remedial Actions for Cybersecurity Incidents: This involves promptly identifying the appropriate response to cybersecurity incidents and executing remedial actions to mitigate any potential impacts on the security of automotive products in the field.
- Maintaining Cybersecurity During and After Updates: Ensuring that the cybersecurity integrity of items or components is preserved both during and after the application of updates. This includes the responsibility to continually assess and enhance cybersecurity measures up until the end of cybersecurity support for the product, safeguarding against both known and emerging threats.

Clause 13 of ISO/SAE 21434 underscores the importance of diligent and proactive cybersecurity management during the operational life of automotive products. By establishing structured processes for incident response and updates, organizations can ensure that automotive products remain secure against evolving cyber threats, maintaining the trust and safety of end-users. This ongoing commitment to cybersecurity in the field reflects the broader objectives of ISO/SAE 21434 to protect automotive systems from

BUPT

cyber threats throughout their entire lifecycle, from initial concept through to decommissioning.

Clause 14: End of Cybersecurity Support and Decommissioning.
Clause 14 of ISO/SAE 21434 delves into the critical aspects of an automotive product's lifecycle: the end of cybersecurity support and the decommissioning process [6]. It's vital to understand that ending cybersecurity support for an item or component does not equate to its decommissioning. An item or component may continue to operate as intended in the field even after the cessation of cybersecurity support. This distinction underscores the unique cybersecurity implications associated with each phase—implications that require separate consideration within the framework of cybersecurity management.

Decommissioning, in particular, presents its own set of challenges, notably when it occurs outside the organization's purview, making it difficult, if not impossible, to enforce standard decommissioning procedures. Recognizing these challenges, ISO/SAE 21434 clarifies that the act of decommissioning, especially when it falls outside organizational control, is beyond the document's scope. However, the standards still emphasize the importance of considering the cybersecurity aspects of both end of support and decommissioning early in the product lifecycle, specifically during the concept and product development phases.

The objectives outlined in Clause 14 aim to provide a strategic approach to managing the transition as automotive products reach the end of their cybersecurity support or are decommissioned. These objectives are as follows[6]:

- Communicate the End of Cybersecurity Support: One of the primary objectives is to ensure clear and effective communication regarding the end of cybersecurity support for items and components. This involves informing all relevant stakeholders, including customers and users, of the timelines and implications associated with the cessation of support. Such communication is crucial for maintaining transparency and enabling users to make informed decisions regarding the continued use of the product.
- Enable Cybersecurity-Conscious Decommissioning: Additionally, the clause focuses on enabling the decommissioning of items and components with cybersecurity considerations in mind. This includes providing guidelines, where possible, for securely decommissioning products to prevent unauthorized access to or misuse of residual data and functionality. The goal is to mitigate cybersecurity risks associated with decommissioned products, ensuring that they do not become vectors for cyber threats even after they are no longer in active use.

Clause 14 of ISO/SAE 21434 addresses the nuanced stages of ending cybersecurity support and decommissioning, highlighting the distinct cybersecurity considerations each phase entails. By delineating clear objectives for communication and the enablement of secure decommissioning practices, this clause provides organizations with guidance on responsibly managing the transition phases of an automotive product's

BUPT

lifecycle. Recognizing and addressing the cybersecurity implications of these stages are essential steps in ensuring that products remain secure throughout their entire lifecycle, ultimately contributing to the broader goal of safeguarding the automotive ecosystem from cyber threats.

Clause 15: Threat Analysis and Risk Assessment Methods.
Lastly, Clause 15 of ISO/SAE 21434 delves into the crucial process of Threat Analysis and Risk Assessment (TARA), a systematic approach designed to evaluate the potential impact of cybersecurity threats on road users [6]. A central element of the recently published cybersecurity standard, ISO/SAE 21434:2021 ,is the execution of threat analysis and risk assessment (TARA) [44]. This clause outlines the methodology for conducting TARA, focusing on assessing how threats could affect the safety and security of those within the operational environment of road vehicles. The methods and work products associated with TARA are crafted from the perspective of affected road users, ensuring that assessments are grounded in the practical realities of vehicle operation and user interaction. The internal impact increases as there is a need to incorporate deep and dark web analysis into TARA frameworks [4].

The TARA process is modular, comprising several generic steps that can be systematically applied at any point in the lifecycle of an item or component. These steps include [6]:

- Asset Identification: This initial step involves identifying the critical assets within the vehicle's system, including their cybersecurity properties and potential damage scenarios.
- Threat Scenario Identification: Following asset identification, potential threat scenarios are outlined, considering how assets might be compromised.
- Impact Rating: Each identified damage scenario is then assessed for its potential impact, helping to prioritize threats based on their severity.
- Attack Path Analysis: This phase involves analyzing possible paths an attacker could take to exploit vulnerabilities and realize the threat scenario.
- Attack Feasibility Rating: The feasibility of each attack path is evaluated to determine how easily an attacker could exploit the path.
- Risk Value Determination: Combining the impact and feasibility ratings, the overall risk value of each threat scenario is calculated.
- Risk Treatment Decision: Based on the determined risk values, appropriate risk treatment options are selected to mitigate or manage the identified risks.

Given their generic nature, the work products resulting from these TARA steps are integrated into the work products produced by other clauses, ensuring a cohesive and comprehensive approach to cybersecurity across the vehicle's lifecycle.

The objectives outlined in Clause 15 aim to provide a structured framework for identifying and assessing cybersecurity threats throughout the lifecycle of automotive products. These objectives include [6]:

BUPT

- Asset and Damage Scenario Identification: Recognizing the critical assets within a system, their cybersecurity properties, and potential damage scenarios that could affect road users.
- Threat Scenario Identification: Outlining possible scenarios in which threats could materialize, impacting the identified assets.
- Impact Rating Determination: Assessing the severity of the impact that each damage scenario could have on road users and the vehicle's operation.
- Attack Path Identification: Analyzing potential paths through which threat scenarios could be executed by attackers.
- Attack Feasibility Evaluation: Evaluating the ease with which identified attack paths could be exploited by potential attackers.
- Risk Value Calculation: Determining the overall risk values associated with each threat scenario, combining impact and feasibility assessments.
- Risk Treatment Selection: Choosing suitable risk treatment strategies to mitigate or manage the risks identified through the TARA process.

Clause 15 of ISO/SAE 21434 establishes a robust framework for conducting Threat Analysis and Risk Assessment (TARA) within the automotive industry. By systematically identifying threats, assessing their potential impact, and evaluating the feasibility of attacks, organizations can determine the risk values associated with various threat scenarios and select appropriate risk treatment options. This comprehensive approach to TARA ensures that automotive products are designed, developed, and maintained with the safety and security of road users as a paramount concern, reinforcing the automotive industry's commitment to cybersecurity resilience.

4.5 Conclusion

The comprehensive exploration of ISO/SAE 21434 across its pivotal clauses from the conceptual foundations to the post-development stages of automotive product life underscores the standard's critical role in shaping the future of automotive cybersecurity. As vehicles become increasingly interconnected and reliant on sophisticated electrical and electronic (E/E) systems, the imperative for robust cybersecurity measures has never been more pronounced. ISO/SAE 21434 emerges not merely as a set of guidelines but as a beacon guiding the automotive industry through the complexities of securing modern vehicles against evolving cyber threats.

The standard meticulously outlines a lifecycle approach to cybersecurity, emphasizing the integration of security measures from the initial concept phase through to decommissioning. It addresses the dynamic nature of cybersecurity threats, offering a flexible yet structured framework for organizations to adapt their cybersecurity practices in response to new vulnerabilities and attack methodologies. Through the specification of cybersecurity requirements, the establishment of a Cybersecurity Management System (CSMS), and the rigorous process of Threat Analysis and Risk Assessment (TARA), ISO/SAE 21434 equips organizations with the tools to build and maintain vehicles that are not only technologically advanced but also resilient to cyber threats.

BUPT

Significantly, ISO/SAE 21434 recognizes the collaborative nature of the automotive supply chain, highlighting the importance of distributed cybersecurity activities and the management of interactions between customers and suppliers. It advocates for continuous cybersecurity activities, ensuring that vehicles remain secure throughout their operational life, with provisions for updates and incident responses to address emerging threats. As the automotive industry continues to evolve, driven by innovations in connectivity and automation, ISO/SAE 21434 will undoubtedly play a pivotal role in shaping secure automotive development. It fosters a culture of cybersecurity awareness and continuous improvement, ensuring that organizations remain vigilant and proactive in the face of an ever-changing cyber threat landscape.

In conclusion, ISO/SAE 21434 stands as a testament to the automotive industry's commitment to cybersecurity excellence. By adhering to its principles, organizations can ensure that automotive products are designed with a strong cybersecurity posture, safeguarding the safety and privacy of users in our increasingly connected world. The standard not only enhances the cybersecurity posture of automotive products but also reinforces the industry's broader commitment to maintaining the trust and confidence of consumers and stakeholders alike. As we navigate the challenges and opportunities of the digital age, ISO/SAE 21434 will continue to serve as a cornerstone of automotive cybersecurity, guiding the industry towards a safer, more secure future.

BUPT

5 ASPICE for Cybersecurity and its Integration

The integration of ASPICE for Cybersecurity [7] into the automotive development landscape represents a critical step in the automotive industry's approach towards cybersecurity. Initiated with the draft version's release in the first quarter of 2021 by the German Association of the Automotive Industry (VDA), this add-on module aims to extend the existing ASPICE process assessment model (PAM) version 3.1 by incorporating cybersecurity considerations. This move is an additional and strategic response to the increasingly complex cybersecurity challenges that OMS and their suppliers have navigate in light of strict regulatory requirements [52]. For projects related to cybersecurity, it is crucial to establish and uphold adequate practices to ensure a robust and secure product. This encompasses the entire engineering cycle, including the development, production, maintenance, and decommissioning phases, as well as organizational policies and project management practices [53]. A new element, "Automotive SPICE® for Cybersecurity," has been added to the framework. This not only provides guidelines for the technical implementation of such systems but also serves as a guide for Process Model implementers and assessors. It aids in evaluating the development process of cybersecurity components (System or Software) against the expectations of relevant standards, such as ISO/SAE 21434 [54]. With the release of ASPICE 4.0[55], a modified process assessment model (PAM) has been introduced to the automotive industry. Despite these updates, ASPICE for Cybersecurity has been kept as an add-on module, rather than being directly integrated into the PAM 4.0 process groups mapping. This decision underscores the specialized nature of cybersecurity within the automotive development lifecycle, recognizing the unique challenges and considerations it presents.

Regulation R155, issued by the United Nations Economic Commission for Europe (UNECE), exemplifies these requirements by mandating vehicle manufacturers to identify and manage cybersecurity risks within their supply chains. This regulation highlights the importance of a methodical and common approach towards identifying process-related product risks [22], a challenge that ASPICE for Cybersecurity seeks to address through its comprehensive nature. At the same time, the norm mandates that organizations implement a CSMS (Cybersecurity Management System). Additionally, in February 2021, the VDA AK13 released a new assessment model specifically designed for evaluating the cybersecurity of automotive development projects[56].

ASPICE for Cybersecurity extends the framework of Automotive SPICE by introducing a new Process Group and implementing subtle modifications to the already established Acquisition (ACQ) and Management (MAN) Process Groups [52]. This development ensures that every process under the ASPICE PAM is supported by specific outcomes, designated output work products, and foundational base practices, thereby reassuring the model's applicability and effectiveness in addressing cybersecurity concerns. While the evaluation of processes in Automotive SPICE for Cybersecurity follows a highly formalized procedure, assessing product quality requires technological considerations and the use of review checklists related to work products [57].

A clearly visible change brought to the Process Groups is the introduction of the Cybersecurity Engineering Process Group (SEC), which further introduces four specialized processes designed to enrich the automotive industry's cybersecurity defenses.

BUPT

These include Cybersecurity Requirements Elicitation (SEC.1), Cybersecurity Implementation (SEC.2), Risk Treatment Verification (SEC.3), and Risk Treatment Validation (SEC.4). Each process within the SEC Group is carefully crafted to align with overarching cybersecurity goals, facilitating a systematic framework to automotive cybersecurity risks[58]. Moreover, the Cybersecurity Risk Management (MAN.7) process, embedded within the Management Process Group (MAN), represents a strategic inclusion aimed at harmonizing these new cybersecurity measures with the management landscape. The Base Practices of MAN.7 pertain to the procedures involved in conducting and monitoring a Threat Analysis and Risk Assessment (TARA) [59]. This integration is crucial as the process aims to continuously identify, prioritize, and analyze risks of damage to relevant stakeholders as well as monitor and control the respective risk treatment options.

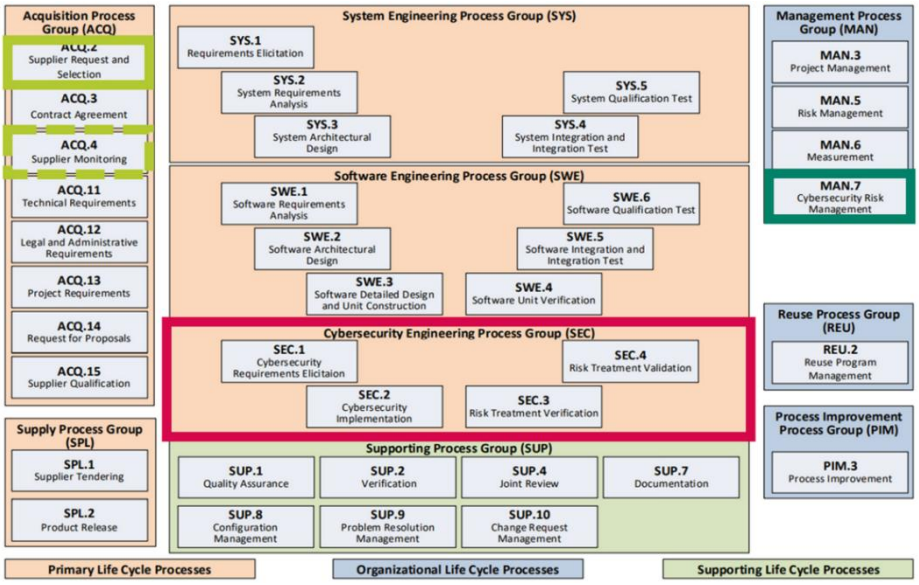


Fig. 14. Overview of ASPICE and ASPICE for Cybersecurity Process Reference Model (PRM) [52]

In addition to these process extensions, ASPICE for Cybersecurity also introduces new work products focused on cybersecurity, marking a significant step forward in the development of cybersecurity capabilities within the automotive sector. These work products, alongside the newly defined processes, are crucial components of the Process Reference and Assessment Model for Cybersecurity Engineering. The new assessment model includes RCs (Recommendations) and RLs (Rules) that assist in interpreting and rating the security-related base practices. It also incorporates work products and work product indicators and enhances existing work products with criteria relevant to cybersecurity [56]. This model expands the scope of Automotive SPICE to include

BUPT

cybersecurity-related processes, providing a robust framework for OEMs and Suppliers to effectively identify, assess, and mitigate cybersecurity risks.

This chapter's exploration into ASPICE for Cybersecurity highlights its vital role in advancing automotive cybersecurity measures. By aligning with UNECE regulation R155 and incorporating a detailed framework for cybersecurity risk management, ASPICE for Cybersecurity not only meets the regulatory demands but also sets a new standard for cybersecurity practices within the automotive industry. Through this integration, the automotive projects are better equipped to navigate the complexities of the digital landscape, ensuring the safety, privacy, and reliability of automotive systems in an increasingly connected world.

5.1 Connection to ISO/SAE 21434.

In the context of ISO/SAE 21434, the aim of conducting an Automotive SPICE assessment is to uncover systemic gaps within the primary lifecycle, management, and support processes [60]. Automotive SPICE PAM 3.1 alongside Automotive SPICE for Cybersecurity encompass areas of system and software engineering, with current previous not addressing indicators for mechanical and hardware engineering disciplines. However, the introduction of ASPICE PAM 4.0 has brought the Hardware Engineering Process Group in the Process Reference Model [55]. The published ASPICE for Cybersecurity does not encompass certain elements of ISO/SAE 21434, as they fall outside the scope of development project activities. Such elements are managed within the Automotive Cybersecurity Management System (ACSMS), covering domains like cybersecurity management, ongoing cybersecurity actions, and stages beyond development, all of which are evaluated during an ACSMS audit [7]. Under ASPICE, the VDA has outlined processes for Cybersecurity Engineering, Cybersecurity Risk Management, and Supplier Request and Selection. Incorporating these processes into the ASPICE assessment to meet the requirements of the ISO/SAE 21434 standard necessitates extra effort from both the assessors and the engineering team[61].

Support for project-dependent cybersecurity management includes:

- Cybersecurity responsibilities: GP 2.1.5 – Define responsibilities and authorities for performing the process.
- Cybersecurity planning: GP 2.1.2 – Plan the performance of the process to fulfill the identified objectives and MAN.3 Project Management.
- Tailoring of cybersecurity activities: PA 3.2 – Process deployment and GP 2.1.2 – Plan the performance of the process to fulfill the identified objectives.
- Reuse: included in make-buy reuse analysis SWE.2.BP6 – Evaluate alternative software architectures, SYS.3.BP5 – Evaluate alternative system architectures and REU.2 – Reuse Program Management.
- Component out of context: covered by Cybersecurity Engineering Process Group (SEC) based on assumptions regarding cybersecurity goals.
- Off-the-shelf component: ACQ.2 – Supplier Request and Selection and MAN.7 – Cybersecurity Risk Management.

BUPT

- Cybersecurity case: input provided by base practices “summarize and communicate results” of engineering processes.
- Cybersecurity assessment: ASPICE for Cybersecurity is a model for process capability determination. An in-depth technical analysis is not part of an ASPICE for Cybersecurity assessment.
- Release for post-development: SPL.2 – Product Release, SUP.8 –Configuration Management Process, and SUP.1 – Quality Assurance Process.

If cybersecurity processes are included in the scope of assessment, the duration of the assessment will be longer. Additionally, the cybersecurity processes establish dependencies with other PAM 3.1 processes [62]. The goal of conducting an Automotive SPICE® for Cybersecurity assessment is to either pinpoint product risks related to the process or to assess process improvements [63]. The evaluation of process capabilities for distributed cybersecurity efforts, from concept and product development to cybersecurity validation and risk assessment, is however covered by the add-on module. An assessment of ASPICE processes within the VDA Scope takes into account the interdependencies among practices within a single process, between different processes, and process attributes, and typically spans 6 days. The duration of the assessment is extended when cybersecurity processes are also included in the scope of the assessment [51]. However, in order to conduct an assessment using the Automotive SPICE for Cybersecurity PAM, it is essential to have an existing ASPICE assessment result for the VDA scope. If this is not available, an assessment must be conducted using both the Automotive SPICE® for Cybersecurity PAM and the Automotive SPICE® PAM for the VDA scope processes [64].

Structure and content.
In this subchapter, we highlight structure of process capability assessment, a fundamental methodology for evaluating the effectiveness and maturity of organizational processes. At the heart of this evaluation lies the process reference model, a structured grouping of process groups that provides a framework against which process capability can be measured [65]. This model is key in identifying the strengths and areas for improvement within an organization's processes, serving as a roadmap for continuous process improvement. We will then broaden our exploration to include the process assessment model, which extends the process reference model by introducing a systematic approach to assess and rate the capability of individual processes. This includes a detailed examination of process capability levels and process attributes. These elements collectively form a multi-dimensional framework that assesses processes not just on their performance, but also on their maturity and ability to achieve desired outcomes consistently. Process capability levels offer a hierarchical structure for grading the maturity of processes, ranging from Level 0 (Incomplete) to Level 5 (Optimizing), with each level providing a progressively more sophisticated process capability. In addition to these levels there are specific process attributes that provide measurable characteristics of process capability at each level, offering a deeper understanding of process performance and areas for improvement [66].

BUPT

By integrating these components—process assessment model, process capability levels and attributes, and the process capability assessment—we aim to provide a comprehensive overview of how organizations can effectively assess and enhance their process capabilities based on the ASPICE framework. This detailed exploration will particularly concentrate on the elements of the process model as it applies to the ASPICE for Cybersecurity PRM, with a focus on the Primary Lifecycle Processes and Organizational Lifecycle Processes categories, highlighting their significance in achieving cybersecurity objectives within the automotive sector [65].

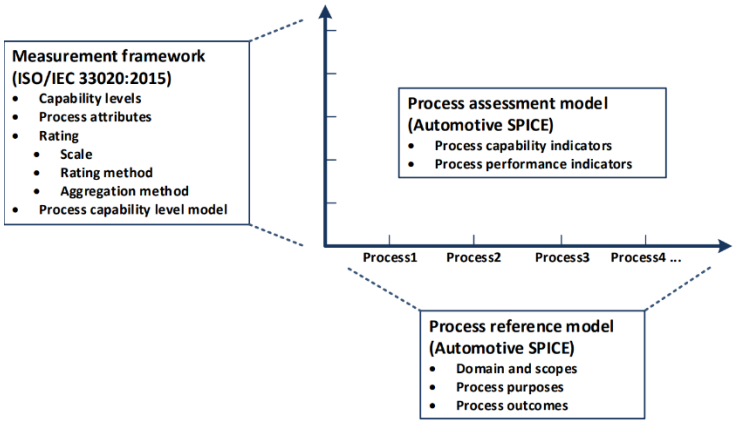


Fig. 15. Relationship overview within the Process Assessment Model [65]

Process Capability Assessment.
The methodology of assessing process capability through a process assessment model utilizes a dual-framework approach. This approach contains two primary dimensions: the first being the processes outlined in a process reference model (known as the process dimension), and the second involving capability levels, which are further broken down into process attributes (referred to as the capability dimension). The relationship between the two is presented in Figure 15. These process attributes offer quantifiable features that signify the capability of a process. Within this model, specific processes are chosen from the process reference model and are enhanced with indicators. These indicators facilitate the gathering of objective evidence, allowing an assessing party to determine and assign ratings to processes based on their level of capability within the capability dimension.

Process reference model.
Processes are categorized and further organized into groups based on the nature of the area they cover. This classification encompasses three main process categories: primary lifecycle processes, organizational lifecycle processes, and supporting lifecycle processes. Every process is characterized by a purpose statement, which outlines the

BUPT

distinct functional goals of the process within a specific context. In further chapters of this thesis, we will discuss the outcomes of the cybersecurity relevant processes. Accompanying each purpose statement is a set of specific outcomes, which depict the anticipated beneficial results stemming from the execution of the process. Going even further, each of these processes contains Base Practices that cover the expected process outcomes. In the context of the process dimension, both the Automotive SPICE and Automotive SPICE for Cybersecurity process reference models outline a compilation of processes, as depicted in Figure 14.

Process assessment model.
The process assessment model utilizes indicators to determine the presence or absence of both process outcomes and the achievements related to process attributes within the specific processes implemented in projects and organizational units. These indicators serve as a tool for assessors to gather the objective evidence needed to make informed capability judgments, rather than acting as a strict checklist that must be adhered to.

To evaluate whether process outcomes and achievements are evident, an assessment relies on objective evidence. Such evidence is derived from analyzing the work products and contents of repositories relevant to the processes under review, as well as from the statements given by individuals who manage or perform within these processes. This evidence is then aligned with the indicators defined in the Process Assessment Model (PAM) to establish a link to the intended process outcomes and attribute achievements. Indicators are categorized into two distinct types [65]:

- Process performance indicators are exclusive to Capability Level 1 and indicate the degree to which process outcomes are achieved.
- Process capability indicators span Capability Levels 2 to 5, measuring the achievement level of process attributes.

These indicators play a crucial role in verifying the execution of specific practices, evidenced through the collection of data during an assessment. This data may originate from assessing the work products associated with the assessed processes or from the statements of the individuals overseeing and executing these processes. The presence of base practices and work products highlights the execution of the processes they are linked to. Likewise, the presence of process capability indicators highlights the level of process capability.

Process capability levels and process attributes.
Process attributes represent characteristics of a process that can be assessed based on their level of achievement, offering an indication of the process's overall capability. These attributes are relevant across all types of processes. A capability level further consists of one or more process attributes that collectively contribute to a significant improvement in the ability to execute a process effectively. Each attribute focuses on a particular facet of the capability level, providing a structured approach to enhancing the capability of any process through gradual improvements. In this process assessment

BUPT

model, the evaluation of process capability relies on the nine process attributes (PA) as defined in ISO/IEC 33020 [67], which are detailed in Table 3.

Table 3. Process attributes [65]

Attribute ID	Process Attributes
Level 0	Incomplete process
Level 1	Performed process PA 1.1 Process performance process attribute
Level 2	Managed process PA 2.1 Performance management process attribute PA 2.2 Work product management process attribute
Level 3	Established process PA 3.1 Process definition process attribute PA 3.2 Process deployment process attribute
Level 4	Predictable process PA 4.1 Quantitative analysis process attribute PA 4.2 Quantitative control process attribute
Level 5	Innovating process PA 5.1 Process innovation process attribute PA 5.2 Process innovation implementation process attribute

5.2 Cybersecurity Relevant Process Groups and Processes

In this subchapter a comprehensive description of the structured approach to process definition as defined in the Process Assessment Model (PAM) is presented. The initial overview of the standard process description sets the stage for a deeper dive into the specific process groups and processes that are relevant for this cybersecurity approach. Following the general introduction to the process structure, the focus narrows to the cybersecurity-relevant process groups and processes. For each identified process group and process, we provide a detailed description, understanding their purpose, scope, and the role they play in the broader cybersecurity landscape.

Through a systematic presentation of each process, this chapter aims to equip readers with a thorough understanding of the essential elements of cybersecurity as defined within the PAM framework. The descriptions will not only highlight the objectives and outcomes associated with each process but will also highlight specific tasks, activities, and output work products that are vital towards achieving cybersecurity objectives. This comprehensive overview serves as a resource for professionals looking to deepen their understanding of cybersecurity processes.

General structure of a process.
The table below (Table 4) features a template of how each process from the process dimension is structured. Every table corresponding to a process within the process dimension showcases the process reference model alongside the essential process

BUPT

performance indicators that are crucial for establishing the process assessment model. These process performance indicators include base practices and output work products[65].

Table 4. Template of each process description [65]

PROCESS REFERENCE MODEL	**Process ID** **Process name** **Process purpose** **Process outcomes**	Each process within the Automotive SPICE process reference model is defined by its name, purpose, and expected outcomes. Furthermore, a process identifier is also supplied to distinguish each process uniquely.
PROCESS PERFORMANCE INDICATORS	**Base practices**	A collection of base practices associated with the process outlines the necessary tasks and activities required to achieve the process's purpose and realize its intended outcomes.
	Output work products	Several output work products are linked to each process.

Newly introduced process groups and processes.
In this subchapter, we will focus on the additions to the ASPICE for Cybersecurity Process Assessment Model (PAM), on the newly introduced process groups and processes that are seen as mandatory to assure cybersecurity compliance within the automotive sector. A significant addition is the Cybersecurity Engineering Process Group (SEC), a dedicated process group that highlights the importance of takin cybersecurity into consideration even from the starting point of engineering development. This process group is formed by four process groups: Cybersecurity Requirements Elicitation (SEC.1), Cybersecurity Implementation (SEC.2), Risk Treatment Verification (SEC.3) and Rist Treatment Validation (SEC.4) [58].

Furthermore, we will examine the process introduced as MAN.7, Cybersecurity Risk Management, which plays a crucial role in identifying, prioritizing and analyzing cybersecurity risks within a project. This process is essential for establishing a robust cybersecurity scope and practices that can respond to and manage the complex risk landscape of today's automotive industry.

Another crucial process to be discussed is ACQ.2, Supplier Request and Selection, which emphasizes the importance of cybersecurity considerations when selecting and engaging with suppliers. This process ensures that cybersecurity requirements are integral to the procurement and supply chain management, reflecting the interconnected nature of cybersecurity risks [58].

For each of these newly introduced processes, a concise analysis of the expected process outcomes will be provided, without going deeper into the Base Practice level. This analysis aims to offer insights into how these processes contribute to the overall

BUPT

cybersecurity approach of a development project, detailing the tasks and activities necessary to achieve the desired outcomes. By exploring these processes, this subchapter intends present the additions brought up with the introduction of the ASPICE for Cybersecurity PAM.

Cybersecurity Requirements Elicitation (SEC.1). The Cybersecurity Requirements Elicitation Process (SEC.1) serves as the initial step in the sequence of four processes within the Cybersecurity Engineering Process Group. The purpose of SEC.1 is to systematically identify cybersecurity goals and requirements by leveraging the outcomes of risk management processes [58]. This ensures that there is a direct correlation between the risk assessment findings, the defined cybersecurity goals, and the cybersecurity requirements. Such alignment is essential for creating a robust cybersecurity approach that is both responsive and resilient to the evolving threat landscape. Successful execution of the SEC.1 process leads to several key outcomes [7]:

1. Cybersecurity Goals Defined: Initiating the sequence of SEC processes, this process defines clear cybersecurity goals, setting the direction for all cybersecurity engineering efforts and serving as a starting point in measuring cybersecurity effectiveness.
2. Cybersecurity Requirements Derived: Building on the defined goals, cybersecurity requirements are systematically derived, ensuring that each requirement is purposefully developed to address specific cybersecurity objectives.
3. Consistency and Traceability Established: A critical outcome of SEC.1 is the establishment of consistency and bidirectional traceability between the cybersecurity requirements and goals, and between the goals and the threat scenarios. This traceability is crucial for maintaining a clear and traceable connection between identified risks and the measures put in place to mitigate them.
4. Cybersecurity Requirements Agreed and Communicated: The final defined outcome of this defined process is focusing on the agreement and communication of cybersecurity requirements to all stakeholders involved. This ensures a unified understanding, approach and agreement to implementing the cybersecurity measures across stakeholders.

By setting a comprehensive and strategic approach towards cybersecurity, the Cybersecurity Requirements Elicitation Process (SEC.1) is crucial in the journey towards adopting a cybersecurity posture within the development project. As the first step in the Cybersecurity Engineering Process Group, it paves the way for the following processes, SEC.2, SEC.3, and SEC.4. Therefore, it ensures that every step taken towards enhancing cybersecurity is informed, targeted, and aligned with the related objectives of risk management. Ultimately, SEC.1 not only initiates the crucial task of cybersecurity goal setting and requirement definition but also supports a culture of continuous improvement in facing cybersecurity challenges.

Cybersecurity Implementation (SEC.2). The Cybersecurity Implementation Process (SEC.2) is further focusing on to the practical application of cybersecurity by ensuring that the previously defined cybersecurity requirements are meticulously allocated to both system and software components, and that these requirements are effectively

BUPT

implemented [7]. It marks a critical step in transitioning from the theoretical aspect established in SEC.1 to tangible cybersecurity measures integrated into the system and software architecture. Successful execution of the SEC.2 process leads to a series of essential outcomes[58]:

1. Refinement of Architectural Design: The process begins with the refinement of the architectural design, ensuring it can effectively address the cybersecurity requirements.
2. Allocation of Cybersecurity Requirements: Cybersecurity requirements are systematically allocated to specific elements of the architectural design, ensuring that each component addresses its designated cybersecurity needs.
3. Selection of Appropriate Cybersecurity Controls: Based on the allocated requirements, appropriate cybersecurity controls are selected to mitigate identified risks and vulnerabilities.
4. Analysis of Vulnerabilities: This step involves an analysis of potential vulnerabilities within the system and software, allowing for proactive measures to be taken against cybersecurity threats.
5. Refinement of Detailed Design: The detailed design is now refined based on the architectural, ensuring a cohesive and secure implementation.
6. Development of Software Units: Software units are developed with cybersecurity in mind, using appropriate modeling and/or programming languages.
7. Establishment of Consistency and Traceability: A crucial outcome is the establishment of consistency and bidirectional traceability between the architectural and detailed designs, ensuring that cybersecurity measures are consistently applied throughout the development process.
8. Agreement and Communication of Cybersecurity Risk Treatment Implementation: Finally, the cybersecurity risk treatment implementation is agreed upon by all stakeholders and communicated effectively to all parties affected, ensuring a collective understanding and commitment.

The Cybersecurity Implementation Process (SEC.2) thus ensures that cybersecurity is not merely a theoretical concept but is actively and effectively integrated into the development and design of automotive projects. Therefore, SEC.2 not only advances the application of cybersecurity measures but also reinforces the overall security of automotive projects against emerging threats and vulnerabilities.

Risk Treatment Verification (SEC.3). The SEC.3 Process, or Risk Treatment Verification, focuses on validating that the cybersecurity implementations across system and software designs adhere to defined cybersecurity requirements and both the refined architectural and detailed designs [58]. This verification process is integral to confirming the effectiveness of cybersecurity measures. The following outcomes are expected for achieving the process [7]:

BUPT

1. Development and Implementation of a Verification Strategy: The initial step of SEC.3 involves crafting and executing a detailed risk treatment verification and integration strategy, which includes a regression strategy.
2. Specification for Risk Treatment Verification: Following the strategy development, a specific verification specification, including test cases, is created. This specification is tailored to demonstrate compliance with cybersecurity requirements and the coherence of the design implementations with the refined architectural and detailed design, serving as a foundation for evidence-based verification.
3. Execution of Verification Activities: Verification activities are conducted as it was defined in the strategy to ensure that identified work products meet their specified requirements. This includes testing the implementation of the design and the integration of components as defined in the risk treatment verification specification, thereby confirming compliance with the established criteria.
4. Establishing Bidirectional Traceability: Another outcome of this process is the establishment of comprehensive bidirectional traceability, which includes:

- Linking cybersecurity requirements with the risk treatment verification specification and its test cases,
- Linking the refined architectural design, detailed design, and software units to the risk treatment verification specification,
- Linking the test cases from the risk treatment verification specification with the verification results, ensuring a clear and traceability from requirements to verification outcomes.

5. Ensuring Consistency: SEC.3 also ensures consistency between the cybersecurity requirements and the risk treatment verification specification, including its test cases, and between the refined architectural and detailed designs and the verification specification. This consistency is key to maintaining alignment across all aspects of the cybersecurity approach.
6. Summarization and Communication of Results: The process concludes with the summarization of the verification results, which are then communicated to all affected parties. This final step guarantees that all stakeholders are kept informed of the outcomes, fostering transparency and enabling informed decisions based on the verification findings.

Through the SEC.3 Process, the emphasis is on a methodical and transparent approach to the verification of cybersecurity implementations, affirming that all cybersecurity measures are not only properly implemented but are effective and compliant with the established cybersecurity approach.

Risk Treatment Validation (SEC.4). The SEC.4 Process, known as Risk Treatment Validation, is the final component of the Cybersecurity Engineering Process Group, designed to ensure that the integrated system meets its cybersecurity objectives effectively. This process plays an essential role as it is verifying that the implemented measures not only adhere to the specified requirements but also achieve the overarching cybersecurity goals defined at the beginning of the project[7].

BUPT

1. Development and Agreement of a Validation Strategy: The process begins with the formulation of a comprehensive risk treatment validation strategy. This strategy is collaboratively developed, implemented, and agreed upon with all relevant stakeholders, ensuring that it is robust enough to demonstrate that the system's implementation aligns with the intended cybersecurity goals. The strategy must be maintained throughout the project lifecycle to adapt to any changes or threats.
2. Validation of Design and Integration: A key outcome of the process is the actual validation of the system's design and the integration of its components. This step is carried out in accordance with the established risk treatment validation strategy, ensuring that every component and system design aspect contributes to achieving the cybersecurity goals.
3. Documentation of Validation Activities: All validation activities undertaken as part of this process are documented and the results meticulously recorded. This documentation serves as detailed evidence of the validation efforts and outcomes, providing a proof of compliance and goal achievement.
4. Establishing Bidirectional Traceability: SEC.4 also emphasizes the importance of establishing bidirectional traceability among the cybersecurity goals, the risk treatment validation specification, and the validation results. This traceability ensures a clear and accountable link between the cybersecurity objectives and the outcomes of the validation activities.
5. Ensuring Consistency: Ensuring consistency between the cybersecurity goals and the risk treatment validation specification is also a crucial outcome of this process.
6. Summarization and Communication of Results: Summarization and communication of the validation results to all affected parties. This step is vital for transparency, providing stakeholders with a clear understanding of the validation outcomes and the effectiveness of the cybersecurity measures implemented.

The SEC.4 - Risk Treatment Validation process is assuring that the cybersecurity measures implemented throughout the project development are not only compliant with the specified requirements but also successful in achieving the intended cybersecurity goals. Through rigorous validation, documentation, and communication, the Risk Treatment Validation process ensures that all stakeholders are confident in the cybersecurity posture of the integrated system.

Cybersecurity Risk Management (MAN.7). Transitioning from the specific Cybersecurity Engineering Process Group, we now turn our attention to the broader strategic process group entitled Management Process Group. This shift now introduces MAN.7 - Cybersecurity Risk Management, a crucial addition aimed at enhancing project oversight in cybersecurity. MAN.7 focuses on identifying, prioritizing, analyzing, and managing cybersecurity risks [7]. This change highlights the importance of integrating risk management practices with technical efforts to ensure comprehensive cybersecurity resilience. The following outcomes are expected[7]:

1. Scope Determination: The process starts with defining the scope of cybersecurity risk management, encompassing projects and assets with cybersecurity properties,

BUPT

potential damage scenarios, relevant stakeholders, impact categories, and associated product phases. The scope is determined in relation to the operational environment and organizational risk management policies, ensuring a comprehensive coverage of all potential risk areas.
2. Implementation of Risk Management Practices: This involves defining and implementing a set of appropriate practices for managing cybersecurity risks within the defined scope. These practices include identifying potential risks, conducting risk analysis, evaluating risks, determining risks and making decisions on risk treatment.
3. Identification of Potential Risks: This outcome focuses on the initial and ongoing identification of potential risks within the project scope, actively searching for risk factors.
4. Prioritization of Risks: Potential risks are prioritized based on their potential damage and impact on relevant categories and stakeholders, ensuring that resources are allocated efficiently to address the most significant threats first.
5. Risk Analysis and Evaluation: Potential risks are analyzed to assess their probability, consequence, and severity. This analysis is crucial for understanding the nature of the risks and for planning appropriate mitigation strategies.
6. Definition of Risk Treatment Options: For each identified risk or group of risks, specific treatment options are defined. These options include accepting, reducing, avoiding, or transferring the risks, providing a strategic approach to managing identified threats.
7. Risk Monitoring: Continuous monitoring of each risk or set of risks is conducted to detect any changes in risk status and to evaluate the effectiveness of treatment activities, ensuring that risk management efforts are current and effective.
8. Corrective Actions: Upon identification of relevant changes to risks, appropriate corrective actions are taken to address these changes, maintaining the integrity of the cybersecurity risk management strategy.

Acquisition Process Group ACQ. Transitioning now to the Acquisition Process Group a new process tailored for the cybersecurity domain, Supplier Request and Selection (ACQ.2) was introduced. This new process emerges as a specific approach to supplier management within ASPICE for Cybersecurity, designed to ensure efficient and secure acquisition of cybersecurity-relevant services and products. The creation of ACQ.2 is a strategic decision to consolidate elements from ACQ.3, ACQ.14, and ACQ.15, focusing on the execution of requests for quotation (RFQ) for cybersecurity services and products—a practice already ingrained and standardized within the automotive industry's purchasing departments [58]. Notably, while these elements were part of ASPICE PAM 3.1, they have been excluded from ASPICE PAM 4.0, signifying a refined focus in the latest model iteration.

The ACQ.2 process is dedicated to optimizing supplier management with an emphasis on cybersecurity, addressing the critical need for robust cybersecurity measures in supplier selections and engagements. This process aligns with the industry's standardized procedures for requesting quotations, ensuring that suppliers of cybersecurity services

BUPT

and products are comprehensively evaluated. The following outcomes have been defined [7]:

1. Establishment of Evaluation Criteria: The foundation of ACQ.2 lies in establishing clear and specific evaluation criteria for suppliers, tailored to assess their capability to meet cybersecurity requirements. This ensures a standardized and objective approach towards evaluating potential suppliers.
2. Supplier Evaluation: Following the established criteria, suppliers are rigorously evaluated to determine their suitability and capability in providing the required cybersecurity services and products.
3. Issuance of Request for Quotation: A formal request for quotation is issued to the shortlisted supplier candidates. This step is a standardized procedure that invites suppliers to submit their proposals, detailing how they intend to meet the cybersecurity service or product requirements.
4. Agreement on Contracts and Plans: The final defined outcome involves reaching agreements on contracts, actions, and risk mitigation plans with the selected supplier, based on the evaluation results. This ensures that the supplier engagement is assured on a clear understanding of the terms, expectations, and cybersecurity objectives, with contractual agreements reflecting the consideration of evaluation outcomes.

Therefore, the ACQ.2 process marks a significant addition to ASPICE for Cybersecurity, emphasizing the critical role of secure and strategic supplier management in the broader cybersecurity ecosystem. By focusing on the efficient execution of requests for quotation and the rigorous evaluation of suppliers against defined cybersecurity criteria, ACQ.2 enhances the cybersecurity posture of automotive industry projects and products. The ACQ.4 process entitled Supplier Monitoring is only relevant to the ASPICE for Cybersecurity due to its already defined content [7].

5.3 Conclusion.

In conclusion, this chapter has explored the ASPICE for Cybersecurity add-on module, highlighting its significance and the strategic integration of newly added processes and process groups. Through a detailed examination, we've highlighted the essence of each process, from the Cybersecurity Engineering Process Group to the Management and Acquisition Process Groups, unveiling how they collectively improve the cybersecurity framework within the automotive industry. By focusing on the specific purposes and outcomes of processes such as Cybersecurity Requirements Elicitation (SEC.1), Cybersecurity Implementation (SEC.2), Risk Treatment Verification (SEC.3), Risk Treatment Validation (SEC.4), Cybersecurity Risk Management (MAN.7), and Supplier Request and Selection (ACQ.2), this chapter has provided a thorough understanding of the of cybersecurity compliance. Each process, with its defined purpose and outcomes, contributes to a layered defense strategy, ensuring that cybersecurity is a foundational element of development processes. A significant advantage of implementing ASPICE for Cybersecurity is that it enables OEMs to evaluate the capabilities of their suppliers and their systems [68].

BUPT

6 Conclusion of Theoretical Aspects

The domain of Cybersecurity Management in the automotive industry, while rapidly gaining prominence, still faces significant challenges due to its relative novelty. This topic was first formally recognized with the introduction of the UNECE WP.29 regulations, specifically R155 and R156. These regulations, which set standards for Cybersecurity Management and Software Update Management Systems, respectively, will not begin enforcement until the second half of 2024. These regulations were implemented at the start of 2021, with two critical deadlines established: from July 2022, the requirements are to be mandatory for all new vehicle types seeking type approval within UNECE member and from July 2024, these requirements will extend to all vehicles [32]. As a result, the breadth of academic articles and practical research on this subject is currently limited. The body of industry experience and case studies, which are crucial for developing a deep understanding and refining compliance practices, is expected to grow and become extensively available post-enforcement. This upcoming period will likely herald a significant expansion in published research and detailed case studies, providing valuable insights and guidance for integrating cybersecurity measures within the automotive industry.

In this comprehensive analysis of cybersecurity standards compliance in the automotive industry, we have delved deep into the evolving landscape of digital threats and the necessary countermeasures required to maintain security and reliability in automotive systems.

6.1 Theoretical Aspects Summary

This part has established a theoretical foundation for integrating multiple cybersecurity standards, particularly highlighting the synergy between ISO/SAE 21434, ASPICE for Cybersecurity, and UNECE WP.29 regulations, namely R155 and R156. It began with an exploration of the evolution of cybersecurity threats within the automotive industry. The automotive industry is experiencing a significant shift as it moves from being centered around hardware to increasingly focusing on software-driven vehicles[9]. Therefore, the evolving threat landscape demands continuous enhancement and adaptation of cybersecurity measures [4], as discussed in the opening chapters, where the growing sophistication of cyber threats was matched with an equally sophisticated set of defensive protocols outlined in international standards. We further analyzed the pivotal role of international regulations, such as UNECE WP.29, and how these create a regulatory framework that complements technical standards like ISO/SAE 21434 and ASPICE for Cybersecurity. This interconnection not only enhances compliance but also ensures a holistic security approach that addresses both current and emerging threats. To address emerging cyber threats, automotive OEMs along with Tier-1 and Tier-2 suppliers are adopting a unified approach by implementing UNECE's WP.29 R155 and R156 regulations, as well as the ISO/SAE 21434 standard[5]. The discussion on the integration of these standards provided insights into the complexities and challenges of achieving a seamless alignment within automotive software development processes. In subsequent chapters, the structural intricacies and

BUPT

implementation challenges of ISO/SAE 21434 and ASPICE for Cybersecurity were scrutinized. This analysis emphasized the necessity for a structured approach to cybersecurity, one that is capable of addressing specific risks associated with automotive software engineering. The standards themselves were revealed not as mere guidelines but as essential frameworks that fortify the entire lifecycle of automotive development.

6.2 Following Practical Application Report

As this part concludes its theoretical discourse on cybersecurity in the automotive industry, it sets the stage for the subsequent practical exploration, particularly through the implementation of a compliance matrix. This matrix is designed to facilitate the alignment of ISO/SAE 21434 and ASPICE for Cybersecurity standards, addressing the pressing need for a coherent strategy to manage cybersecurity risks effectively across the automotive supply chain. The development of the compliance matrix marks a critical transition from theoretical analysis to practical application, embodying the core of the thesis. It is conceived as a tool to significantly enhance the efficiency of the compliance process by systematically aligning the detailed requirements of both standards. This alignment is not just about compliance but also about fostering a holistic approach to cybersecurity that incorporates the entire automotive ecosystem. The matrix aims to reduce the redundancies and complexities that often arise when attempting to meet diverse regulatory demands, thereby minimizing the resources needed for audits, assessments, and ongoing compliance management in terms of time, costs, and manpower.

By bridging theoretical concepts with practical applications, the compliance matrix not only seeks to streamline the process of adhering to complex standards but also aims to contribute substantively to the field of automotive cybersecurity. This approach underscores the importance of integrating comprehensive cybersecurity measures that are robust, scalable, and adaptable to the evolving landscape of cyber threats and technological advancements in the automotive industry. This foundation and the insights gained from forthcoming practical evaluations will provide a robust framework for Tier 1 suppliers and other stakeholders striving to navigate the intricate web of cybersecurity threats and compliance obligations.

BUPT

B. Practical Aspects

1 Introduction

In the rapidly evolving digital landscape, the automotive industry is undergoing a significant transformation characterized by the integration of advanced technologies such as connectivity, automation, and electrification. The expanding interconnectivity of essential systems, such as those used in transportation, is prompting the creation of new standards that aim to establish a foundational framework for addressing cybersecurity alongside safety considerations [69]. Vehicles are no longer mere mechanical constructs; they have become sophisticated cyber-physical systems interconnected with external networks, other vehicles, and infrastructure. This heightened level of connectivity offers numerous benefits, including enhanced safety features, improved user experiences, and access to real-time data. However, it also introduces a plethora of cybersecurity threats that can compromise the safety, privacy, and functionality of both vehicles and their users. Cybersecurity has thus emerged as a paramount concern in the automotive sector. High-profile incidents of vehicle hacking have demonstrated the potential risks associated with inadequate cybersecurity measures, ranging from unauthorized access and data breaches to the manipulation of vehicle controls. These incidents underscore the urgent need for robust cybersecurity practices that safeguard automotive systems against malicious attacks and vulnerabilities throughout the vehicle lifecycle.

To address these challenges, several industry standards and regulations have been developed, providing frameworks for implementing effective cybersecurity management. Among these, ISO/SAE 21434 "Road Vehicles—Cybersecurity Engineering" [6] and Automotive SPICE (ASPICE) for Cybersecurity [7]are pivotal standards guiding organizations in establishing systematic cybersecurity processes. In contemporary practice, the development of software systems must adhere to various standards, which frequently share common requirements or at the very least offer considerable opportunities for synergy [70]. ISO/SAE 21434 offers a comprehensive approach to cybersecurity risk management tailored specifically for the automotive sector, covering the entire product lifecycle from conception to decommissioning. ASPICE, on the other hand, provides a process assessment model that evaluates the maturity of software development processes, including those related to cybersecurity. Current automotive development frameworks are increasingly integrating comprehensive cybersecurity processes mandated by new standards [71]. There is a need to enhance the optimization of these processes and improve their integration across the entire development cycle [72].

In the part, a thorough theoretical exploration of these standards, delving into their structures, challenges, and implementation nuances was presented. It also discussed the interplay between ISO/SAE 21434, ASPICE for Cybersecurity, and UNECE WP.29 regulations, specifically R155 (Cybersecurity and Cybersecurity Management) and R156 (Software Update and Software Update Management Systems). The development of regulation UNECE R155 and standard ISO/SAE 21434 began when it became clear that cybersecurity needed to be implemented in road vehicles to maintain user safety and safeguard personal data [73]. This theoretical foundation set the stage for the

BUPT

strategic integration of multiple cybersecurity standards within automotive projects. Building upon the insights from the theoretical analysis, the current part focuses on the practical implementation of a compliance matrix designed to align the requirements of ISO/SAE 21434 with those of the ASPICE for Cybersecurity framework. The compliance matrix serves as a comprehensive tool that systematically maps and rationalizes the interrelations between these two critical standards, providing clear reasoning for each mapping to facilitate understanding and implementation. To enhance the usability and accessibility of the compliance matrix, a web application has been developed and is introduced in this part. This application is specifically designed to improve user-friendliness, allowing stakeholders to navigate the compliance matrix more efficiently. It offers interactive features such as intuitive search functions, dynamic cross-referencing, and user-friendly interfaces that simplify the process of ensuring compliance.

The practical application of the compliance matrix, coupled with the web application, aims to significantly streamline the compliance process within automotive projects. By reducing the resources required for audits and assessments—namely time, costs, and manpower—the tools developed contribute to more efficient and effective cybersecurity management. This approach demonstrates the feasibility and benefits of aligning multiple cybersecurity standards, addressing the challenges organizations often face when complying with different requirements due to variations in structure, terminology, and documentation expectations. By bridging the gap between theoretical frameworks and practical implementation, this work provides valuable insights into the strategic integration of multiple cybersecurity standards within automotive software development projects. It illustrates how the compliance matrix, and the web application can serve as practical solutions to the complexities of standards compliance, enabling organizations to adopt a unified approach to cybersecurity management.

Ultimately, this part contributes to enhancing cybersecurity practices in the automotive industry, promoting the development of safer and more secure automotive systems. The tools and methodologies presented aim to support organizations in navigating the complexities of standards compliance, ensuring that they can effectively protect their products and users in an increasingly connected world.

BUPT

2 Compliance Matrix Development

In the realm of automotive cybersecurity, ensuring compliance with multiple industry standards is a complex yet essential task. ISO/SAE 21434 [6]and ASPICE for Cybersecurity [7]are two pivotal standards that provide comprehensive frameworks for cybersecurity engineering and process assessment within the automotive industry. Given the intricate nature of these standards and the necessity for organizations to adhere to both, developing a tool that systematically aligns their requirements becomes imperative. This chapter details the development of a compliance matrix designed to map the requirements of ISO/SAE 21434 to the base practices of ASPICE for Cybersecurity. The objective is to create a structured approach that facilitates understanding, implementation, and concurrent compliance with both standards.

The primary purpose of the compliance matrix is to provide a clear and systematic mapping between the requirements outlined in ISO/SAE 21434 and the base practices defined in ASPICE for Cybersecurity. By doing so, the matrix serves several key objectives. It streamlines compliance efforts by identifying overlaps and correspondences between the two standards, allowing organizations to reduce duplication of efforts and save time and resources during audits and assessments. It enhances clarity and understanding by providing detailed rationalizations for each mapping, aiding practitioners in comprehending how requirements from one standard relate to practices in the other. Additionally, it facilitates integrated implementation, enabling organizations to develop processes and documentation that satisfy both standards simultaneously, and supports continuous improvement by serving as a reference for ongoing process enhancement.

The development of the compliance matrix began with the creation of a comprehensive Excel table. Excel was chosen for its versatility and ability to handle large datasets with complex relationships. The initial steps involved identifying all relevant requirements from ISO/SAE 21434 and listing them along one axis of the table. This included specific clauses, mandates, recommendations, and notes critical for compliance. Along the other axis, the base practices from ASPICE for Cybersecurity were enumerated, encompassing essential processes and activities that organizations must implement to achieve various capability levels.

The core of the matrix involved mapping the relationships between the ISO requirements and the ASPICE base practices. Recognizing that the relationships could be one-to-one, one-to-many, many-to-one, or many-to-many, the mapping required a detailed analysis to ensure accuracy and completeness. For each mapping, a rationalization was provided to explain the reasoning behind the relationship. This involved analyzing the content, carefully reviewing the text of the requirements and practices to understand their intent, scope, and application; identifying common themes where the standards address similar concepts, such as risk assessment, threat analysis, or verification activities; and explaining the linkages by articulating how the implementation of an ASPICE practice satisfies the corresponding ISO requirement or vice versa. These rationalizations are crucial for practitioners to understand how compliance with one standard contributes to compliance with the other.

The development of the compliance matrix presented several challenges. Differences in terminology between the two standards sometimes led to potential

BUPT

misunderstandings. Identifying these equivalencies required careful analysis. Variations in structure also posed difficulties, as ISO/SAE 21434 is requirement-centric while ASPICE focuses on process capability and assessment, necessitating a flexible approach in mapping. Additionally, overlapping and diverging requirements meant that some ISO requirements overlapped with multiple ASPICE practices, while others did not have a direct counterpart. Addressing these overlaps and gaps required thoughtful consideration.

After the initial mapping, the compliance matrix underwent several iterations of refinement. Subject matter experts in automotive cybersecurity were consulted to review the mappings and rationalizations, and their feedback helped identify any inaccuracies or areas needing clarification. The matrix was tested in real-world scenarios to assess its practicality and effectiveness, involving applying the matrix to existing projects to evaluate how well it facilitated compliance efforts. Based on the reviews and testing, adjustments were made to improve the accuracy and utility of the compliance matrix.

Recognizing the limitations of an Excel-based tool, particularly in terms of scalability and user experience, the decision was made to transition the compliance matrix into a web application. This move offered several advantages. A web application allows users to access the compliance matrix from any location and device with internet connectivity, facilitating collaboration among team members who may be geographically dispersed. It offers a more intuitive and interactive interface compared to Excel, with features such as search functions, filtering options, and hyperlinks enhancing the user experience. Updates to the compliance matrix can be implemented centrally and reflected in real-time for all users, ensuring that the most current information is always available. Moreover, the web application can be designed to integrate with other project management and documentation tools, further streamlining compliance processes.

The development of the compliance matrix and its transition into a web application have significant implications for compliance efforts. Organizations can save time and resources by leveraging the matrix to address multiple standards concurrently. The web application simplifies navigation and information retrieval, reducing the effort required to understand and implement requirements. With a centralized tool, organizations can ensure that compliance practices are applied consistently across different projects and teams, reducing the risk of gaps or inconsistencies. The detailed rationalizations help practitioners comprehend the interrelations between standards, improving their ability to implement processes effectively. During audits or assessments, the compliance matrix serves as evidence of how requirements are met, and the web application allows for easy presentation and review of compliance information.

2.1 Selection of ISO 21434 Clauses for Mapping

In developing the compliance matrix between ISO/SAE 21434 and ASPICE for Cybersecurity, only specific clauses of ISO 21434 have been chosen for mapping. The focus is on the product development aspects, deliberately setting aside organizational elements. This approach ensures a stable and suitable mapping to ASPICE for Cybersecurity, concentrating on technical processes that are directly relevant to practitioners involved in automotive cybersecurity engineering. The clauses selected for mapping are:

BUPT

Clause 7: Distributed Cybersecurity Activities.
Clause 7 includes requirements for assigning responsibilities for cybersecurity activities between the customer and the supplier [6]. It addresses the coordination and management of cybersecurity tasks across different organizational units and external parties involved in the development process. Including this clause in the mapping ensures that roles and obligations concerning cybersecurity are clearly defined and communicated among all stakeholders. This clarity is essential for integrating cybersecurity measures effectively throughout the supply chain and development lifecycle.

Clause 9: Concept.
Clause 9 encompasses activities that determine cybersecurity risks, cybersecurity goals, and cybersecurity requirements for an item [6]. It involves the initial identification and assessment of potential threats, leading to the establishment of objectives and specifications that guide subsequent development phases. Focusing on this clause ensures that cybersecurity considerations are integrated from the earliest stages of product development, aligning with ASPICE practices related to requirements elicitation and risk management.

Clause 10: Product Development.
Clause 10 includes activities that define the cybersecurity specifications and implement and verify cybersecurity requirements [6]. It covers the detailed design, implementation, and testing processes necessary to realize the cybersecurity goals established during the concept phase. By mapping this clause, the core development activities are aligned with the corresponding practices in ASPICE for Cybersecurity. This alignment ensures consistency in applying cybersecurity measures throughout the product development process.

Clause 11: Cybersecurity Validation.
Clause 11 involves the cybersecurity validation of an item at the vehicle level. It encompasses the evaluation and confirmation that the implemented cybersecurity measures effectively achieve the intended goals when integrated into the complete vehicle system[6]. Including this clause ensures that validation activities are adequately addressed, aligning with ASPICE practices related to integration and validation. This verification confirms that the product meets both functional and cybersecurity requirements before release.

Clause 15: Threat Analysis and Risk Assessment Methods.
Clause 15 includes modular methods for analysis and assessment to determine the extent of cybersecurity risk so that treatment can be pursued [6]. It provides the methodological foundation for systematically identifying threats, evaluating risks, and deciding on appropriate mitigation strategies. Mapping this clause is essential for ensuring that risk assessment processes are harmonized between ISO 21434 and ASPICE for

BUPT

Cybersecurity. This harmonization facilitates a consistent approach to managing cybersecurity risks throughout the development lifecycle.

2.2 Rationale for Selecting These Clauses

By focusing on these specific clauses, the mapping concentrates on the product development aspects that are directly relevant to the technical processes within ASPICE for Cybersecurity. This targeted approach facilitates a more effective and practical mapping, allowing organizations to implement cybersecurity measures that are consistent with both standards without the complexities introduced by organizational considerations.

Setting aside the organizational aspects reduces potential confusion and streamlines the mapping process, making it more accessible and actionable for practitioners focused on the technical implementation of cybersecurity in automotive systems. The selected clauses provide comprehensive coverage of the product development lifecycle from a cybersecurity perspective. Including Clause 7 ensures that distributed activities and responsibilities are clearly defined, which is crucial for collaborative development environments.

This approach facilitates a coherent and efficient strategy for organizations to meet the requirements of both standards. By aligning the technical processes and focusing on product development, the mapping supports the development of secure and resilient automotive products. It ensures that cybersecurity is integrated at every stage, from initial concept through design, implementation, verification, and validation.

Concentrating on Clauses 7, 9, 10, 11, and 15 of ISO/SAE 21434 provides a focused and practical basis for mapping to ASPICE for Cybersecurity. This selection emphasizes the critical technical activities essential for embedding cybersecurity into automotive products while leaving aside organizational aspects that are outside the immediate scope of product development teams. The resulting compliance matrix offers a stable and suitable alignment between the two standards, facilitating a clearer understanding of how to implement cybersecurity requirements effectively. Ultimately, this focused mapping contributes to the development of vehicles that are resilient against cyber threats and compliant with industry standards.

BUPT

3 Mapping between ISO 21434 and ASPICE for Cybersecurity

The mapping between ISO/SAE 21434 [6]and ASPICE for Cybersecurity [7] involves aligning the requirements and processes of these two standards to facilitate integrated compliance and efficient implementation of cybersecurity practices in automotive development. This chapter presents the detailed mappings between selected clauses of ISO 21434, specifically Clauses 7, 9, 10, 11, and 15, and the corresponding base practices in ASPICE for Cybersecurity.

For each clause, the mapping includes detailed explanations of how specific requirements in ISO 21434 correspond to base practices in ASPICE for Cybersecurity. Rationalizations are provided to clarify the relationships and ensure that practitioners understand how compliance with one standard supports compliance with the other.

This comprehensive mapping serves as a practical tool for organizations to integrate their compliance efforts, reducing duplication and enhancing efficiency. By understanding the alignments and correspondences, practitioners can implement processes that satisfy both standards simultaneously, promoting a cohesive approach to automotive cybersecurity.

3.1 Mapping of Clause 7

Clause 7 of ISO/SAE 21434 addresses the management of distributed cybersecurity activities when responsibilities are shared between different parties involved in the development of an item or component. This clause is particularly relevant in scenarios where development tasks are distributed between customers and suppliers, including both external partners and internal divisions functioning as suppliers. It emphasizes the need for clear definitions of interactions, dependencies, and responsibilities to ensure effective collaboration in cybersecurity efforts.

This clause applies to items and components developed through distributed activities, interactions between customers and suppliers, and all phases where agreements govern the customer-supplier interface. The primary objective is to establish agreements that delineate each party's obligations regarding cybersecurity tasks, communication protocols, and handling of cybersecurity-related information.

In this chapter, the requirements outlined in Clause 7 are mapped to the corresponding base practices in ASPICE for Cybersecurity. This mapping provides a coherent framework that organizations can use to ensure that distributed cybersecurity activities are managed effectively and are compliant with both ISO/SAE 21434 and ASPICE standards. By aligning the requirements and practices, organizations can enhance collaboration, ensure consistency in cybersecurity practices across all involved parties, and improve the overall security posture of automotive products throughout their development lifecycle.

BUPT

Supplier Capability (7.4.1).

Mapping Between ISO 21434 Requirements RQ-07-01, RQ-07-02 and ASPICE for Cybersecurity Base Practices ACQ.2.BP1, ACQ.2.BP2.
The ISO 21434 Requirements RQ-07-01 and RC-07-02 emphasize the critical need for evaluating and documenting a supplier's capability in cybersecurity within the automotive industry. These requirements are directly mapped to the ASPICE for Cybersecurity base practices ACQ.2.BP1 and ACQ.2.BP2, which provide a structured framework for establishing evaluation criteria and assessing potential suppliers based on their cybersecurity competencies.

ISO 21434 Requirement RQ-07-01 mandates that the capability of a candidate supplier to develop and, if applicable, perform post-development activities in accordance with the standard must be evaluated. This evaluation is essential for supplier selection and can be based on the supplier’s ability to conform to ISO 21434 or previous implementations of other cybersecurity engineering standards. ASPICE base practice ACQ.2.BP1 aligns with this requirement by instructing organizations to establish supplier evaluation criteria through the analysis of relevant requirements to define the necessary capabilities of suppliers. This practice suggests that the criteria may consider technical evaluations regarding the supplier's cybersecurity capabilities, including concepts and methods such as threat analysis, risk assessment, attack models, and vulnerability analysis. By incorporating these technical aspects, ACQ.2.BP1 ensures that suppliers are assessed on their ability to meet the specific cybersecurity requirements outlined in ISO 21434.

Moreover, ACQ.2.BP1 recommends evaluating the organization's capability concerning cybersecurity, encompassing best practices from development, post-development, governance, quality, and information security. This comprehensive approach addresses both the development and post-development activities highlighted in RQ-07-01, ensuring that suppliers are capable of maintaining cybersecurity standards throughout the product lifecycle. Additionally, the practice includes considering the supplier's performance evidence from previous projects, which aligns with the ISO requirement's note about evaluating prior implementations of cybersecurity standards. ASPICE base practice ACQ.2.BP2 complements this by focusing on the evaluation of potential suppliers. It involves collecting information about the suppliers' capabilities and evaluating it against the established criteria, leading to the short-listing of preferred suppliers and documentation of the results. This practice operationalizes RQ-07-01 by facilitating a systematic assessment process. The notes under ACQ.2.BP2 specify that the evaluation may be supported by summaries of previous Automotive SPICE for Cybersecurity assessments and evidence of the supplier's cybersecurity and information security management systems. These elements provide concrete evidence of the supplier's capability to conform to ISO 21434 or other relevant standards, fulfilling the intent of RQ-07-01.

ISO 21434 Requirement RC-07-02 further specifies that suppliers should provide a record of cybersecurity capability to support a customer's evaluation. This record can include evidence of the organization's capability concerning cybersecurity, evidence of continual cybersecurity activities (as per Clause 8), cybersecurity incident response (as per Clause 13), and summaries of previous cybersecurity assessment reports.

BUPT

ACQ.2.BP1 addresses this requirement by suggesting that the evaluation criteria may include the organization's capability concerning cybersecurity, covering best practices from development to information security. By establishing criteria that require suppliers to demonstrate their organizational capabilities, ACQ.2.BP1 ensures that suppliers provide comprehensive records of their cybersecurity capabilities, as recommended in RC-07-02. ACQ.2.BP2 supports this by indicating that the evaluation may be supplemented with summaries of previous assessments and evidence of the supplier's cybersecurity management systems. This aligns with RC-07-02's emphasis on suppliers providing documentation that demonstrates their ongoing commitment to cybersecurity practices.

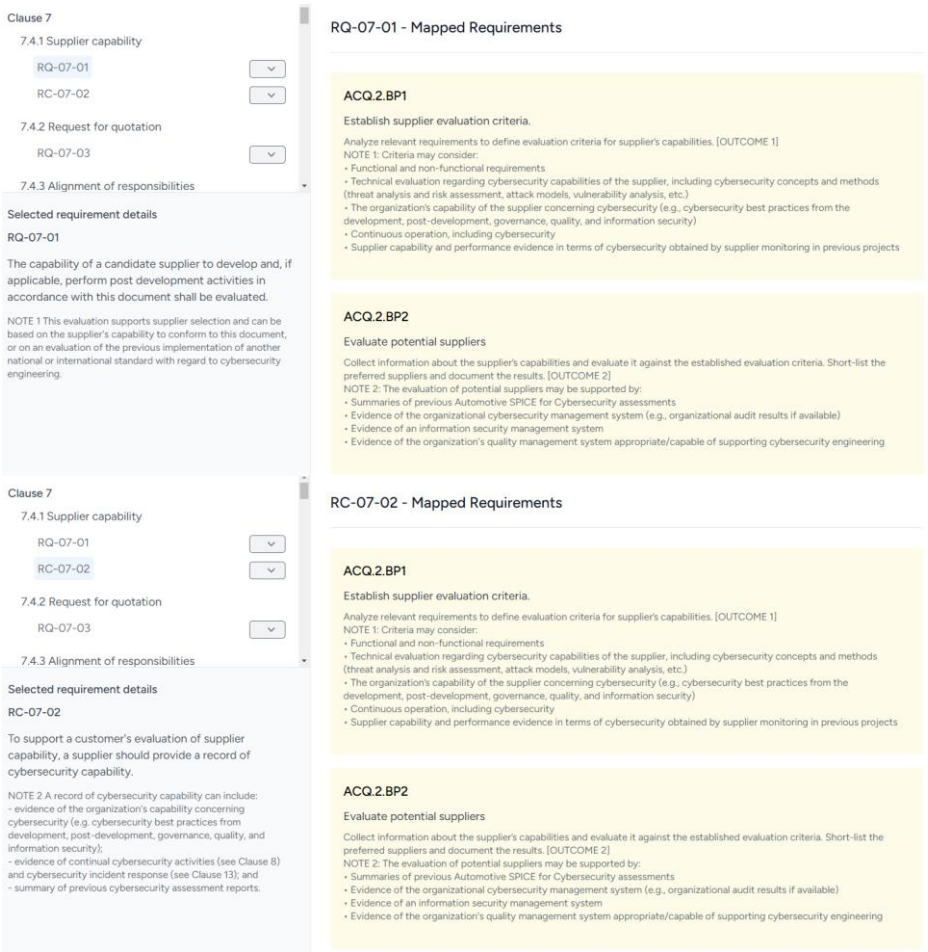


Fig. 16. Mapping of ISO 21434 Requirements RQ-07-01, RQ-07-02

BUPT

However, there are aspects of RC-07-02 that are not fully covered by the ASPICE base practices. Specifically, RC-07-02 mentions the need for evidence of continual cybersecurity activities and cybersecurity incident response mechanisms, referring to Clauses 8 and 13 of ISO 21434. While ACQ.2.BP1 and ACQ.2.BP2 recommend evaluating the supplier's organizational capabilities and management systems, they do not explicitly require evidence of these continual activities or incident response capabilities. This omission could result in a less comprehensive evaluation of the supplier's ability to maintain and improve cybersecurity measures over time, which is critical for long-term product security.

To fully align with ISO 21434 RC-07-02, organizations should consider enhancing their evaluation criteria within ACQ.2.BP1 to explicitly include requirements for evidence of continual cybersecurity activities and incident response mechanisms. This would ensure that suppliers are not only assessed on their current capabilities but also on their ability to sustain and evolve their cybersecurity practices in response to emerging threats. Additionally, while ACQ.2.BP2 focuses on the collection of information by the customer, RC-07-02 suggests that suppliers should proactively provide records to support the evaluation. Encouraging a more proactive approach from suppliers can lead to a more collaborative evaluation process and ensure that all necessary information is available for a thorough assessment.

In summary, the ASPICE for Cybersecurity base practices ACQ.2.BP1 and ACQ.2.BP2 are closely mapped to ISO 21434 Requirements RQ-07-01 and RC-07-02, providing a robust framework for evaluating a supplier's cybersecurity capabilities. They cover essential aspects such as the establishment of evaluation criteria, assessment of technical capabilities, organizational practices, and consideration of past performance. However, to achieve full compliance with the ISO requirements, organizations should explicitly include the evaluation of continual cybersecurity activities and incident response capabilities in their assessment criteria. By addressing these areas, organizations can ensure a comprehensive evaluation that not only meets regulatory standards but also enhances the overall cybersecurity posture of the automotive supply chain.

Request for Quotation (7.4.2)

Mapping Between ISO 21434 Requirement RQ-07-03 and ASPICE for Cybersecurity Base Practice ACQ.2.BP3

The ISO 21434 Requirement RQ-07-03 mandates that a customer's request for quotation (RFQ) to a candidate supplier must include specific cybersecurity-related elements. These elements are crucial for ensuring that the supplier is fully aware of the cybersecurity expectations and obligations associated with the project. The requirement specifies that the RFQ shall include: a formal request for the supplier to conform to ISO 21434, the expectation that the supplier will assume cybersecurity responsibilities as outlined in Clause 7.4.3 of the standard, and the cybersecurity goals or a set of cybersecurity requirements relevant to the item or component being quoted. This requirement is directly mapped to the ASPICE for Cybersecurity base practice ACQ.2.BP3. This base practice focuses on the preparation and execution of the RFQ, ensuring that it

BUPT

encompasses all necessary information and requirements related to cybersecurity. ACQ.2.BP3 involves identifying supplier candidates based on prior evaluations and preparing an RFQ that includes a corrective action plan for any identified deviations. The notes accompanying this base practice suggest that the RFQ may include a formal request for the supplier to conform with all customer-relevant and legal standards, specify the cybersecurity responsibilities of the supplier, outline the scope of work regarding cybersecurity—including the cybersecurity goals or relevant requirements—and include an action plan for identified deviations and risks.

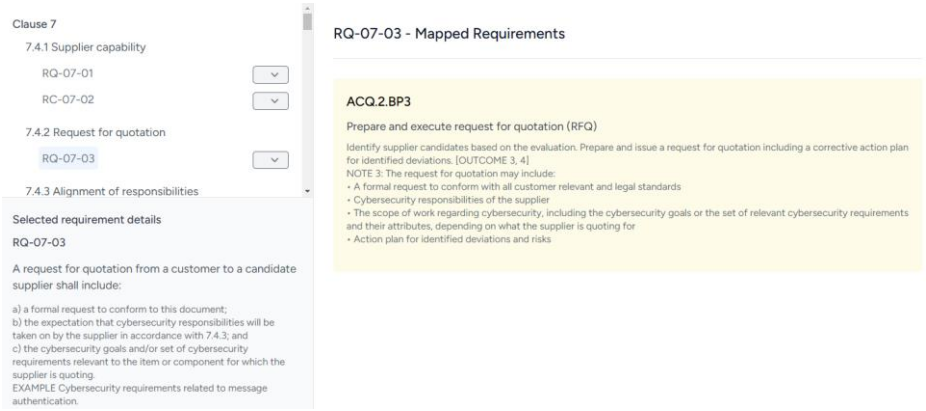


Fig. 17. Mapping of ISO 21434 Requirement RQ-07-03

The mapping between ISO RQ-07-03 and ASPICE ACQ.2.BP3 is evident in several key aspects. Firstly, both emphasize the inclusion of a formal request for the supplier to conform to relevant cybersecurity standards. In the ISO requirement, this is a direct request to conform to ISO 21434, ensuring that the supplier is contractually bound to adhere to the industry's cybersecurity standard throughout the development and post-development processes. Similarly, ACQ.2.BP3 recommends that the RFQ include a formal request to conform with all customer-relevant and legal standards, which would naturally encompass ISO 21434 for projects within its scope. Secondly, both the ISO requirement and the ASPICE base practice highlight the importance of clarifying the supplier's cybersecurity responsibilities within the RFQ. ISO RQ-07-03 specifies that the RFQ should include the expectation that cybersecurity responsibilities will be assumed by the supplier in accordance with Clause 7.4.3 of ISO 21434. This clause details the allocation of cybersecurity responsibilities between the customer and supplier, emphasizing collaboration and clear delineation of tasks. ACQ.2.BP3 mirrors this by advising that the RFQ should include the cybersecurity responsibilities of the supplier. By explicitly stating these responsibilities, the customer ensures that the supplier understands their role in maintaining cybersecurity throughout the project, fostering accountability and minimizing potential misunderstandings. Thirdly, both documents stress the necessity of including the cybersecurity goals and/or relevant cybersecurity requirements in the RFQ. ISO RQ-07-03 requires that the RFQ provide the cybersecurity goals

BUPT

or set of cybersecurity requirements relevant to the item or component for which the supplier is quoting. This provision allows the supplier to comprehend the specific cybersecurity measures expected, enabling them to prepare a quotation that accurately reflects the scope of work and associated costs. Correspondingly, ACQ.2.BP3 suggests that the RFQ include the scope of work regarding cybersecurity, including the cybersecurity goals or the set of relevant cybersecurity requirements and their attributes. By providing detailed requirements, the RFQ facilitates a mutual understanding between the customer and supplier, ensuring that the supplier can meet the project's cybersecurity needs effectively.

An additional aspect included in ACQ.2.BP3, although not explicitly mentioned in ISO RQ-07-03, is the recommendation to include an action plan for identified deviations and risks within the RFQ. This proactive approach encourages suppliers to consider potential issues and outline strategies for managing and mitigating risks. While ISO RQ-07-03 does not specifically require this element, incorporating it enhances the robustness of the RFQ and contributes to a more comprehensive cybersecurity strategy. Despite the strong alignment, there is a minor gap in that ACQ.2.BP3 does not explicitly reference Clause 7.4.3 of ISO 21434 when detailing the supplier's cybersecurity responsibilities. ISO RQ-07-03 specifically points to this clause, which provides detailed guidance on the allocation of cybersecurity responsibilities between the customer and supplier. The absence of an explicit reference in the ASPICE base practice might lead to potential misunderstandings if the supplier is not fully aware of the specific expectations outlined in that clause. To address this gap and ensure full alignment with ISO 21434 RQ-07-03, it is advisable for organizations applying ACQ.2.BP3 to explicitly reference Clause 7.4.3 in the RFQ when specifying the supplier's cybersecurity responsibilities. By doing so, the RFQ would provide clear and direct guidance, ensuring that suppliers are fully informed of their obligations as per the standard. This explicit reference would enhance clarity, reduce the risk of misinterpretation, and promote better collaboration between the customer and supplier.

In conclusion, the ASPICE for Cybersecurity base practice ACQ.2.BP3 effectively maps to ISO 21434 Requirement RQ-07-03 by providing comprehensive guidelines for preparing an RFQ that integrates essential cybersecurity elements. Both the ISO requirement and the ASPICE practice emphasize the necessity of a formal request for conformance to cybersecurity standards, the importance of defining the supplier's cybersecurity responsibilities, and the inclusion of specific cybersecurity goals and requirements relevant to the project. By addressing the minor gap of explicitly referencing Clause 7.4.3 in the RFQ, organizations can ensure complete alignment with ISO 21434, thereby enhancing the effectiveness of the supplier evaluation and selection process. This alignment not only fulfills regulatory requirements but also strengthens the overall cybersecurity posture of the automotive industry by fostering clear communication and shared responsibility between customers and suppliers.

BUPT

Alignment of Responsibilities (7.4.3)

Mapping Between ISO 21434 Requirements RQ-07-04, RQ-07-05 and ASPICE for Cybersecurity Base Practices ACQ.2.BP4, ACQ.4.BP1

The ISO 21434 Requirements RQ-07-04 and RC-07-05 emphasize the critical need for a detailed cybersecurity interface agreement between the customer and the supplier in automotive projects. RQ-07-04 mandates that this agreement should specify the distributed cybersecurity activities, including the appointment of points of contact, identification of cybersecurity activities to be performed by each party, joint tailoring of activities, shared information and work products, milestones, and the definition of the end of cybersecurity support for the item or component. RC-07-05 further stipulates that this agreement should be mutually agreed upon before the start of the distributed cybersecurity activities. These requirements align closely with the ASPICE for Cybersecurity base practices ACQ.2.BP4 and ACQ.4.BP1. ACQ.2.BP4 focuses on negotiating and awarding the contract or agreement, establishing it based on the evaluation of the request for quotation results, and covering the relevant requirements and agreed corrective actions. It suggests that distributed cybersecurity activities may be specified within a cybersecurity interface agreement, considering aspects such as contacts, tailoring, responsibilities, information sharing, milestones, and timing. This directly corresponds with the elements outlined in ISO RQ-07-04. ACQ.4.BP1 emphasizes agreeing on and maintaining joint processes, interfaces, and the information to be exchanged. It involves establishing and maintaining an agreement on joint processes, interfaces, responsibilities, the type and frequency of joint activities, communications, meetings, status reports, and reviews. This practice supports ISO RQ-07-04 by ensuring that both parties have a clear understanding of how they will collaborate on cybersecurity activities, including project management, requirements management, change management, configuration management, problem resolution, quality assurance, and customer acceptance.

The mapping between the ISO requirements and the ASPICE base practices is evident in several key aspects. Firstly, the appointment of customer's and supplier's points of contact regarding cybersecurity, as required by ISO RQ-07-04(a), is addressed in both ACQ.2.BP4 and ACQ.4.BP1 through the emphasis on clear communication channels and responsibilities. Secondly, the identification of cybersecurity activities to be performed by the customer and supplier, as per ISO RQ-07-04(b), is supported by ACQ.2.BP4's focus on defining responsibilities and agreed corrective actions, as well as ACQ.4.BP1's emphasis on joint processes and responsibilities.

BUPT

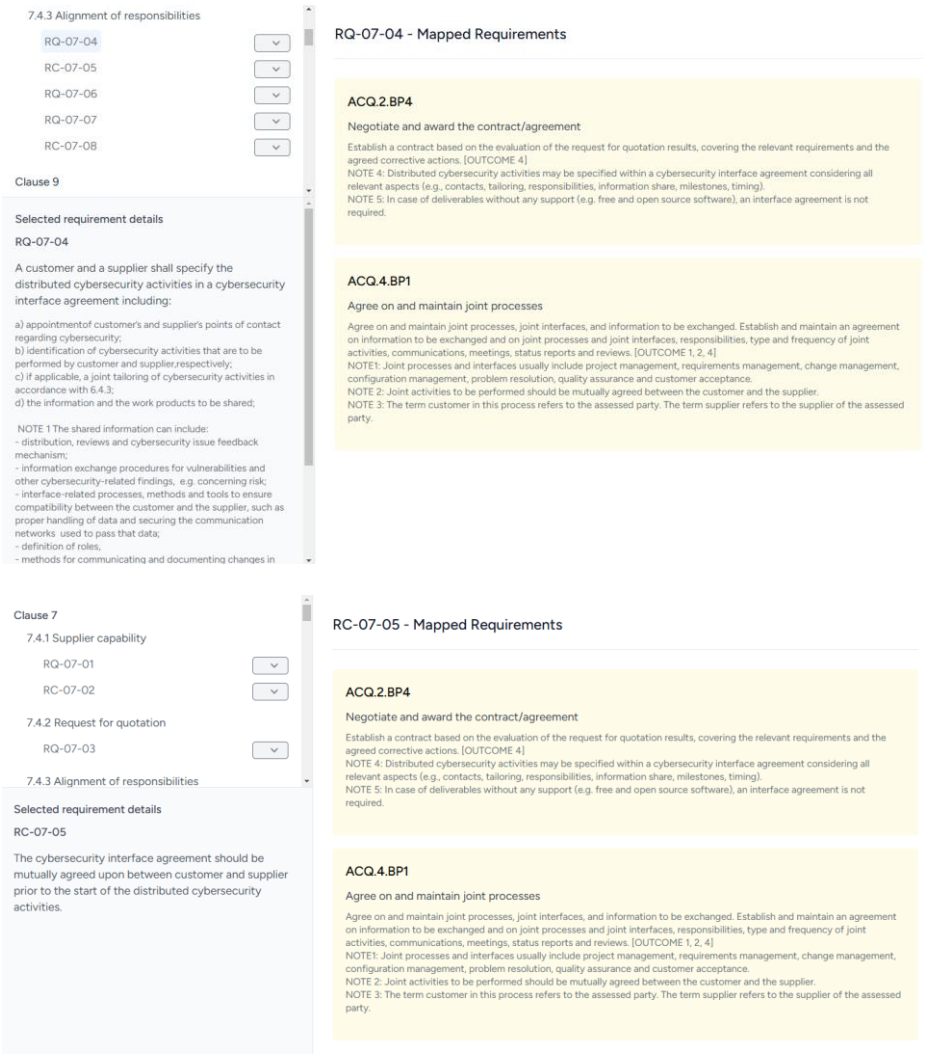


Fig. 18. Mapping of ISO 21434 Requirements RQ-07-04, RQ-07-05

The joint tailoring of cybersecurity activities in accordance with ISO 21434 Clause 6.4.3, mentioned in ISO RQ-07-04(c), is facilitated by ACQ.2.BP4's consideration of tailoring within the cybersecurity interface agreement. The information and work products to be shared, as outlined in ISO RQ-07-04(d), are addressed in ACQ.4.BP1's requirement to agree on the information to be exchanged and the joint interfaces. ISO RQ-07-04's Note 1 provides detailed examples of shared information, such as distribution, reviews, cybersecurity issue feedback mechanisms, information exchange procedures for vulnerabilities and other cybersecurity-related findings, interface-related processes, methods and tools to ensure compatibility, definition of roles, methods for

BUPT

communicating and documenting changes, alignment on requirements management tools, and results of cybersecurity assessments. These are encompassed within ACQ.4.BP1's scope, which includes joint activities like project management, requirements management, change management, configuration management, and problem resolution. The inclusion of milestones regarding the distributed cybersecurity activities, as per ISO RQ-07-04(e), is supported by ACQ.2.BP4's suggestion to consider milestones and timing within the cybersecurity interface agreement. The definition of the end of cybersecurity support for the item or component, required by ISO RQ-07-04(f), aligns with ACQ.2.BP4's emphasis on covering all relevant requirements within the contract. ISO RC-07-05's stipulation that the cybersecurity interface agreement should be mutually agreed upon between the customer and supplier prior to the start of the distributed cybersecurity activities is reinforced by ACQ.4.BP1's focus on establishing and maintaining an agreement on joint processes and interfaces, and by ACQ.2.BP4's guidance on negotiating and awarding the contract based on the evaluation results.

While the ASPICE practices cover the majority of the ISO requirements, there are aspects that may not be fully addressed. For instance, although ACQ.4.BP1 emphasizes agreeing on joint processes and interfaces, it may not explicitly mention certain specific elements highlighted in ISO RQ-07-04 Note 1, such as methods for communicating and documenting changes in the item or component, including potential reiteration of the Threat Analysis and Risk Assessment (TARA), or the alignment on requirements management tools. These could be inferred under project management and requirements management, but making explicit references to these elements could enhance the alignment. Additionally, while ACQ.2.BP4 and ACQ.4.BP1 cover the need for agreements prior to commencing activities, the emphasis on mutual agreement before the start of distributed cybersecurity activities, as specified in ISO RC-07-05, underscores the importance of timing in establishing these agreements. Ensuring that agreements are not only established but also mutually agreed upon before activities commence is crucial. While this is generally implied in the ASPICE practices, explicitly stating the requirement for mutual agreement prior to starting activities would strengthen compliance with ISO requirements.

In conclusion, the ASPICE for Cybersecurity base practices ACQ.2.BP4 and ACQ.4.BP1 closely align with ISO 21434 Requirements RQ-07-04 and RC-07-05 by providing a structured approach to establishing a cybersecurity interface agreement that specifies distributed cybersecurity activities, responsibilities, processes, and information exchange between the customer and supplier. The mapping covers key aspects such as appointing points of contact, identifying activities and responsibilities, joint tailoring, information sharing, setting milestones, and defining the end of support. By thoroughly integrating these practices and addressing the minor gaps identified, organizations can establish clear and effective collaboration agreements that support robust cybersecurity throughout the development lifecycle.

Mapping Between ISO 21434 Requirement RQ-07-06 and ASPICE for Cybersecurity Base Practices ACQ.2.BP4, ACQ.4.BP5

ISO 21434 Requirement RQ-07-06 underscores the critical importance of collaboration between the customer and supplier when an identified vulnerability needs to be

BUPT

managed according to the specified procedures in RQ-08-07. This requirement mandates that both parties must come to an agreement on the actions to be taken and clearly define the responsibilities for those actions. This collaborative approach ensures that vulnerabilities are addressed effectively, minimizing potential risks to the automotive product's cybersecurity posture. The ASPICE for Cybersecurity base practices ACQ.2.BP4 and ACQ.4.BP5 align closely with this ISO requirement by providing structured methodologies for negotiating agreements and managing deviations from agreed objectives. ACQ.2.BP4 focuses on the negotiation and awarding of the contract or agreement. It involves establishing a contract based on the evaluation of the request for quotation results, covering all relevant requirements and the agreed corrective actions. This practice ensures that any known vulnerabilities or potential cybersecurity issues are identified and addressed within the contractual framework. By including agreed corrective actions in the contract, ACQ.2.BP4 directly supports the ISO requirement for the customer and supplier to agree on actions and responsibilities regarding identified vulnerabilities. Furthermore, Note 4 under ACQ.2.BP4 mentions that distributed cybersecurity activities may be specified within a cybersecurity interface agreement, considering all relevant aspects such as contacts, tailoring, responsibilities, information sharing, milestones, and timing. This detailed consideration of responsibilities and information sharing is essential for effectively managing vulnerabilities. It ensures that both the customer and supplier have a clear understanding of their roles and the procedures to follow when a vulnerability is identified, aligning with the collaborative spirit of ISO RQ-07-06.

ACQ.4.BP5 emphasizes the importance of acting to correct deviations from the agreed project plans. It requires taking action when agreed objectives are not achieved, correcting deviations, and preventing the recurrence of identified problems. This involves negotiating changes to objectives and documenting them in the agreements. ACQ.4.BP5 directly correlates with the ISO requirement by ensuring that when a vulnerability is identified—a deviation from the expected cybersecurity standards—the customer and supplier work together to agree on corrective actions and adjust their agreements accordingly. By mandating the negotiation and documentation of changes to objectives, ACQ.4.BP5 ensures that both parties remain aligned in their approach to addressing vulnerabilities. This practice not only addresses immediate concerns but also contributes to the continuous improvement of the cybersecurity processes by preventing the recurrence of similar issues. This proactive stance is essential for maintaining the cybersecurity integrity of automotive products throughout their lifecycle.

While the ASPICE practices effectively cover the collaborative agreement on actions and responsibilities, there is a subtle aspect in ISO RQ-07-06 that may not be explicitly addressed. The ISO requirement specifies that the vulnerability management should be in accordance with RQ-08-07, which likely contains detailed procedures and standards for handling vulnerabilities. The ASPICE practices do not explicitly reference RQ-08-07 or provide specific guidelines on the vulnerability management processes outlined therein. To fully align with ISO 21434, organizations should ensure that their contracts and agreements not only include provisions for agreeing on actions and responsibilities but also explicitly reference and adhere to the detailed procedures specified in RQ-08-07. This would involve integrating the specific vulnerability

BUPT

management processes into the contractual agreements and the corrective action plans, ensuring comprehensive compliance with the ISO standard.

In summary, the ASPICE for Cybersecurity base practices ACQ.2.BP4 and ACQ.4.BP5 provide a robust framework that aligns with ISO 21434 Requirement RQ-07-06 by facilitating collaboration between the customer and supplier in managing identified vulnerabilities. ACQ.2.BP4 ensures that contracts include agreed corrective actions and responsibilities, while ACQ.4.BP5 focuses on taking corrective actions when deviations occur, negotiating changes, and documenting them appropriately. By addressing the minor gap of explicitly incorporating the procedures from RQ-08-07 into their agreements, organizations can achieve full alignment with the ISO requirement, thereby enhancing their cybersecurity resilience and compliance.

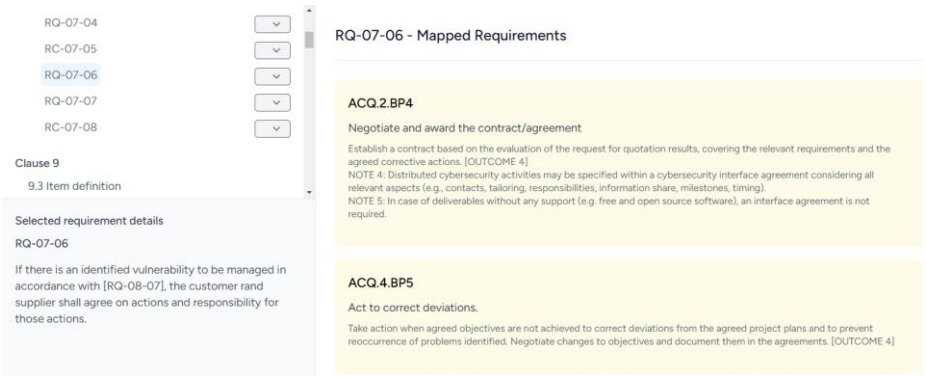


Fig. 19. Mapping of ISO 21434 Requirement RQ-07-06

Mapping Between ISO 21434 Requirement RQ-07-07 and ASPICE for Cybersecurity Base Practices ACQ.4.BP2, ACQ.4.BP5

The ISO 21434 Requirement RQ-07-07 emphasizes the importance of effective communication between the customer and the supplier when dealing with cybersecurity requirements that are unclear, not feasible, or in conflict with other cybersecurity requirements or requirements from other disciplines. This requirement mandates that both parties must promptly notify each other of such issues to enable appropriate decisions and actions to be taken. This collaborative approach is crucial in the automotive industry, where the complexity of systems and the critical nature of cybersecurity necessitate clear and timely communication to ensure the security and reliability of the final product.

This ISO requirement aligns closely with the ASPICE for Cybersecurity base practices ACQ.4.BP2 and ACQ.4.BP5, which provide a structured framework for managing such situations. ACQ.4.BP2 focuses on the exchange of all agreed information between the customer and supplier using defined joint interfaces. This practice ensures that there are established channels and protocols for communication, facilitating the efficient sharing of information related to project requirements, progress, and any issues that

BUPT

arise. By utilizing these joint interfaces, both parties can promptly communicate when they encounter unclear, infeasible, or conflicting requirements. This immediate exchange of information allows for quicker identification of problems and collaborative resolution, which is essential for maintaining project timelines and ensuring that cybersecurity considerations are adequately addressed. For example, if a supplier identifies that a specific cybersecurity requirement is not feasible due to technical limitations or conflicts with other system requirements, ACQ.4.BP2 encourages the supplier to use the agreed communication channels to inform the customer promptly. Similarly, if the customer recognizes that provided requirements may conflict with other disciplines such as safety or performance, they can notify the supplier through these interfaces. This proactive communication helps prevent misunderstandings and ensures that both parties are aligned in their understanding of the project's objectives and constraints.

ACQ.4.BP5 addresses the need to act to correct deviations when agreed objectives are not achieved. This practice involves taking corrective actions to address deviations from the agreed project plans and preventing the recurrence of identified problems. It requires the negotiation of changes to objectives and the documentation of these changes in the agreements. In the context of ISO RQ-07-07, when unclear, infeasible, or conflicting requirements are identified, they represent deviations from the original project plan. ACQ.4.BP5 provides a mechanism for the customer and supplier to collaboratively develop solutions to these issues. Through ACQ.4.BP5, both parties engage in discussions to understand the nature of the problem, assess its impact on the project, and agree on the necessary adjustments to requirements or project plans. This may involve redefining requirements to make them more achievable, resolving conflicts between requirements from different disciplines, or exploring alternative solutions that meet the project's objectives. By documenting these changes in the agreements, both the customer and supplier have a clear record of the decisions made and the new expectations, which helps in maintaining transparency and accountability throughout the project lifecycle.

Together, ACQ.4.BP2 and ACQ.4.BP5 facilitate a collaborative and systematic approach to managing issues related to cybersecurity requirements. They ensure that communication lines are open and effective, and that there are established processes for addressing and documenting changes. This alignment with ISO RQ-07-07 ensures that potential problems are addressed proactively, reducing the risk of delays, cost overruns, or compromised cybersecurity in the final product. Moreover, these practices promote a culture of continuous improvement and adaptability within both organizations. By encouraging open dialogue and collaborative problem-solving, they help build stronger partnerships between customers and suppliers. This is particularly important in the automotive industry, where the rapid evolution of technology and the increasing complexity of systems require agile and responsive project management practices. In conclusion, the ISO 21434 Requirement RQ-07-07 and the ASPICE for Cybersecurity base practices ACQ.4.BP2 and ACQ.4.BP5 are closely aligned in their emphasis on communication, collaboration, and proactive management of project requirements. By ensuring that both the customer and supplier are engaged in identifying and resolving issues related to unclear, infeasible, or conflicting requirements, these standards contribute to the development of secure, reliable, and high-quality automotive systems.

BUPT

Implementing these practices helps organizations navigate the complexities of cybersecurity requirements and fosters a cooperative environment that is essential for the successful delivery of automotive projects.

Mapping Between ISO 21434 Requirement RQ-07-08 and ASPICE for Cybersecurity Base Practice ACQ.4.BP1

ISO 21434 Requirement RC-07-08 emphasizes the importance of specifying responsibilities within a responsibility assignment matrix, suggesting the use of tools like a RASIC table as mentioned in Annex C of the standard. This requirement highlights the necessity for clear delineation of roles and responsibilities among all parties involved in cybersecurity activities. By defining who is Responsible, Accountable, Supporting, Informed, and Consulted (RASIC), organizations can ensure that each task is assigned appropriately, reducing ambiguity and enhancing accountability throughout the cybersecurity process. This requirement aligns closely with the ASPICE for Cybersecurity base practice ACQ.4.BP1, which focuses on agreeing upon and maintaining joint processes, interfaces, and the exchange of information. ACQ.4.BP1 mandates that organizations establish and maintain an agreement on various aspects, including the responsibilities of both the customer and the supplier. This agreement should cover the type and frequency of joint activities, communications, meetings, status reports, and reviews. By doing so, it ensures that both parties have a mutual understanding of their roles, responsibilities, and expectations, which is crucial for effective collaboration and successful project outcomes.



Fig. 20. Mapping of ISO 21434 Requirement RQ-07-08

The practice further elaborates that joint processes and interfaces typically include essential project areas such as project management, requirements management, change management, configuration management, problem resolution, quality assurance, and customer acceptance. By specifying responsibilities in these areas, organizations can ensure that all critical aspects of the project are managed effectively, and any potential issues are addressed promptly. The emphasis on mutual agreement between the customer and the supplier in ACQ.4.BP1 underscores the importance of collaboration and shared understanding, which directly supports the intent of ISO RC-07-08. While ACQ.4.BP1 covers the need to establish and maintain agreements on responsibilities,

BUPT

it does not explicitly mention the use of a responsibility assignment matrix or a RASIC table as recommended in ISO RC-07-08. The inclusion of such a tool in the ISO standard provides a structured method for documenting and communicating responsibilities, enhancing clarity and ensuring that all parties are aligned. The RASIC table serves as a valuable instrument for mapping out who is involved in each activity and their level of involvement, thereby minimizing misunderstandings and overlaps in responsibilities. The absence of an explicit reference to the responsibility assignment matrix in ACQ.4.BP1 could be seen as a gap in fully meeting the ISO requirement. Although the ASPICE practice emphasizes the agreement on responsibilities, the lack of guidance on how to document and formalize these responsibilities may lead to inconsistencies in implementation. Incorporating the use of a responsibility assignment matrix, as suggested by ISO RC-07-08, could strengthen the practice by providing a clear framework for assigning and communicating responsibilities.

In practice, organizations adopting ACQ.4.BP1 can bridge this gap by integrating the responsibility assignment matrix into their agreements on responsibilities. By doing so, they not only comply with the ISO requirement but also enhance their project management processes. The matrix can serve as a living document that is updated as the project evolves, ensuring that all parties remain informed of any changes in responsibilities and can adapt accordingly. In conclusion, ASPICE for Cybersecurity base practice ACQ.4.BP1 aligns with ISO 21434 Requirement RC-07-08 by emphasizing the importance of agreeing on and maintaining responsibilities between the customer and the supplier. Both standards recognize that clear communication and mutual understanding of roles are vital for the successful execution of cybersecurity activities. While ACQ.4.BP1 does not explicitly mention the use of a responsibility assignment matrix, incorporating this tool can enhance compliance with the ISO requirement and improve the effectiveness of responsibility management within projects. Organizations are encouraged to adopt such matrices to formalize responsibilities, facilitate better communication, and ensure that all parties are aligned in their efforts to address cybersecurity challenges.

3.2 Mapping of Clause 9

Clause 9 of ISO/SAE 21434 focuses on the concept phase of cybersecurity engineering within the automotive industry. This phase involves the consideration of vehicle-level functionality as implemented in items, where an "Item Definition" is created to identify the item and its operational environment (refer to section 9.3 of the standard). The item definition serves as the foundational basis for all subsequent cybersecurity activities, providing a comprehensive understanding of the item's characteristics and how it interacts within its operational context.

Within this clause, cybersecurity goals for the item are specified (see section 9.4). These goals represent the highest level of cybersecurity requirements and are established based on an assessment of cybersecurity risks, conducted using the methods outlined in Clause 15. Additionally, section 9.4 includes the specification of cybersecurity claims, which are used to justify decisions regarding risk retention or sharing,

BUPT

explaining why certain risks are considered acceptable or manageable without further mitigation.

The cybersecurity concept, detailed in section 9.5, comprises cybersecurity requirements and requirements on the operational environment. These are derived from the cybersecurity goals and are based on a comprehensive view of the item, ensuring that all aspects of the item's operation and interactions are considered. The cybersecurity concept outlines the strategies and measures necessary to achieve the cybersecurity goals throughout the item's lifecycle.

The objectives of Clause 9 are to define the item, its operational environment, and their interactions in the context of cybersecurity; to specify cybersecurity goals and cybersecurity claims; and to develop the cybersecurity concept to achieve the cybersecurity goals.

In this chapter, the requirements related to Clause 9 are mapped to the corresponding base practices in ASPICE for Cybersecurity. This mapping provides a structured framework for integrating the concept phase activities of ISO/SAE 21434 with the process assessment model of ASPICE for Cybersecurity. By aligning these requirements and practices, organizations can effectively incorporate cybersecurity considerations from the earliest stages of product development, ensuring a robust and comprehensive approach to managing cybersecurity risks in automotive systems.

Item Definition (9.3)

Mapping of ISO 21434 Requirements RQ-09-01, RQ-09-02

ISO 21434 Requirements RQ-09-01 and RQ-09-02 are fundamental steps in establishing a comprehensive cybersecurity framework within the automotive industry. Requirement RQ-09-01 mandates the identification of essential information about the item under consideration. This includes defining the item boundary, which distinguishes the item from its operational environment and clarifies interfaces with both internal vehicle systems and external entities. Additionally, it requires a detailed description of the item's functions across various lifecycle phases, such as development, production, operation, maintenance, and decommissioning. Understanding these functions is crucial for anticipating potential vulnerabilities and threat scenarios that may arise during the item's use. The requirement also calls for a preliminary architecture, providing an initial overview of the item's components, their connections, and external interfaces. This preliminary architecture is vital for identifying cybersecurity risks associated with different components and interfaces within the item.

Requirement RQ-09-02 extends this foundational work by necessitating a description of the operational environment relevant to the item's cybersecurity. This involves detailing all external factors and conditions under which the item operates, including assumptions about external systems, user interactions, and environmental conditions. A thorough understanding of the operational environment is essential for recognizing how external factors might introduce or influence cybersecurity threats, enabling a more accurate and effective risk assessment.

In the context of ASPICE for Cybersecurity, there is no direct mapping of specific base practices to these ISO requirements. Instead, the information gathered from RQ-

BUPT

09-01 and RQ-09-02 serves as critical input to the MAN.7 Cybersecurity Risk Management Process. The purpose of the MAN.7 process is to identify, prioritize, and analyze risks of damage to relevant stakeholders, as well as to monitor and control respective risk treatment options continuously. By thoroughly defining the item and understanding its operational environment, organizations provide the necessary foundation for the MAN.7 process to function effectively.

The detailed information from the ISO requirements enables the MAN.7 process to identify valuable assets that need protection and to recognize potential threats that could exploit vulnerabilities. A clear picture of the item boundary and operational environment allows for an in-depth analysis of where vulnerabilities may exist, both within the item itself and at its interfaces with other systems. This comprehensive understanding facilitates accurate estimation of the likelihood and impact of potential cybersecurity incidents, which is essential for effective risk prioritization. Consequently, organizations can develop tailored mitigation strategies that address specific vulnerabilities and threats identified through this detailed analysis. The absence of a direct mapping in ASPICE highlights the different focuses of the two frameworks at this stage. While ISO 21434 emphasizes the importance of item definition as a preliminary step in cybersecurity activities, ASPICE for Cybersecurity integrates this information into its risk management processes rather than defining separate base practices for item definition. In practice, organizations should ensure that the outputs from fulfilling ISO Requirements RQ-09-01 and RQ-09-02 are systematically integrated into the MAN.7 Cybersecurity Risk Management Process. This integration involves clearly documenting the item boundary, functions, preliminary architecture, and operational environment to serve as reference material throughout the risk management process. Maintaining up-to-date information as the item evolves during development ensures that risk assessments remain accurate and relevant. Engaging stakeholders from different disciplines—such as engineering, security, and operations—in contributing to the item definition and operational environment description enriches the risk analysis with diverse perspectives, leading to a more robust cybersecurity strategy.

In conclusion, although ISO 21434 Requirements RQ-09-01 and RQ-09-02 do not have a direct equivalent in the ASPICE base practices, they play a pivotal role in informing the MAN.7 Cybersecurity Risk Management Process within ASPICE for Cybersecurity. By thoroughly defining the item and its operational environment, organizations equip themselves with the necessary insights to perform effective cybersecurity risk management. This alignment between ISO 21434 and ASPICE ensures a cohesive approach to cybersecurity, ultimately contributing to the development of secure automotive systems that protect stakeholders from potential risks.

BUPT

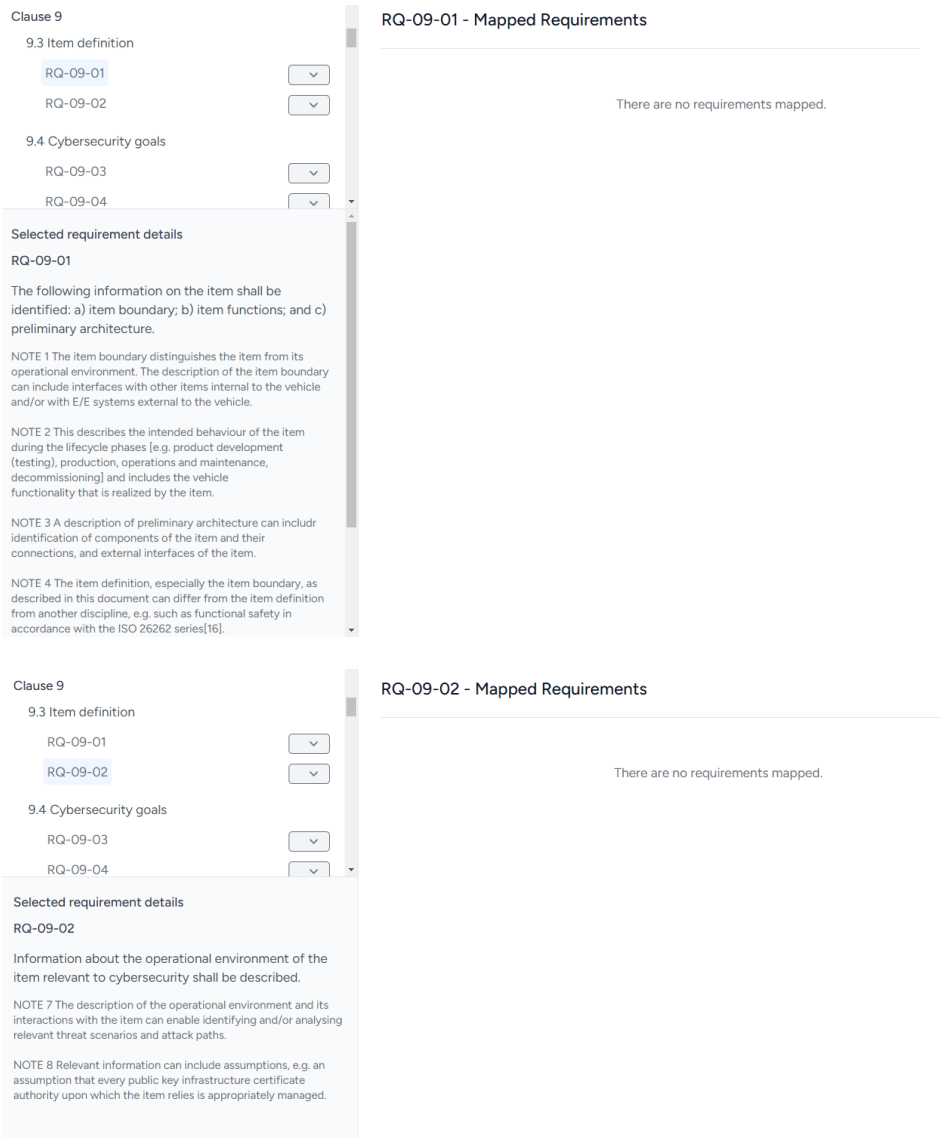


Fig. 21. Mapping of ISO 21434 Requirements RQ-09-01, RQ-09-02

Cybersecurity Goals (9.4)

Mapping Between ISO 21434 Requirement RQ-09-03 and ASPICE for Cybersecurity Base Practice MAN.7.BP1

ISO 21434 Requirement RQ-09-03 mandates a comprehensive analysis based on the item definition, which involves several critical steps essential for establishing a robust

BUPT

cybersecurity framework. These steps include asset identification, threat scenario identification, impact rating, attack path analysis, attack feasibility rating, and risk value determination, all in accordance with the respective clauses of ISO 21434 Clause 15. This requirement ensures that organizations systematically identify and assess potential cybersecurity risks associated with the item, laying the groundwork for effective risk management strategies. The ASPICE for Cybersecurity base practice MAN.7.BP1 aligns closely with this ISO requirement by focusing on determining the scope of cybersecurity risk management to be performed. This involves identifying project assets with cybersecurity properties, defining damage scenarios, relevant stakeholders, impact categories, and related product phases, all in accordance with the operational environment and organizational risk management policies. By establishing this scope, MAN.7.BP1 sets the stage for a thorough risk assessment process.

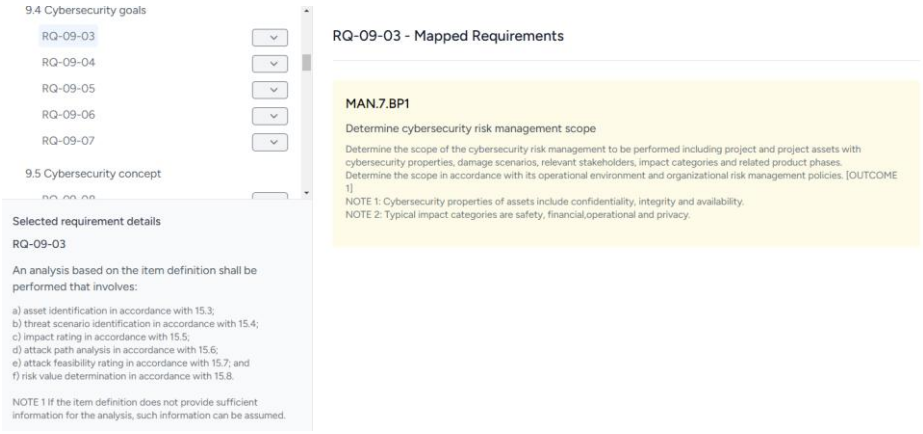


Fig. 22. Mapping of ISO 21434 Requirement RQ-09-03

Both RQ-09-03 and MAN.7.BP1 are actually starting points for the Threat Analysis and Risk Assessment (TARA) process. TARA is a fundamental component of cybersecurity risk management, providing a structured approach to identifying threats, assessing risks, and determining appropriate mitigation strategies. The steps outlined in RQ-09-03 correspond directly to the key activities within TARA, such as identifying assets and threats, analyzing attack paths, assessing impact and feasibility, and calculating risk values. Similarly, MAN.7.BP1 prepares the organization for TARA by defining the scope and context within which the risk assessment will occur. By determining the relevant assets, stakeholders, and impact categories, it ensures that the TARA process is focused and comprehensive, addressing all critical aspects of the item's cybersecurity. The mapping of TARA from ISO Clause 15 and the ASPICE MAN.7 Process will be highlighted later, providing a detailed correlation between the specific activities and outputs of both frameworks. This mapping will illustrate how the systematic approach prescribed in ISO Clause 15 is operationalized within the ASPICE MAN.7

BUPT

Process, ensuring that organizations can effectively integrate the requirements of both standards into their cybersecurity practices.

In conclusion, ISO 21434 Requirement RQ-09-03 and ASPICE MAN.7.BP1 are closely interconnected through their shared role in initiating the TARA process. By adhering to these requirements, organizations establish a solid foundation for identifying, assessing, and managing cybersecurity risks. The forthcoming detailed mapping between ISO Clause 15 and the ASPICE MAN.7 Process will further clarify how these standards align, enabling organizations to leverage the strengths of both frameworks in enhancing their cybersecurity posture.

Mapping Between ISO 21434 Requirements RQ-09-04, RQ-09-05, RQ-09-06 and ASPICE for Cybersecurity Base Practice MAN.7.BP6

ISO 21434 Requirements RQ-09-04, RQ-09-05, and RQ-09-06 focus on the critical process of determining risk treatment options for each identified threat scenario, which is a fundamental aspect of cybersecurity risk management in the automotive industry. These requirements ensure that organizations systematically assess and decide on how to handle the risks associated with various threat scenarios, whether by reducing, accepting, avoiding, or sharing the risks.

Requirement RQ-09-04 mandates that, based on the results of the analysis performed in RQ-09-03, organizations must determine appropriate risk treatment options for each threat scenario in accordance with Section 15.9 of ISO 21434. This involves a thorough evaluation of each threat scenario to decide the most suitable course of action to manage the associated risks effectively. The accompanying note emphasizes that avoiding a risk by removing its source may lead to changes in the item, which should be managed through proper change management processes as outlined in Section 5.4.4. This highlights the interconnected nature of risk treatment decisions and change management within the cybersecurity framework.

Requirement RQ-09-05 specifies that if the decision is to reduce the risk for a particular threat scenario, then one or more corresponding cybersecurity goals must be specified. Cybersecurity goals are high-level objectives that define the desired security properties of the item to mitigate the identified risks. By establishing these goals, organizations provide clear direction for designing and implementing security measures that effectively reduce risks to an acceptable level. The note reiterates that avoiding a risk by eliminating its source may necessitate changes to the item, again linking risk treatment decisions to change management procedures.

BUPT

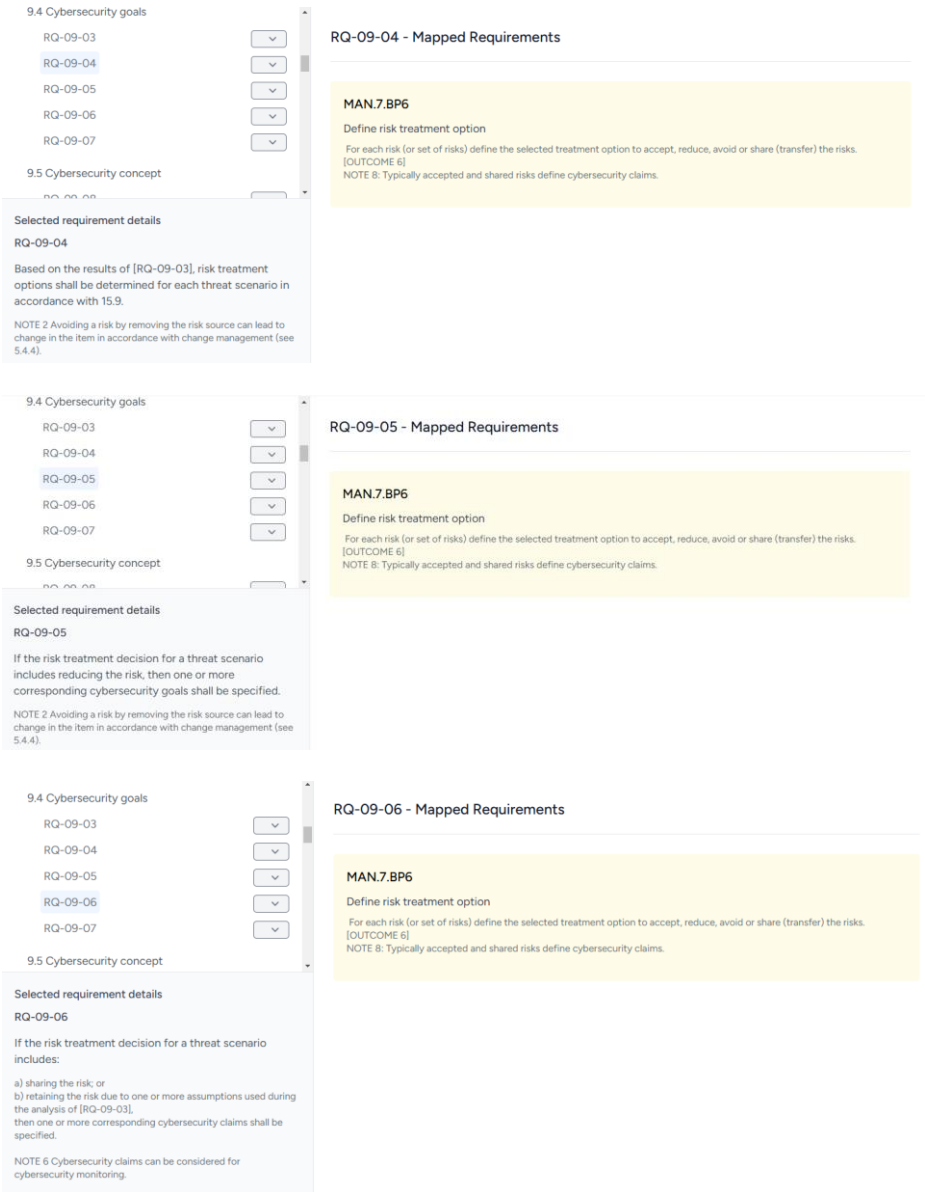


Fig. 23. Mapping of ISO 21434 Requirements RQ-09-04, RQ-09-05, RQ-09-06

Requirement RQ-09-06 addresses situations where the risk treatment decision involves sharing the risk or retaining the risk due to certain assumptions made during the analysis in RQ-09-03. In such cases, one or more corresponding cybersecurity claims must be specified. Cybersecurity claims are statements that acknowledge the acceptance or

BUPT

transfer of certain risks based on specific assumptions or external factors. These claims serve as documentation of the organization's rationale for accepting or sharing the risk and can be important for ongoing cybersecurity monitoring. The note mentions that cybersecurity claims can be considered for cybersecurity monitoring, emphasizing the need to keep track of these decisions and revisit them as necessary.

The ASPICE for Cybersecurity base practice MAN.7.BP6 aligns closely with these ISO requirements by providing a structured approach to defining risk treatment options. MAN.7.BP6 requires that for each identified risk or set of risks, organizations must define the selected treatment option—whether to accept, reduce, avoid, or share (transfer) the risks. This practice ensures that all risks are addressed systematically and that decisions are made transparently. The accompanying note clarifies that typically accepted and shared risks define cybersecurity claims, directly correlating with the requirements of ISO RQ-09-06.

The alignment between the ISO requirements and the ASPICE base practice is evident in their shared emphasis on a methodical approach to risk treatment. Both frameworks recognize the importance of specifying cybersecurity goals when the decision is to reduce risks. This ensures that there are clear targets for security measures and that the organization is proactive in mitigating risks. Similarly, both frameworks underscore the necessity of defining cybersecurity claims when risks are accepted or shared. This practice provides accountability and facilitates communication among stakeholders regarding the organization's risk posture. By adhering to these requirements, organizations establish a robust cybersecurity risk management process that not only addresses existing risks but also adapts to new threats as they emerge. The integration of ISO 21434's detailed guidance on risk treatment with ASPICE's structured process approach ensures that organizations can effectively manage cybersecurity risks throughout the development lifecycle of automotive systems. This alignment fosters a cohesive and comprehensive cybersecurity strategy, ultimately contributing to the protection of stakeholders and the enhancement of overall system security.

Mapping of ISO 21434 Requirement RQ-09-07

ISO 21434 Requirement RQ-09-07 emphasizes the critical importance of verifying the outcomes of the Threat Analysis and Risk Assessment (TARA) process to ensure the integrity and effectiveness of cybersecurity measures in automotive systems. This requirement mandates a comprehensive verification to confirm the correctness and completeness of the TARA results with respect to the item definition. It also requires the verification of the completeness, correctness, and consistency of the risk treatment decisions in relation to the TARA results. Furthermore, it calls for the verification of the completeness, correctness, and consistency of the cybersecurity goals and cybersecurity claims concerning the risk treatment decisions. Lastly, it insists on ensuring the consistency of all cybersecurity goals and claims for the item as a whole.

In the context of ASPICE for Cybersecurity, this verification requirement does not have a direct equivalent within the MAN.7 Cybersecurity Risk Management process. While MAN.7 focuses on identifying, analyzing, and treating cybersecurity risks, it does not explicitly address the verification activities outlined in ISO RQ-09-07. However, the necessary verification processes are comprehensively covered by the SUP.1

BUPT

Quality Assurance process, which is part of the ASPICE Process Assessment Model (PAM) in versions 3.1 and 4.0. The SUP.1 Quality Assurance process ensures that all processes and work products meet the defined requirements and quality standards set by the organization and relevant industry standards. It involves planning and performing quality assurance activities, independently verifying work products and processes, ensuring compliance with standards and procedures, and documenting and communicating findings. By incorporating SUP.1 into the cybersecurity risk management activities, organizations can fulfill the verification requirements of ISO RQ-09-07 effectively. Through the implementation of SUP.1, organizations can conduct thorough verifications to confirm that the TARA results are accurate and complete in relation to the item definition. They can ensure that the risk treatment decisions are comprehensive, correct, and consistent with the TARA results. Additionally, they can verify that the cybersecurity goals and claims are fully aligned with the risk treatment decisions and that all cybersecurity goals and claims for the item are consistent.

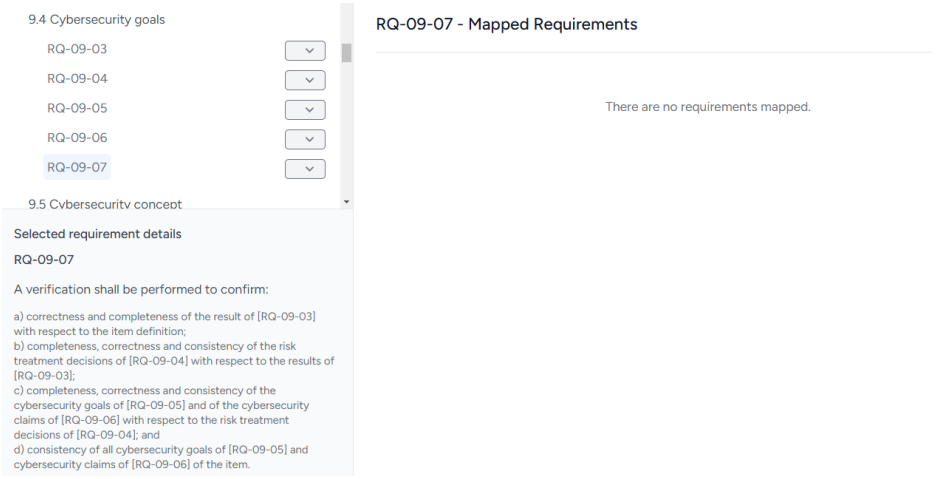


Fig. 24. Mapping of ISO 21434 Requirement RQ-09-07

In conclusion, while the MAN.7 process in ASPICE for Cybersecurity does not explicitly cover the verification activities required by ISO 21434 Requirement RQ-09-07, these activities are effectively addressed within the SUP.1 Quality Assurance process of the ASPICE framework. By implementing the SUP.1 process, organizations can ensure that all aspects of the cybersecurity risk management process—including the TARA results, risk treatment decisions, cybersecurity goals, and claims—are thoroughly verified for correctness, completeness, and consistency. This alignment not only satisfies the ISO requirement but also contributes to a robust and reliable cybersecurity framework within automotive systems, ultimately enhancing the protection of stakeholders and the resilience of the product against cybersecurity threats.

BUPT

Cybersecurity Concept (9.5)

Mapping Between ISO 21434 Requirement RQ-09-08 and ASPICE for Cybersecurity Base Practice SEC.2.BP3

ISO 21434 Requirement RQ-09-08 mandates that technical and operational cybersecurity controls, along with their interactions necessary to achieve the cybersecurity goals, must be thoroughly described. This description should take into account dependencies between the item's functions and any existing cybersecurity claims. The requirement emphasizes that the description can include conditions for achieving cybersecurity goals, such as prevention of compromise or detection and monitoring mechanisms, and functions dedicated to addressing specific threat scenarios, like the implementation of secure communication channels. This detailed description serves not only to evaluate designs but also to determine targets for cybersecurity validation. This requirement highlights the necessity for organizations to identify and articulate how specific controls will work together to meet the established cybersecurity goals. By considering dependencies between functions, organizations ensure that the controls are integrated seamlessly into the item's architecture, effectively mitigating risks without introducing new vulnerabilities. The inclusion of cybersecurity claims acknowledges situations where certain risks are accepted or shared, and how controls relate to these decisions.

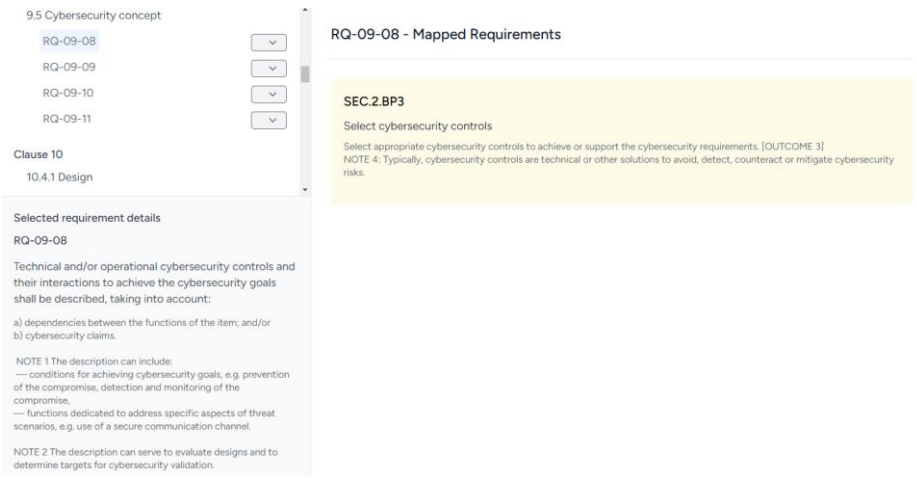


Fig. 25. Mapping of ISO 21434 Requirement RQ-09-08

In alignment with this ISO requirement, the ASPICE for Cybersecurity base practice SEC.2.BP3 focuses on the selection of appropriate cybersecurity controls to achieve or support the cybersecurity requirements. This practice recognizes that cybersecurity controls are typically technical or other solutions designed to avoid, detect, counteract, or mitigate cybersecurity risks. By selecting controls that directly address the identified

BUPT

risks and support the cybersecurity requirements, organizations can implement effective measures to protect the system.

The mapping between ISO RQ-09-08 and ASPICE SEC.2.BP3 is evident in their shared emphasis on not just selecting cybersecurity controls, but also ensuring these controls are appropriate and effective in achieving cybersecurity goals. Both standards underscore the importance of a deliberate and methodical approach to control selection, considering how each control interacts with others and contributes to the overall security posture. ISO RQ-09-08's requirement to describe the interactions of controls and consider dependencies aligns with ASPICE SEC.2.BP3's focus on selecting controls that support the cybersecurity requirements. In practice, this means that during the control selection process, organizations must evaluate how each control fits within the system's architecture, how it interacts with other controls, and how it affects or is affected by other system functions. This holistic approach ensures that the implementation of controls is coherent and that all aspects of the system work synergistically to maintain security. Furthermore, the ISO requirement's note that the description can include conditions for achieving cybersecurity goals, such as prevention or detection mechanisms, resonates with the ASPICE practice's recognition that controls are solutions to avoid, detect, counteract, or mitigate risks. Both standards acknowledge that effective cybersecurity involves a range of strategies, from preventative measures to detection and response capabilities.

By adhering to ISO RQ-09-08, organizations ensure that they have a comprehensive understanding of how their chosen controls will achieve the cybersecurity goals. This involves not only selecting appropriate controls but also documenting their interactions and dependencies, which is crucial for evaluating designs and setting validation targets. ASPICE SEC.2.BP3 complements this by providing a structured process for selecting these controls, ensuring they are suitable and effective for the specific cybersecurity requirements identified. In conclusion, ISO 21434 Requirement RQ-09-08 and ASPICE for Cybersecurity base practice SEC.2.BP3 are closely aligned in promoting a thorough and systematic approach to implementing cybersecurity controls. Both emphasize the importance of understanding the relationships and interactions between controls and system functions to achieve cybersecurity objectives effectively. By integrating these practices, organizations can enhance their cybersecurity posture, ensuring that controls are not only appropriately selected but also effectively integrated into the system to mitigate risks and protect against threats.

Mapping Between ISO 21434 Requirement RQ-09-09 and ASPICE for Cybersecurity Base Practices SEC.1.BP1, SEC.1.BP2, SEC.1.BP3, SEC.1.BP4

ISO 21434 Requirement RQ-09-09 mandates that cybersecurity requirements for both the item and its operational environment must be defined to achieve the cybersecurity goals as described in RQ-09-08. This requirement recognizes that cybersecurity goals cannot be met by focusing solely on the item in isolation; instead, it necessitates a holistic approach that includes the operational environment in which the item functions. The cybersecurity requirements may depend on or include specific features of the item, such as update capabilities or the ability to obtain user consent during operations. Additionally, requirements on the operational environment are realized outside of the item

BUPT

but are included in the cybersecurity validation to confirm whether the corresponding cybersecurity goals are achieved. Requirements on other items within the operational environment can also be considered as cybersecurity requirements for those items. This ISO requirement aligns closely with several ASPICE for Cybersecurity base practices within the SEC.1 process, specifically SEC.1.BP1 through SEC.1.BP4. SEC.1.BP1 focuses on deriving cybersecurity goals and cybersecurity requirements. It mandates that organizations derive cybersecurity goals for threat scenarios where the risk treatment decision requires risk reduction. Furthermore, it requires the specification of both functional and non-functional cybersecurity requirements for these goals, including criteria for their achievement. This practice ensures that all necessary requirements are identified and defined in alignment with the cybersecurity goals, reflecting the ISO's emphasis on comprehensive requirement definition.

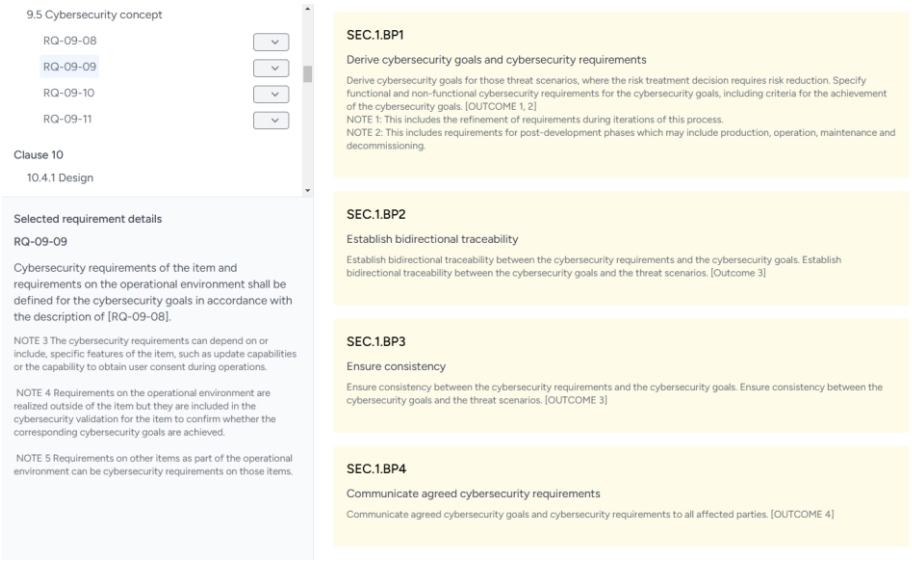


Fig. 26. Mapping of ISO 21434 Requirement RQ-09-09

Additionally, SEC.1.BP1 acknowledges that this process includes the refinement of requirements during iterative cycles, which is crucial as new information emerges or as the item evolves. It also encompasses requirements for post-development phases, such as production, operation, maintenance, and decommissioning. This broad scope aligns with the ISO requirement's consideration of requirements that depend on specific item features and operational phases. SEC.1.BP2 involves establishing bidirectional traceability between the cybersecurity requirements and the cybersecurity goals, as well as between the cybersecurity goals and the threat scenarios. This traceability is essential for ensuring that all requirements are directly linked to the goals they aim to achieve and the threats they intend to mitigate. It enables organizations to verify that each

BUPT

cybersecurity goal is supported by appropriate requirements and that no threats are left unaddressed. This practice aligns with the ISO's emphasis on defining requirements in accordance with the cybersecurity goals and ensuring that they collectively contribute to achieving those goals. SEC.1.BP3 focuses on ensuring consistency between the cybersecurity requirements and the cybersecurity goals, and between the cybersecurity goals and the threat scenarios. This consistency check is vital to identify and resolve any discrepancies or conflicts that could undermine the effectiveness of the cybersecurity measures. By maintaining consistency, organizations can ensure that their cybersecurity strategy is coherent and that all components work synergistically towards mitigating identified risks. This practice directly supports the ISO requirement's objective of defining requirements that are consistent with the cybersecurity goals and the overall security strategy. Finally, SEC.1.BP4 emphasizes the importance of communicating the agreed-upon cybersecurity goals and requirements to all affected parties. Effective communication ensures that everyone involved in the development, deployment, and operation of the item is aware of the cybersecurity objectives and their roles in achieving them. This includes stakeholders responsible for aspects of the operational environment, which the ISO requirement highlights as essential for validating the achievement of cybersecurity goals. By disseminating this information, organizations foster collaboration and coordination across different teams and disciplines, which is crucial for the successful implementation of cybersecurity measures.

In conclusion, ISO 21434 Requirement RQ-09-09 and ASPICE for Cybersecurity base practices SEC.1.BP1 through SEC.1.BP4 are closely aligned in their approach to defining and managing cybersecurity requirements. Both emphasize the necessity of establishing comprehensive requirements that address both the item and its operational environment to achieve cybersecurity goals. The ASPICE practices provide a structured methodology for deriving requirements, ensuring traceability and consistency, and facilitating effective communication among stakeholders. This alignment ensures that organizations can effectively translate cybersecurity goals into actionable requirements, thereby enhancing the security posture of the item and its operational environment and ultimately protecting against cybersecurity threats.

Mapping Between ISO 21434 Requirement RQ-09-10 and ASPICE for Cybersecurity Base Practices SEC.2.BP2, SEC.2.BP3

ISO 21434 Requirement RQ-09-10 emphasizes the necessity of allocating cybersecurity requirements to the item in question and, if applicable, to its individual components. This allocation ensures that every part of the system is assigned specific security responsibilities, facilitating a comprehensive defense against potential cyber threats. The accompanying note highlights that the description of cybersecurity controls complements both the specification and allocation of these requirements, as well as any requirements on the operational environment. Together, these elements form the cybersecurity concept, which serves as the foundational framework guiding the implementation of cybersecurity measures within the item.

BUPT

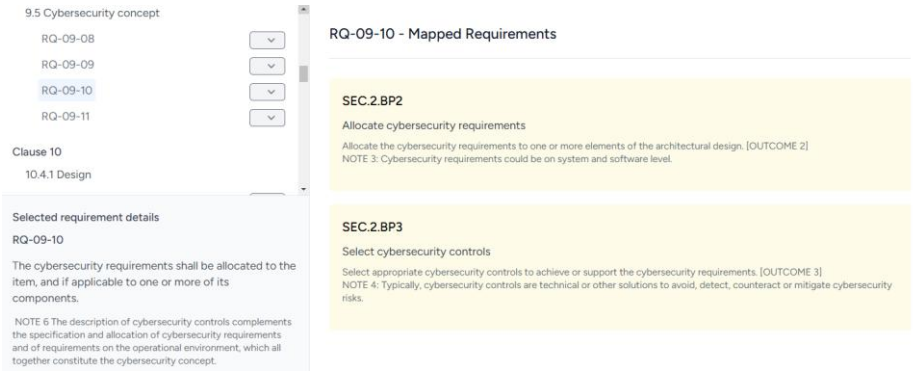


Fig. 27. Mapping of ISO 21434 Requirement RQ-09-10

Aligning with this ISO requirement, the ASPICE for Cybersecurity base practice SEC.2.BP2 focuses on the allocation of cybersecurity requirements to elements of the architectural design. This practice ensures that cybersecurity considerations are integrated into the system's architecture from the outset. By assigning specific requirements to particular components—whether at the system or software level—organizations can systematically address potential vulnerabilities and ensure that each component contributes to the overall cybersecurity objectives. Further complementing this process, SEC.2.BP3 involves selecting appropriate cybersecurity controls to achieve or support the allocated cybersecurity requirements. Cybersecurity controls are the technical or procedural solutions implemented to avoid, detect, counteract, or mitigate cybersecurity risks. By carefully selecting controls that align with the specific requirements of each component, organizations can effectively address identified threats and vulnerabilities. This targeted approach enhances the system's resilience and ensures that the cybersecurity measures are both efficient and effective.

The mapping between ISO RQ-09-10 and ASPICE SEC.2.BP2 and SEC.2.BP3 is evident in their shared emphasis on not only identifying cybersecurity requirements but also ensuring their practical implementation within the system's architecture. Both frameworks recognize that it is insufficient to merely define cybersecurity requirements; these requirements must be systematically assigned and implemented through appropriate controls within the system's components. This alignment underscores the importance of a cohesive cybersecurity concept. By allocating requirements and selecting corresponding controls, organizations create a comprehensive strategy that addresses cybersecurity at every level of the system. This approach ensures that all potential entry points for cyber threats are secured and that the system's components work together to maintain the integrity, confidentiality, and availability of the system.

Moreover, this methodology facilitates better communication and understanding among stakeholders involved in the system's development and maintenance. Clear allocation of requirements and controls helps delineate responsibilities, making it easier for teams to collaborate and for management to oversee the cybersecurity efforts effectively. In conclusion, ISO 21434 Requirement RQ-09-10 and ASPICE for

BUPT

Cybersecurity base practices SEC.2.BP2 and SEC.2.BP3 are closely aligned in promoting a systematic and integrated approach to cybersecurity. Both emphasize the critical steps of allocating cybersecurity requirements to specific components of the system and selecting appropriate controls to fulfill these requirements. This alignment ensures that organizations can develop a robust cybersecurity concept, effectively safeguarding the system against potential cyber threats and enhancing overall security posture.

Mapping Between ISO 21434 Requirement RQ-09-11 and ASPICE for Cybersecurity Base Practice SEC.1.BP3

ISO 21434 Requirement RQ-09-11 emphasizes the critical need to verify the outcomes of the cybersecurity concept development process to ensure they are fully aligned with the established cybersecurity goals and claims. Specifically, it mandates that the results from RQ-09-08 (description of cybersecurity controls), RQ-09-09 (definition of cybersecurity requirements), and RQ-09-10 (allocation of cybersecurity requirements) must be thoroughly verified. This verification process aims to confirm the completeness, correctness, and consistency of these results concerning the cybersecurity goals, as well as ensuring consistency with the cybersecurity claims. This requirement underscores the importance of a rigorous validation step in the cybersecurity development lifecycle. By verifying the completeness and correctness, organizations ensure that all necessary cybersecurity controls and requirements have been identified and accurately reflect what is needed to achieve the cybersecurity goals. Consistency checks guarantee that there are no contradictions or misalignments between the controls, requirements, goals, and claims, which could otherwise lead to vulnerabilities or ineffective security measures.

In alignment with this ISO requirement, the ASPICE for Cybersecurity base practice SEC.1.BP3 focuses on ensuring consistency between the cybersecurity requirements and the cybersecurity goals, as well as between the cybersecurity goals and the threat scenarios. This practice involves a systematic review process where the derived cybersecurity requirements are checked against the cybersecurity goals to confirm that they adequately address the intended security objectives. It also involves ensuring that the cybersecurity goals themselves are consistent with the identified threat scenarios, meaning that all significant threats have corresponding goals aimed at mitigating them. By implementing SEC.1.BP3, organizations engage in a detailed examination of their cybersecurity requirements and goals, verifying that the requirements are not only aligned but also sufficient to meet the goals. This practice directly supports the ISO requirement's emphasis on verifying completeness and correctness, as it helps identify any gaps where requirements may be missing or insufficient. Additionally, by ensuring consistency, SEC.1.BP3 aids in detecting any discrepancies or conflicts that could compromise the effectiveness of the cybersecurity measures.

BUPT

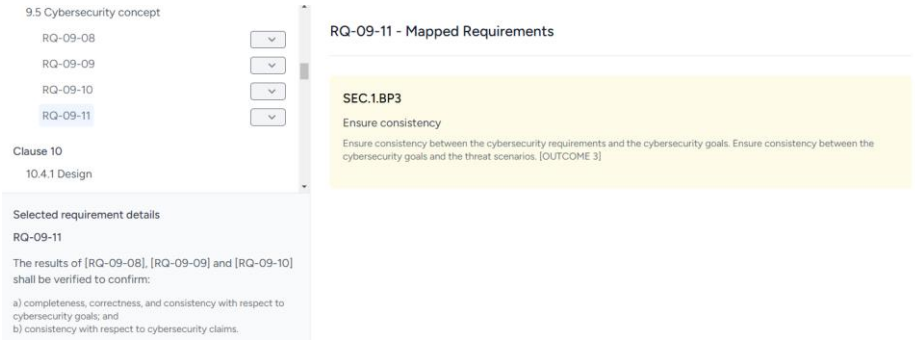


Fig. 28. Mapping of ISO 21434 Requirement RQ-09-11

Furthermore, the aspect of verifying consistency with respect to cybersecurity claims, as required by ISO RQ-09-11, is inherently supported by SEC.1.BP3's focus on alignment between goals, requirements, and threat scenarios. Cybersecurity claims often stem from accepted risks or assumptions made during the risk assessment process. Ensuring that these claims are consistent with the cybersecurity goals and requirements means that any accepted risks are appropriately acknowledged and managed within the overall security strategy.

In conclusion, ISO 21434 Requirement RQ-09-11 and ASPICE for Cybersecurity base practice SEC.1.BP3 are closely aligned in promoting a rigorous verification process to ensure the effectiveness of the cybersecurity concept. Both emphasize the necessity of confirming that the cybersecurity controls, requirements, goals, and claims are complete, correct, and consistent with one another. By adhering to these practices, organizations can enhance the integrity of their cybersecurity strategies, ensuring that all measures are properly aligned to protect against identified threats and achieve the desired security outcomes. This thorough verification is essential for developing robust automotive systems capable of withstanding the complex cybersecurity challenges present in today's connected vehicle landscape.

3.3 Mapping of Clause 10

Clause 10 of ISO/SAE 21434 focuses on the product development phase of cybersecurity engineering within the automotive industry. This clause outlines the processes involved in specifying cybersecurity requirements and developing the architectural design, as detailed in section 10.4.1. It also describes the integration and verification activities essential for ensuring that the implemented cybersecurity measures meet the defined specifications, as covered in section 10.4.2.

BUPT

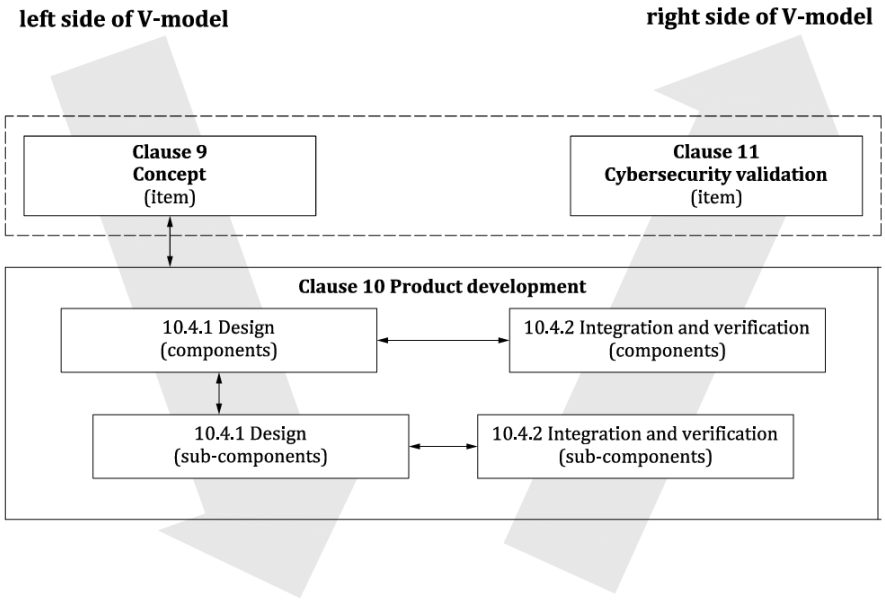


Fig. 29. V-Cycle Product Development Activities [6]

In this phase, cybersecurity activities are performed iteratively until no further refinements of cybersecurity controls are necessary. The cybersecurity specifications are established and confirmed through verification activities to fulfill the cybersecurity concept defined in earlier stages. Figure 29 [6]illustrates an example of how product development activities can be applied using a V-model-based workflow. In this model, section 10.4.1 corresponds to the left side of the V-model, emphasizing design and specification, while section 10.4.2 corresponds to the right side, focusing on implementation, integration, and verification. The example assumes two layers of abstraction beneath the item level—component level and sub-component level—but this workflow can be extended to cover any level of abstraction as required.

The objectives of Clause 10 are to define cybersecurity specifications, which may include the specification of cybersecurity-related components not present in the existing architectural design; to verify that the defined cybersecurity specifications conform to those from higher levels of architectural abstraction; to identify weaknesses in components (noting that vulnerability analysis and management are described in Clause 8); and to provide evidence that the results of the implementation and integration of components conform to the cybersecurity specifications.

In this chapter, the requirements related to Clause 10 are mapped to the corresponding base practices in ASPICE for Cybersecurity. This mapping provides a structured framework for integrating the product development activities prescribed by ISO/SAE 21434 with the process assessment model of ASPICE for Cybersecurity. By aligning these requirements and practices, organizations can systematically incorporate cybersecurity considerations throughout the product development lifecycle, ensuring that automotive systems are both robust and secure against cyber threats.

BUPT

Design (10.4.1)

Mapping Between ISO 21434 Requirement RQ-10-01 and ASPICE for Cybersecurity Base Practices SEC.2.BP1, SEC.2.BP4, SEC.2.BP6.

ISO 21434 Requirement RQ-10-01 mandates that cybersecurity specifications must be defined based on several key elements: cybersecurity specifications from higher levels of architectural abstraction, the cybersecurity controls selected for implementation if applicable, and the existing architectural design if applicable. This requirement underscores the importance of integrating cybersecurity considerations into the architectural design process, ensuring that security measures are built into the system from the outset rather than being added later. The requirement elaborates that cybersecurity specifications should include detailed descriptions of interfaces between sub-components related to fulfilling cybersecurity requirements, covering their usage as well as static and dynamic aspects. It also suggests considering the cybersecurity implications of post-development phases, such as secure management of key stores, deactivation of debug interfaces, and procedures to delete personally identifiable information. Furthermore, the specifications may include identifying configuration and calibration parameters crucial for fulfilling cybersecurity requirements, along with their settings or permitted value ranges—for instance, correctly configuring a hardware security module. The capability of components necessary to implement the cybersecurity controls, like processor performance and memory resources, should also be taken into account.

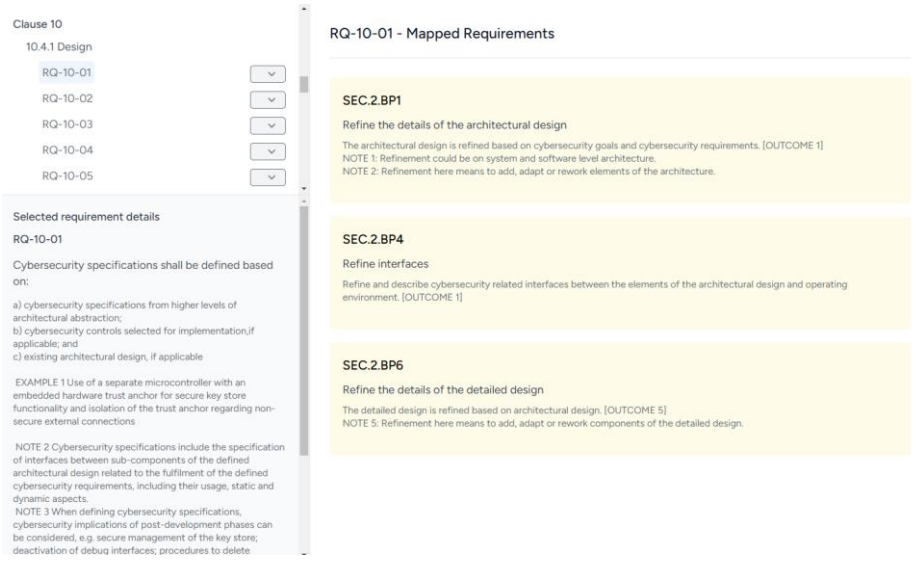


Fig. 30. Mapping of ISO 21434 Requirement RQ-10-01

BUPT

Aligning with this ISO requirement, the ASPICE for Cybersecurity base practices SEC.2.BP1, SEC.2.BP4, and SEC.2.BP6 provide a structured approach to refining both the architectural and detailed designs based on cybersecurity considerations. SEC.2.BP1 focuses on refining the details of the architectural design in light of cybersecurity goals and requirements. This refinement involves adding, adapting, or reworking elements of the architecture at both the system and software levels. By integrating cybersecurity goals and requirements into the architectural design, organizations ensure that security is embedded into the system's foundation, which resonates with the ISO's emphasis on utilizing higher-level specifications and existing architectures.

SEC.2.BP4 extends this refinement by specifically addressing the refinement and description of cybersecurity-related interfaces between elements of the architectural design and the operating environment. This practice ensures that all interfaces are thoroughly analyzed and defined concerning their security implications, directly aligning with RQ-10-01's requirement to specify interfaces between sub-components. By considering both static and dynamic aspects of these interfaces, organizations can anticipate potential vulnerabilities and ensure secure interactions between components. SEC.2.BP6 focuses on refining the details of the detailed design based on the architectural design. This involves adding, adapting, or reworking components of the detailed design to incorporate cybersecurity measures. By refining the detailed design, organizations can address specific implementation aspects of cybersecurity controls, such as selecting appropriate hardware with sufficient processor performance and memory resources or configuring software components to meet security requirements. This aligns with RQ-10-01's emphasis on considering the capabilities of components necessary to implement cybersecurity controls and identifying relevant configuration parameters. Together, these ASPICE practices ensure that cybersecurity specifications are thoroughly integrated into both the architectural and detailed designs of the system. They promote a cohesive approach where cybersecurity considerations influence every layer of the design process, from high-level architecture to component-level details. This comprehensive integration is essential for developing robust cybersecurity controls that effectively mitigate risks identified during the threat analysis and risk assessment phases.

By adhering to these practices, organizations can also address the ISO requirement's notes on considering the cybersecurity implications of post-development phases. For example, refining the design to include secure key management or procedures for deleting personally identifiable information ensures that security is maintained throughout the system's lifecycle. Additionally, by refining interfaces and configurations, organizations can ensure that the system is prepared to handle future updates and changes without compromising security. In conclusion, ISO 21434 Requirement RQ-10-01 and the ASPICE for Cybersecurity base practices SEC.2.BP1, SEC.2.BP4, and SEC.2.BP6 are closely aligned in their objectives to integrate cybersecurity into the system design comprehensively. The ASPICE practices provide a clear methodology for refining architectural and detailed designs based on cybersecurity goals and requirements, ensuring that the resulting specifications meet the ISO's criteria for thoroughness and effectiveness. This alignment enables organizations to develop secure automotive systems

BUPT

that are resilient against cyber threats and compliant with industry standards, ultimately protecting stakeholders and enhancing the trustworthiness of automotive products.

Mapping Between ISO 21434 Requirement RQ-10-02 and ASPICE for Cybersecurity Base Practice SEC.2.BP2

ISO 21434 Requirement RQ-10-02 mandates that the defined cybersecurity requirements must be allocated to components of the architectural design. This requirement emphasizes the critical importance of integrating cybersecurity considerations directly into the system's architecture. By allocating specific security requirements to individual components, organizations ensure that each part of the system is designed with security in mind, contributing to a cohesive and comprehensive defense against potential cyber threats. This allocation process is essential for establishing a robust cybersecurity framework, as it ensures that all components collectively work towards fulfilling the overarching cybersecurity goals.

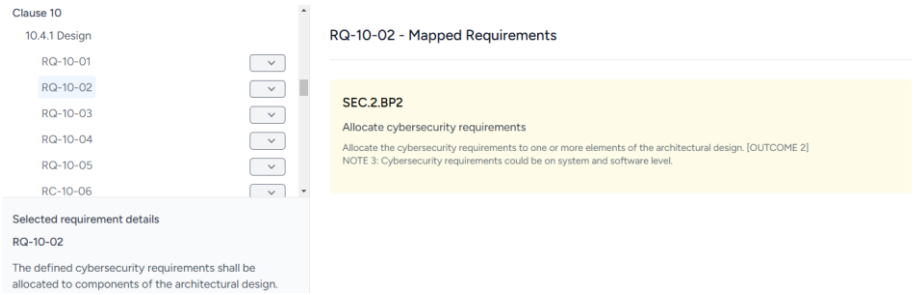


Fig. 31. Mapping of ISO 21434 Requirement RQ-10-02

This ISO requirement aligns closely with the ASPICE for Cybersecurity base practice SEC.2.BP2, which focuses on the allocation of cybersecurity requirements to one or more elements of the architectural design. This practice involves a deliberate and systematic approach to assigning cybersecurity requirements to specific architectural elements at both the system and software levels. By doing so, organizations can address security considerations at every layer of the system, ensuring that both hardware and software components are equipped to mitigate identified risks. The note accompanying SEC.2.BP2 highlights that cybersecurity requirements could be on the system level, dealing with hardware and infrastructure, or on the software level, addressing applications and code. The mapping between ISO RQ-10-02 and ASPICE SEC.2.BP2 is evident in their shared emphasis on embedding cybersecurity into the architectural design through precise allocation of requirements. Both standards recognize that merely defining cybersecurity requirements is insufficient; these requirements must be thoughtfully distributed across the system's components to be effective. By allocating requirements to specific components, developers can tailor security measures to the unique functionalities and potential vulnerabilities of each component. This targeted approach enhances the overall security posture of the system, as it ensures that security measures

BUPT

are not generic but specifically designed to address the risks associated with each component.

In addition, both the ISO requirement and the ASPICE practice underscore the importance of considering both system-level and software-level components in the allocation process. Cybersecurity threats can exploit vulnerabilities at any level of the system architecture. By ensuring that requirements are allocated across all levels, organizations can build layered defenses that provide comprehensive protection. This approach aligns with the defense-in-depth strategy commonly advocated in cybersecurity practices, where multiple layers of security controls are implemented to protect against a wide range of threats.

In conclusion, ISO 21434 Requirement RQ-10-02 and ASPICE for Cybersecurity base practice SEC.2.BP2 are closely aligned in promoting a systematic and integrated approach to cybersecurity within the architectural design of automotive systems. Both emphasize the necessity of allocating cybersecurity requirements to specific components, ensuring that each element of the system contributes to the overall security objectives. This alignment ensures that cybersecurity is not an afterthought but an integral part of the system development process, ultimately leading to more secure and resilient automotive products.

Mapping of ISO 21434 Requirement RQ-10-03

ISO 21434 Requirement RQ-10-03 mandates that procedures to ensure cybersecurity after the development of a component must be specified, if applicable. This requirement recognizes that cybersecurity is an ongoing concern that extends beyond the development phase into integration, production, and operational stages. For example, it calls for procedures that ensure the correct integration and initialization of cybersecurity controls, as well as maintaining cybersecurity measures throughout the production process. This emphasis on post-development activities highlights the importance of sustaining cybersecurity efforts to protect against vulnerabilities that may emerge during later stages of the component's lifecycle.

In the context of ASPICE for Cybersecurity, there is a notable difference. ASPICE primarily focuses on processes leading up to the Start of Production (SOP) and does not explicitly address post-development phases such as production, operation, maintenance, or decommissioning. As a result, there is no direct mapping of ISO 21434 Requirement RQ-10-03 within the ASPICE framework. The ASPICE model concentrates on ensuring that cybersecurity considerations are integrated into the development processes but does not extend its scope to include procedures for maintaining cybersecurity after the component has been developed.

This discrepancy highlights a gap when attempting to align ISO 21434 and ASPICE for Cybersecurity regarding post-development cybersecurity activities. While ISO 21434 advocates for a comprehensive approach that encompasses the entire lifecycle of a component—including development, production, and operation—ASPICE limits its focus to the development phase up to SOP. Therefore, organizations relying solely on ASPICE for their process assessments may not fully address the post-development cybersecurity requirements specified in ISO 21434. To bridge this gap, organizations need to recognize the importance of implementing additional processes or frameworks

BUPT

that cover the post-development stages of a component's lifecycle. This may involve developing specific procedures for the integration and initialization of cybersecurity controls during production, as well as establishing protocols for maintaining and monitoring cybersecurity measures throughout the component's operational life. By doing so, organizations can ensure that they meet the comprehensive requirements of ISO 21434, providing robust cybersecurity protections that extend beyond the initial development phase.

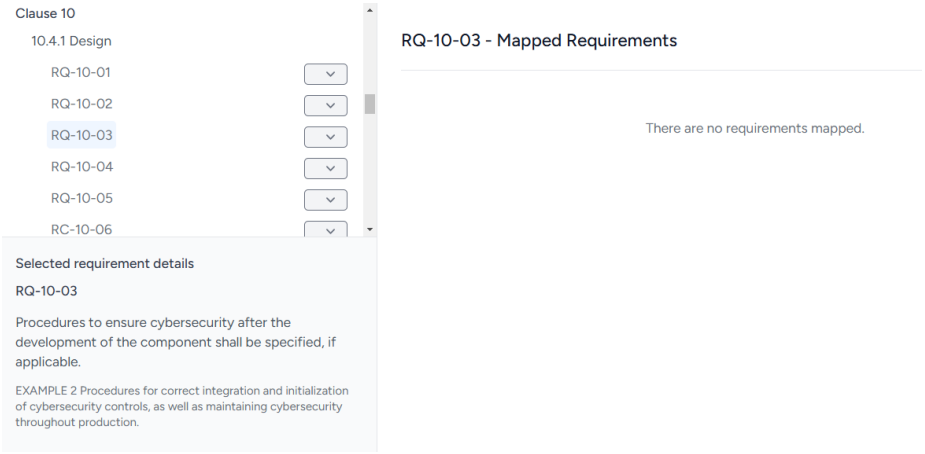


Fig. 32. Mapping of ISO 21434 Requirement RQ-10-03

In conclusion, ISO 21434 Requirement RQ-10-03 underscores the necessity of specifying procedures to maintain cybersecurity after component development, reflecting the ongoing nature of cybersecurity risks. However, ASPICE for Cybersecurity does not directly address this requirement, as its scope concludes with the Start of Production and does not encompass post-development phases. Organizations aiming for full compliance with ISO 21434 should, therefore, supplement their ASPICE-based processes with additional measures that address post-development cybersecurity activities, ensuring comprehensive protection throughout the entire lifecycle of their automotive components.

Mapping Between ISO 21434 Requirement RQ-10-04 and ASPICE for Cybersecurity Base Practices SEC.2.BP1, SEC.2.BP6, SEC.2.BP7

ISO 21434 Requirement RQ-10-04 emphasizes the critical importance of selecting appropriate design, modeling, or programming notations and languages for cybersecurity specifications and their implementation. This requirement mandates that when such notations or languages are used, several key factors must be considered to ensure the effectiveness and security of the resulting system. These factors include an unambiguous and comprehensible definition in both syntax and semantics, support for modularity, abstraction, and encapsulation, the use of structured constructs, support for secure

BUPT

design and implementation techniques, the ability to integrate existing components (such as libraries, frameworks, or software components written in other languages), and resilience against vulnerabilities due to improper use (for example, resilience against buffer overflows). This requirement acknowledges that the choice of notation or language can significantly impact the security and integrity of the system. An unambiguous syntax and semantics ensure that all stakeholders have a clear understanding of the system's behavior, reducing the likelihood of misinterpretation and errors. Support for modularity, abstraction, and encapsulation allows for separation of concerns, making it easier to manage complexity and enhance security by isolating different system components. Structured constructs facilitate the creation of organized and maintainable code, which is essential for identifying and mitigating security vulnerabilities. Support for secure design and implementation techniques enables developers to incorporate security best practices directly into the development process. The ability to integrate existing components allows for leveraging proven solutions, enhancing functionality while maintaining security. Finally, selecting languages that are resilient against vulnerabilities due to improper use helps prevent common security issues such as buffer overflows.

In alignment with this ISO requirement, the ASPICE for Cybersecurity base practices SEC.2.BP1, SEC.2.BP6, and SEC.2.BP7 provide a structured approach to incorporating these considerations into the system development process. SEC.2.BP1 focuses on refining the details of the architectural design based on cybersecurity goals and requirements. This refinement involves adding, adapting, or reworking elements of the architecture at both the system and software levels. By integrating cybersecurity goals into the architectural design, organizations ensure that security considerations are embedded from the earliest stages of development. This practice directly supports the ISO requirement by ensuring that the architectural design is conducive to secure implementation and supports the necessary features such as modularity and abstraction.

SEC.2.BP6 extends this approach to the detailed design phase, refining the components based on the architectural design. This practice ensures that the detailed design accurately reflects the architectural considerations for cybersecurity, further embedding security into the system. It involves careful selection and use of design notations that support secure design principles, structured constructs, and the ability to integrate existing components securely. By refining the detailed design with these factors in mind, organizations can mitigate risks associated with design flaws or vulnerabilities introduced during this phase.

SEC.2.BP7 focuses on the development of software units by implementing the software using appropriate modeling or programming languages. This practice is directly aligned with ISO RQ-10-04's emphasis on selecting suitable programming languages for cybersecurity. It specifies that criteria for appropriate modeling and programming languages for cybersecurity can include the use of language subsets, enforcement of strong typing, and the use of defensive implementation techniques. For example, using a programming language that enforces strong typing can prevent type-related vulnerabilities, while defensive programming techniques can help in detecting and handling unexpected inputs or conditions securely.

BUPT

Additionally, SEC.2.BP7 suggests that utilizing coding guidelines or appropriate development environments can support the defined criteria. Coding guidelines, such as MISRA C for the C programming language, provide a set of best practices and rules aimed at enhancing code safety and security. Development environments that support static code analysis and other security tools can help identify potential vulnerabilities early in the development process.

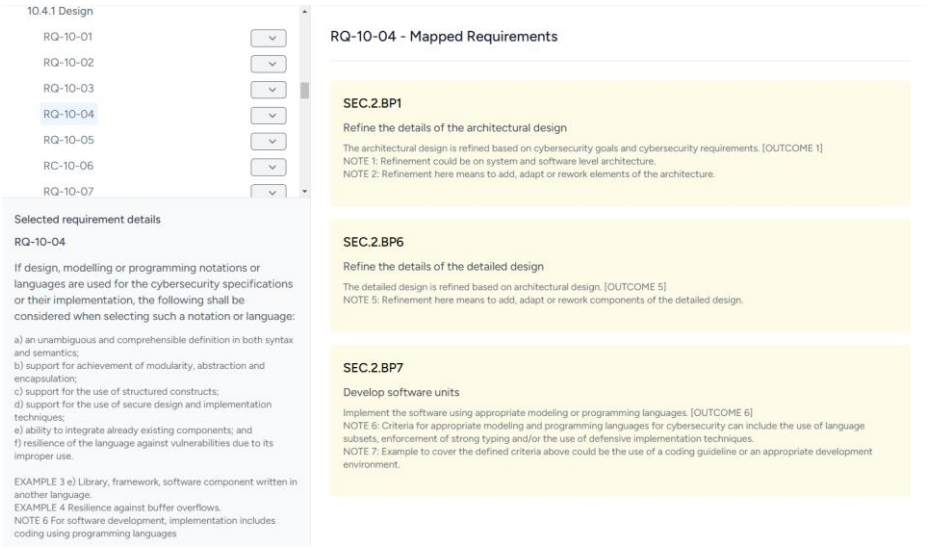


Fig. 33. Mapping of ISO 21434 Requirement RQ-10-04

In conclusion, ISO 21434 Requirement RQ-10-04 and ASPICE for Cybersecurity base practices SEC.2.BP1, SEC.2.BP6, and SEC.2.BP7 are closely aligned in their emphasis on the careful selection and use of design, modeling, and programming notations and languages for cybersecurity purposes. The ASPICE practices provide a structured methodology for refining architectural and detailed designs and for developing software units with appropriate languages that meet the security criteria outlined in the ISO standard. By adhering to these practices, organizations can ensure that their cybersecurity specifications and implementations are robust, secure, and resilient against vulnerabilities, ultimately enhancing the overall security of automotive systems and protecting stakeholders from potential cyber threats.

Mapping of ISO 21434 Requirements RQ-10-05, RC-10-06

ISO 21434 Requirement RQ-10-05 underscores the necessity of addressing criteria for suitable design, modeling, or programming languages for cybersecurity that are not inherently covered by the language itself. This requirement builds upon the previous mandate in RQ-10-04, which emphasizes selecting languages with unambiguous syntax and semantics, support for modularity and abstraction, structured constructs, secure design

BUPT

techniques, integration capabilities for existing components, and resilience against vulnerabilities due to improper use. When a chosen language lacks certain security features or criteria essential for cybersecurity, RQ-10-05 mandates that these gaps must be bridged through design, modeling, and coding guidelines or by utilizing supportive development environments. For example, programming languages like C, which may not enforce strong typing or prevent buffer overflows by default, require the adoption of coding standards such as MISRA C:2012 or CERT C. These guidelines provide a set of rules and best practices that help developers write code that minimizes vulnerabilities and adheres to secure coding principles. Furthermore, the criteria for suitable languages include the use of language subsets to restrict potentially unsafe language features, enforcement of strong typing to prevent type-related errors, and the application of defensive implementation techniques to safeguard against unexpected inputs or states. By incorporating these criteria through external guidelines or development tools, developers can enhance the security posture of their software even when the language itself does not provide built-in safeguards.

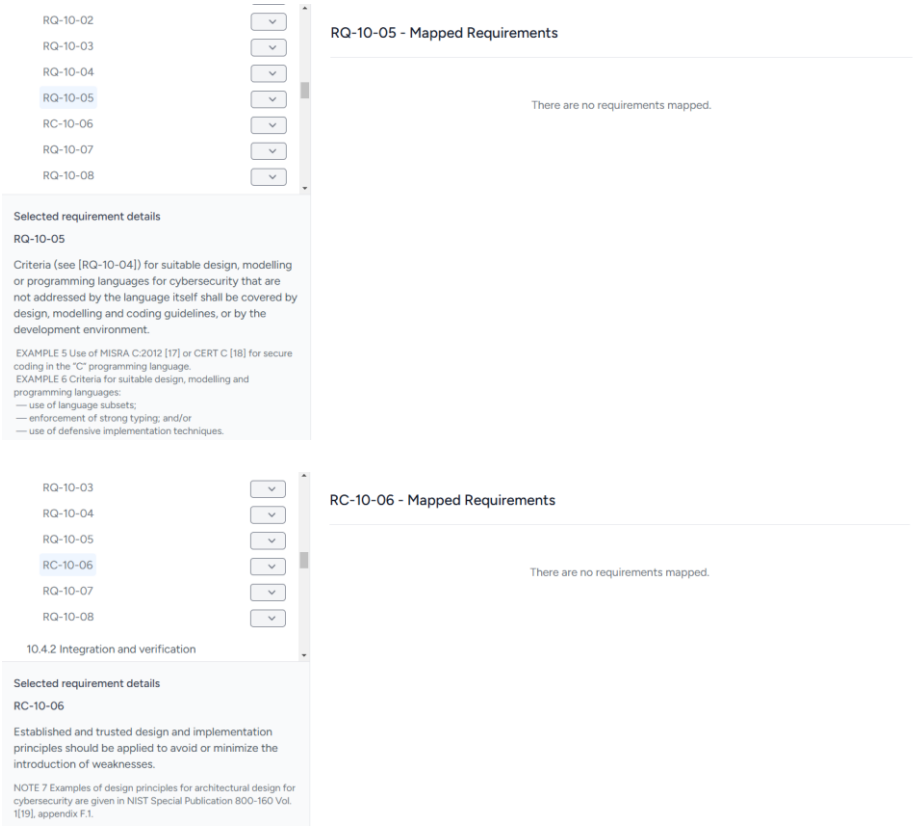


Fig. 34. Mapping of ISO 21434 Requirements RQ-10-05, RC-10-06

BUPT

ISO 21434 Recommendation RC-10-06 complements this requirement by advising that established and trusted design and implementation principles should be applied to avoid or minimize the introduction of weaknesses. This recommendation points to resources like NIST Special Publication 800-160 Vol. 1, which provides comprehensive design principles for architectural design in cybersecurity. Applying such principles helps in creating robust architectures that are resilient to cyber threats and reduce the likelihood of vulnerabilities being introduced during the design phase. In the context of ASPICE for Cybersecurity, there is no direct mapping to these specific ISO requirements regarding coding guidelines and established design principles. ASPICE focuses on process assessment and improvement for software development within the automotive industry, emphasizing the processes and practices rather than prescribing specific technical guidelines or coding standards. While ASPICE includes practices related to refining architectural and detailed designs and developing software units using appropriate modeling or programming languages (as seen in SEC.2.BP1, SEC.2.BP6, and SEC.2.BP7), it does not delve into the specifics of coding guidelines like MISRA C or CERT C, nor does it mandate the application of particular design principles as outlined in ISO RQ-10-05 and RC-10-06.

In conclusion, while ASPICE for Cybersecurity provides a robust framework for assessing and improving software development processes, it does not explicitly address the use of specific coding guidelines or design principles as required by ISO 21434 RQ-10-05 and RC-10-06. Therefore, organizations should proactively incorporate these elements into their cybersecurity practices to ensure comprehensive compliance with ISO 21434. This approach enhances the overall security of automotive systems by ensuring that both the development processes and the technical implementations are aligned with industry best practices for cybersecurity.

Mapping Between ISO 21434 Requirement RQ-10-07 and ASPICE for Cybersecurity Base Practice SEC.2.BP5

ISO 21434 Requirement RQ-10-07 mandates that the architectural design defined in RQ-10-01 must be analyzed to identify weaknesses. This involves a thorough examination of the system's architecture to uncover any potential flaws or vulnerabilities that could compromise cybersecurity. The requirement specifically highlights the importance of considering known weaknesses and vulnerabilities from reused components, acknowledging that integrating existing elements can introduce unforeseen risks. It also notes that identified weaknesses can sometimes be resolved through changes to the architectural design without necessarily performing a full vulnerability analysis, although any identified vulnerabilities should be managed according to the standard's guidelines in sections 8.5 and 8.6. This ISO requirement aligns closely with the ASPICE for Cybersecurity base practice SEC.2.BP5, which focuses on analyzing the architectural design to identify and analyze vulnerabilities. This practice underscores the necessity of systematically reviewing the architectural design to detect potential security issues that could be exploited by malicious actors. By performing such analysis, organizations can proactively address vulnerabilities at an early stage, potentially saving significant time and resources by avoiding later-stage modifications.

BUPT

The mapping between ISO RQ-10-07 and ASPICE SEC.2.BP5 is evident in their shared emphasis on the importance of architectural analysis in ensuring cybersecurity. Both standards recognize that the architectural design serves as the foundation for the system's security posture, and that weaknesses at this level can have far-reaching consequences. By analyzing the architectural design, organizations can identify inherent weaknesses, such as insecure interfaces, inadequate segregation of critical components, or insufficient consideration of threat vectors. Moreover, the ISO requirement's consideration of known weaknesses and vulnerabilities from reused components is mirrored in the ASPICE practice's focus on comprehensive vulnerability analysis. Reused components, whether software libraries, hardware modules, or third-party services, may harbor vulnerabilities that were not apparent in their original context or have emerged over time due to new attack methods. Including these components in the architectural analysis ensures that their integration does not compromise the overall security of the system. Additionally, the ISO requirement acknowledges that some identified weaknesses can be resolved by modifying the architectural design without the need for an extensive vulnerability analysis. This approach aligns with the proactive and iterative nature of the ASPICE process, where continuous improvement and refinement of the design are encouraged to enhance security. By addressing weaknesses through design changes, organizations can mitigate risks more efficiently and effectively.

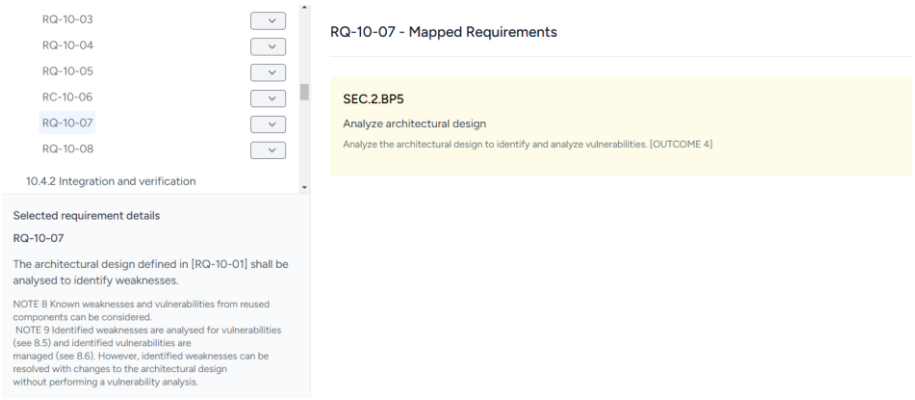


Fig. 35. Mapping of ISO 21434 Requirement RQ-10-07

Furthermore, both the ISO and ASPICE standards emphasize the importance of integrating security analysis into the development lifecycle. By embedding these practices into the architectural design phase, organizations can ensure that security considerations are not an afterthought but a fundamental aspect of the system's development. This integration helps prevent costly redesigns and reduces the likelihood of security issues arising during later stages of development or after deployment. In conclusion, ISO 21434 Requirement RQ-10-07 and ASPICE for Cybersecurity base practice SEC.2.BP5 are closely aligned in their objectives and methodologies. Both advocate

BUPT

for a systematic analysis of the architectural design to identify and address weaknesses and vulnerabilities. This alignment ensures that organizations adopting these standards can effectively enhance their systems' cybersecurity by proactively identifying potential issues and implementing appropriate mitigations at the architectural level.

Mapping Between ISO 21434 Requirement RQ-10-08 and ASPICE for Cybersecurity Base Practice SEC.2.BP9

ISO 21434 Requirement RQ-10-08 mandates that the defined cybersecurity specifications must be verified to ensure their completeness, correctness, and consistency with the cybersecurity specifications from higher levels of architectural abstraction. This verification is crucial to confirm that the cybersecurity measures implemented at various levels align with the overarching cybersecurity goals and that no discrepancies exist between different layers of the system's design. The requirement suggests using methods such as review, analysis, simulation, and prototyping to perform this verification, ensuring a thorough examination of the specifications from multiple perspectives. This ISO requirement aligns closely with the ASPICE for Cybersecurity base practice SEC.2.BP9, which focuses on ensuring consistency between the refined architectural design and the detailed design. This practice is essential to maintain coherence throughout the development process, guaranteeing that the detailed design faithfully implements the architectural intentions, including all cybersecurity considerations. By ensuring consistency between these levels of design, organizations can prevent misalignments that might introduce vulnerabilities or compromise the effectiveness of cybersecurity controls.

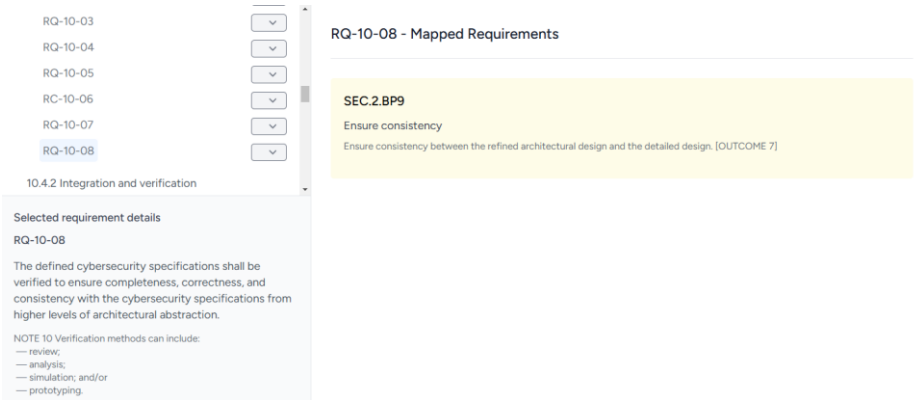


Fig. 36. Mapping of ISO 21434 Requirement RQ-10-08

The mapping between ISO RQ-10-08 and ASPICE SEC.2.BP9 is evident in their shared emphasis on verification and consistency across different abstraction levels in the system's design. Both standards recognize the importance of validating that lower-level designs and specifications accurately reflect and fulfill the requirements and intentions

BUPT

established at higher levels. This alignment ensures that cybersecurity measures are properly integrated and that the system's security posture is robust and coherent. While ISO RQ-10-08 specifically addresses the verification of cybersecurity specifications, ASPICE SEC.2.BP9 encompasses a broader scope by ensuring overall design consistency, which inherently includes cybersecurity aspects. The verification methods suggested by ISO, such as review and analysis, are common practices within the ASPICE framework for validating designs and ensuring they meet the required standards and specifications. It's important to note that although ISO RQ-10-08 could also be mapped to general practices from ASPICE Level 2, such mapping falls outside the scope of this specific discussion. The focus here is on the direct correlation between the ISO requirement and the ASPICE base practice within the context of cybersecurity.

In conclusion, ISO 21434 Requirement RQ-10-08 and ASPICE for Cybersecurity base practice SEC.2.BP9 are closely aligned in promoting thorough verification to ensure that cybersecurity specifications and designs are complete, correct, and consistent with higher-level abstractions. By adhering to these practices, organizations can effectively integrate cybersecurity measures throughout the development process, thereby enhancing the overall security and reliability of automotive systems.

Integration and Verification (10.4.2)

Mapping Between ISO 21434 Requirements RQ-10-09, RQ-10-10 and ASPICE for Cybersecurity Base Practices SEC.3.BP1, SEC.3.BP2

ISO 21434 Requirements RQ-10-09 and RQ-10-10 emphasize the critical importance of integration and verification activities in ensuring that the implementation and integration of components fulfill the defined cybersecurity specifications. RQ-10-09 mandates that these activities must verify the fulfillment of cybersecurity specifications by the components. RQ-10-10 further specifies that the integration and verification activities should consider several factors: the defined cybersecurity specifications, configurations intended for series production if applicable, sufficient capability to support the specified functionalities, and conformity with the modeling, design, and coding guidelines outlined in RQ-10-05. These ISO requirements highlight the necessity of a comprehensive approach to verification and integration, ensuring that cybersecurity measures are effectively implemented and integrated into the final product. The notes accompanying RQ-10-10 provide guidance on methods for verification, including requirements-based testing, interface testing, resource usage evaluation, control flow and data flow verification, dynamic and static analysis. They also suggest considerations for test cases and test environments, such as the level of integration for testing, the need for additional tests during subsequent integration activities, and methods for deriving test cases like analysis of requirements and boundary value analysis.

BUPT

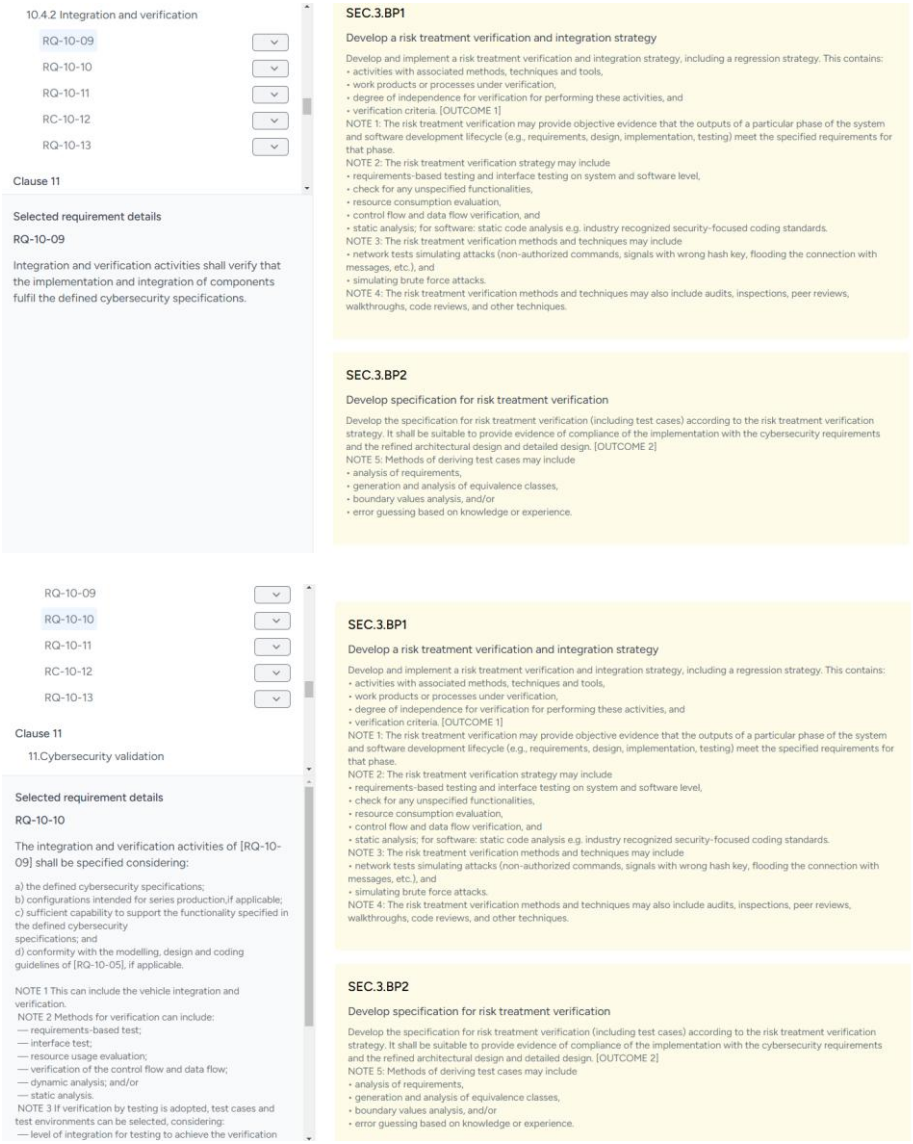


Fig. 37. Mapping of ISO 21434 Requirements RQ-10-09, RQ-10-10

In alignment with these ISO requirements, the ASPICE for Cybersecurity base practices SEC.3.BP1 and SEC.3.BP2 provide a structured framework for developing and implementing a risk treatment verification and integration strategy. SEC.3.BP1 focuses on creating a comprehensive strategy that includes activities with associated methods, techniques, and tools; work products or processes under verification; the degree of independence required for verification activities; and verification criteria. This strategy

BUPT

ensures that verification efforts are well-planned and tailored to provide objective evidence that the outputs of each phase of the system and software development lifecycle meet the specified requirements. SEC.3.BP1's notes elaborate on the types of verification activities that can be included in the strategy, mirroring the methods suggested in ISO RQ-10-10. These activities encompass requirements-based testing, interface testing at both system and software levels, checks for unspecified functionalities, resource consumption evaluation, control flow and data flow verification, and static analysis, including the use of industry-recognized security-focused coding standards. Additionally, the strategy may involve network tests simulating attacks, such as unauthorized commands or flooding, and techniques like audits, inspections, peer reviews, walkthroughs, and code reviews. SEC.3.BP2 builds upon this strategy by developing detailed specifications for risk treatment verification, including test cases, according to the established strategy. The specifications must be suitable to provide evidence of compliance of the implementation with the cybersecurity requirements and the refined architectural and detailed designs. The notes under SEC.3.BP2 recommend methods for deriving test cases that align closely with those suggested in ISO RQ-10-10, such as analysis of requirements, generation and analysis of equivalence classes, boundary value analysis, and error guessing based on knowledge or experience.

The alignment between the ISO requirements and the ASPICE base practices is evident in their shared emphasis on thorough verification and integration activities that are meticulously planned and executed. Both frameworks recognize the importance of considering the defined cybersecurity specifications, ensuring that configurations intended for series production are accounted for, verifying that the system has sufficient capability to support the specified functionalities, and ensuring conformity with modeling, design, and coding guidelines. By following SEC.3.BP1, organizations develop a risk treatment verification and integration strategy that encompasses all necessary activities and specifies the methods and tools to be used. This strategy addresses the need outlined in ISO RQ-10-09 and RQ-10-10 for verification activities that confirm the fulfillment of cybersecurity specifications. The inclusion of regression strategies and considerations for the degree of independence in verification activities further strengthens the robustness of the verification process. SEC.3.BP2 ensures that the specifications for risk treatment verification are detailed and aligned with the overall strategy, providing a clear roadmap for executing verification activities. This practice addresses the ISO's emphasis on specifying integration and verification activities, considering factors such as test case development and selection of test environments.

In conclusion, ISO 21434 Requirements RQ-10-09 and RQ-10-10 and ASPICE for Cybersecurity base practices SEC.3.BP1 and SEC.3.BP2 are closely aligned in promoting a comprehensive and methodical approach to integration and verification in the context of cybersecurity. Both frameworks stress the importance of planning, specifying, and executing verification activities that ensure the implemented components fulfill the defined cybersecurity specifications. By integrating these practices, organizations can enhance their cybersecurity posture, ensuring that their products are secure, reliable, and compliant with industry standards throughout the development lifecycle.

BUPT

Mapping Between ISO 21434 Requirement RQ-10-11 and ASPICE for Cybersecurity Base Practice SEC.3.BP6

ISO 21434 Requirement RQ-10-11 emphasizes the importance of evaluating test coverage when verification by testing is adopted in the cybersecurity context. It mandates that organizations must use defined test coverage metrics to determine the sufficiency of their test activities. This requirement acknowledges that standard test coverage metrics, such as statement coverage for software, may be inadequate for cybersecurity purposes. The unique and complex nature of cybersecurity threats demands more rigorous and specialized testing approaches to ensure that vulnerabilities are effectively identified and mitigated.

The essence of RQ-10-11 lies in ensuring that testing efforts are comprehensive and that the metrics used accurately reflect the extent to which the system has been tested against potential cybersecurity threats. By using appropriate test coverage metrics, organizations can assess whether their testing activities are sufficient to uncover and address security vulnerabilities. This process is crucial for validating that the implemented cybersecurity measures are effective and that the system can withstand cyber-attacks.

In the Automotive SPICE (ASPICE) framework, the corresponding practice is SEC.3.BP6, which focuses on summarizing and communicating the results of risk treatment verification. This practice requires organizations to compile the outcomes of their verification activities and convey them to all affected parties. The summary should provide all necessary information from the risk treatment verification execution, enabling stakeholders to understand the consequences and make informed decisions. By effectively communicating these results, organizations ensure transparency and facilitate collaboration among teams responsible for different aspects of the system's cybersecurity.

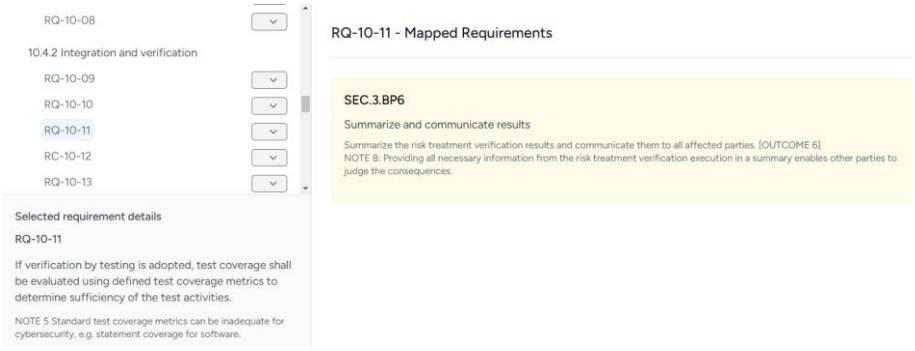


Fig. 38. Mapping of ISO 21434 Requirement RQ-10-11

While ISO RQ-10-11 concentrates on the evaluation of test coverage metrics to determine the sufficiency of test activities, ASPICE SEC.3.BP6 emphasizes the importance of communicating the verification results. There is a complementary relationship between the two: ISO focuses on the quantitative assessment of testing efforts, while ASPICE stresses the qualitative aspect of sharing findings and insights derived from

BUPT

those efforts. However, it is important to note that ASPICE does not explicitly mandate the evaluation of test coverage metrics within the SEC.3.BP6 practice. The ASPICE framework assumes that organizations have established processes for verification activities, including the use of appropriate metrics, but it does not provide detailed guidance on how to evaluate test coverage specifically for cybersecurity. Instead, ASPICE places greater emphasis on the overall process of risk treatment verification and the communication of results. This difference highlights a potential gap between the ISO requirement and the ASPICE practice. While ISO 21434 explicitly requires organizations to assess the sufficiency of their test activities using defined coverage metrics tailored for cybersecurity, ASPICE does not provide a direct equivalent practice that focuses on this quantitative evaluation. Organizations adhering to ASPICE may need to incorporate additional processes or guidelines to ensure compliance with ISO RQ-10-11. To bridge this gap, organizations can integrate the evaluation of test coverage metrics into their risk treatment verification strategy as part of the SEC.3.BP1 and SEC.3.BP2 practices in ASPICE. By doing so, they can define specific metrics suitable for cybersecurity testing and incorporate them into their verification activities. These metrics should go beyond traditional software testing metrics to address the unique challenges of cybersecurity, such as testing for known vulnerabilities, simulating cyberattacks, and assessing the system's resilience under various threat scenarios. Moreover, the results of this comprehensive testing, including the evaluation of test coverage, can then be summarized and communicated as per SEC.3.BP6. This approach ensures that all affected parties are informed not only about the outcomes of the verification activities but also about the extent and adequacy of the testing performed. By providing detailed insights into test coverage, organizations enable stakeholders to understand the confidence level in the system's cybersecurity posture and identify any areas that may require further attention.

In conclusion, ISO 21434 Requirement RQ-10-11 and ASPICE for Cybersecurity practice SEC.3.BP6 address different but related aspects of cybersecurity verification. ISO emphasizes the need for evaluating test coverage using defined metrics to ensure the sufficiency of testing activities in the cybersecurity domain. ASPICE focuses on summarizing and communicating the results of risk treatment verification to stakeholders. While there is no direct mapping of the ISO requirement to an ASPICE practice that specifies test coverage evaluation, organizations can enhance their ASPICE processes by integrating test coverage assessments into their verification strategies. This integration ensures compliance with ISO 21434 and strengthens the overall cybersecurity verification process by combining quantitative evaluation with effective communication of results.

Mapping Between ISO 21434 Recommendation RC-10-12 and ASPICE for Cybersecurity Base Practices SEC.3.BP3, SEC.3.BP4, SEC.3.BP5

ISO 21434 Requirement RC-10-12 emphasizes the critical importance of conducting comprehensive testing to confirm that any remaining unidentified weaknesses and vulnerabilities in a component are minimized. This requirement acknowledges that even after implementing cybersecurity measures, there may still be latent vulnerabilities that could be exploited by malicious actors. The requirement points out that unnecessary

BUPT

functionalities can introduce weaknesses into a system, highlighting the need to scrutinize all aspects of the component. It suggests various testing methods such as functional testing, vulnerability scanning, fuzz testing, and penetration testing as effective means to uncover these hidden vulnerabilities. This requirement aligns closely with the ASPICE for Cybersecurity base practices SEC.3.BP3, SEC.3.BP4, and SEC.3.BP5, which together provide a structured framework for verification activities, ensuring thoroughness and consistency in testing.

The practice SEC.3.BP3 focuses on performing verification activities by verifying identified work products according to a specified strategy to confirm that they meet their specified requirements. This involves testing the implementation of the design and component integration according to the risk treatment verification specification and recording the results and logs. By conducting these verification activities, organizations can systematically identify discrepancies between the implemented components and the cybersecurity specifications, thereby detecting any remaining weaknesses or vulnerabilities. This practice directly supports the intent of ISO RC-10-12 by ensuring that comprehensive testing is conducted to minimize unidentified vulnerabilities in the component.

SEC.3.BP4 emphasizes establishing bidirectional traceability between the cybersecurity requirements and the risk treatment verification specification, including the test cases, as well as between the refined architectural design, detailed design, software units, and the risk treatment verification specification. It also involves establishing traceability between the test cases and the verification results. This bidirectional traceability is crucial for ensuring that every cybersecurity requirement is adequately tested and that the results of these tests are accurately linked back to the requirements and designs. By maintaining this level of traceability, organizations can ensure that all aspects of the component have been examined, supporting coverage, consistency, and impact analysis. This practice aligns with ISO RC-10-12's objective of confirming that unidentified weaknesses and vulnerabilities are minimized through thorough testing.

SEC.3.BP5 focuses on ensuring consistency between the cybersecurity requirements and the risk treatment verification specification, including the test cases, as well as between the refined architectural and detailed designs and the risk treatment verification specification. Consistency here is vital to ensure that the testing activities are directly aligned with the cybersecurity requirements and designs, thereby enhancing the effectiveness of the testing process. By ensuring this consistency, organizations can prevent gaps or overlaps in testing, which might otherwise leave vulnerabilities undetected. This practice supports ISO RC-10-12 by promoting a coherent and focused approach to testing, ensuring that all potential weaknesses are addressed.

BUPT

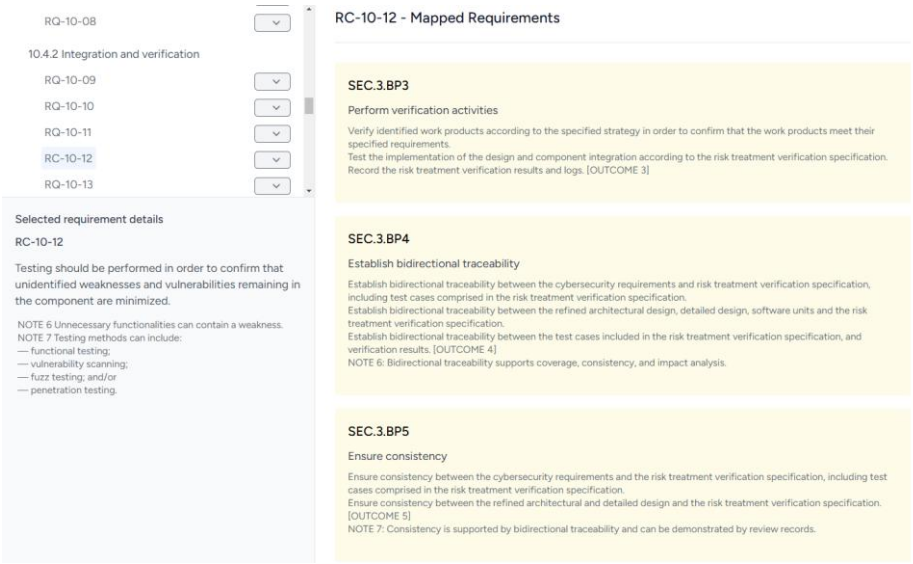


Fig. 39. Mapping of ISO 21434 Requirement RQ-10-12

Together, these ASPICE practices facilitate a comprehensive and methodical approach to testing, which is essential for uncovering and minimizing any remaining vulnerabilities in a component. They encourage the use of various testing methods suggested by ISO RC-10-12, such as functional testing to verify the component's functionality against its specifications; vulnerability scanning to detect known vulnerabilities within the component; fuzz testing to identify how the component handles unexpected or random inputs; and penetration testing to simulate attacks and identify potential exploitation paths. By integrating these testing methods within the structured framework provided by the ASPICE practices, organizations can achieve a high level of confidence in the security of their components. The practices ensure that testing is not only thorough but also effectively managed and documented, enabling organizations to demonstrate due diligence in their cybersecurity efforts.

In conclusion, ISO 21434 Requirement RC-10-12 and ASPICE for Cybersecurity base practices SEC.3.BP3, SEC.3.BP4, and SEC.3.BP5 are closely aligned in their goals and methodologies. Both emphasize the necessity of rigorous testing to uncover and mitigate any residual vulnerabilities in components. By adhering to these practices, organizations can ensure that their components are secure, reliable, and compliant with cybersecurity standards, ultimately enhancing the trustworthiness of automotive systems and protecting stakeholders from potential cyber threats.

Mapping Between ISO 21434 Requirement RQ-10-13 and ASPICE for Cybersecurity Base Practice SEC.3.BP6

ISO 21434 Requirement RQ-10-13 mandates that if the testing activities outlined in RC-10-12 are not performed, a clear and documented rationale must be provided. This

BUPT

requirement recognizes that there may be valid reasons why certain cybersecurity testing methods—such as functional testing, vulnerability scanning, fuzz testing, or penetration testing—are not applicable or feasible for a specific component. The rationale should consider factors such as the feasibility of accessing the component's attack surface, the potential for direct or indirect access in combination with the compromise of other components, and the simplicity or complexity of the component. By providing this rationale, organizations demonstrate due diligence in their cybersecurity efforts and maintain transparency regarding the security posture of their components.

In the context of ASPICE for Cybersecurity, there is no explicit process that directly corresponds to ISO RQ-10-13, as ASPICE does not specifically require providing a rationale when certain cybersecurity tests are not conducted. However, this aspect is effectively covered through the practice of summarizing and communicating risk treatment verification results, as outlined in **SEC.3.BP6**. This practice involves compiling a comprehensive summary of the verification activities and communicating the results to all affected parties. A well-documented test result report, as expected in ASPICE, would include not only the outcomes of the tests performed but also explanations for any deviations from the planned verification activities, including the omission of specific tests.

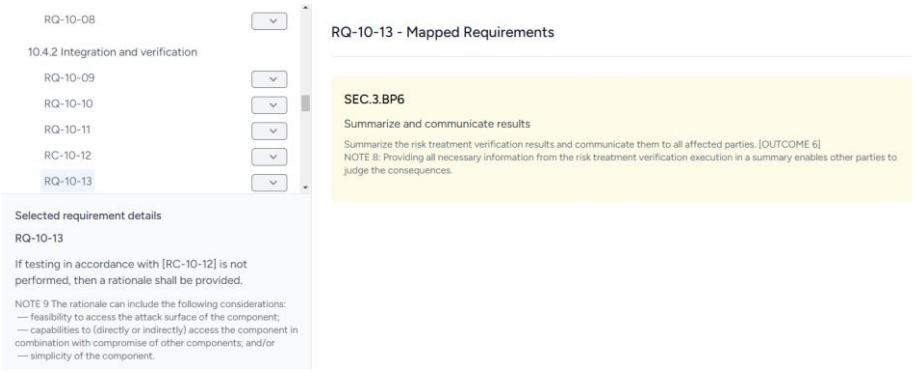


Fig. 40. Mapping of ISO 21434 Requirement RQ-10-13

By providing detailed summaries that include the reasons why certain tests were not performed, organizations ensure that stakeholders are fully informed about the scope and limitations of the verification efforts. This transparency allows for an informed assessment of any residual risks and facilitates decision-making regarding additional measures that may be necessary. Including such rationales in test result documents aligns with the intent of ISO RQ-10-13 by ensuring that any potential gaps in testing are acknowledged and justified. In practice, when adhering to ASPICE SEC.3.BP6, organizations can incorporate explanations for not performing certain cybersecurity tests within their test reports or verification summaries. This approach ensures that the information is captured within the standard documentation processes, maintaining consistency with ASPICE practices while also satisfying the requirements of ISO 21434.

BUPT

By doing so, organizations enhance the completeness and usefulness of their verification summaries, providing stakeholders with a clear understanding of the cybersecurity verification activities and any associated limitations. In conclusion, while ASPICE for Cybersecurity does not have a dedicated base practice that directly mirrors ISO 21434 Requirement RQ-10-13, the requirement is effectively addressed through the comprehensive summarization of verification results in SEC.3.BP6. By including rationales for not performing specific tests in test result documents, organizations can meet the requirements of ISO RQ-10-13 and ensure transparency and accountability in their cybersecurity practices. This integration strengthens the alignment between ASPICE and ISO 21434, contributing to the development of secure and reliable automotive systems that are resilient against cyber threats.

3.4 Mapping of Clause 11

Clause 11 of ISO/SAE 21434 focuses on cybersecurity validation activities at the vehicle level for the item under consideration (refer to Figure 9 in the standard). This clause addresses the processes involved in validating that the item, within its operational environment at the vehicle level and including configurations intended for series production, meets the cybersecurity goals and claims established earlier in the development lifecycle.

The primary objectives of Clause 11 are to validate the cybersecurity goals and cybersecurity claims, confirm that the item achieves these cybersecurity goals, and ensure that no unreasonable risks remain. This involves comprehensive testing and evaluation of the implemented cybersecurity measures to verify their effectiveness in real-world operational conditions. Cybersecurity validation is essential to demonstrate that the item can withstand potential cyber threats without compromising safety, functionality, or data integrity.

In this chapter, the requirements related to Clause 11 are mapped to the corresponding base practices in ASPICE for Cybersecurity. This mapping provides a structured framework for integrating the cybersecurity validation activities prescribed by ISO/SAE 21434 with the process assessment model of ASPICE. By aligning these requirements and practices, organizations can ensure that cybersecurity validation is conducted systematically and thoroughly, reinforcing the overall cybersecurity posture of the automotive product before it reaches the market.

Cybersecurity Validation

Mapping of ISO 21434 Requirement RQ-11-01 and ASPICE for Cybersecurity Base Practices SEC.1.BP1 – SEC.1.BP6

ISO 21434 Requirement RQ-11-01 emphasizes the necessity of conducting validation activities at the vehicle level for the item, considering the configurations intended for series production. These validation activities must confirm the adequacy of the cybersecurity goals with respect to the identified threat scenarios and corresponding risks, the achievement of the cybersecurity goals of the item, the validity of the cybersecurity

BUPT

claims, and the validity of the requirements on the operational environment, if applicable. The requirement notes that if any risks not addressed by the cybersecurity goals are identified during validation, they should be managed accordingly. Validation activities may include reviewing previous work products to confirm the achievement of cybersecurity goals, conducting penetration testing to demonstrate both the adequacy and fulfillment of cybersecurity goals, and reviewing all managed risks identified throughout the development process. The depth and rigor of penetration testing can be scaled using the Cybersecurity Assurance Level (CAL), ensuring that testing efforts are commensurate with the item's risk profile. Any weaknesses identified during validation should be analyzed for vulnerabilities and managed appropriately.

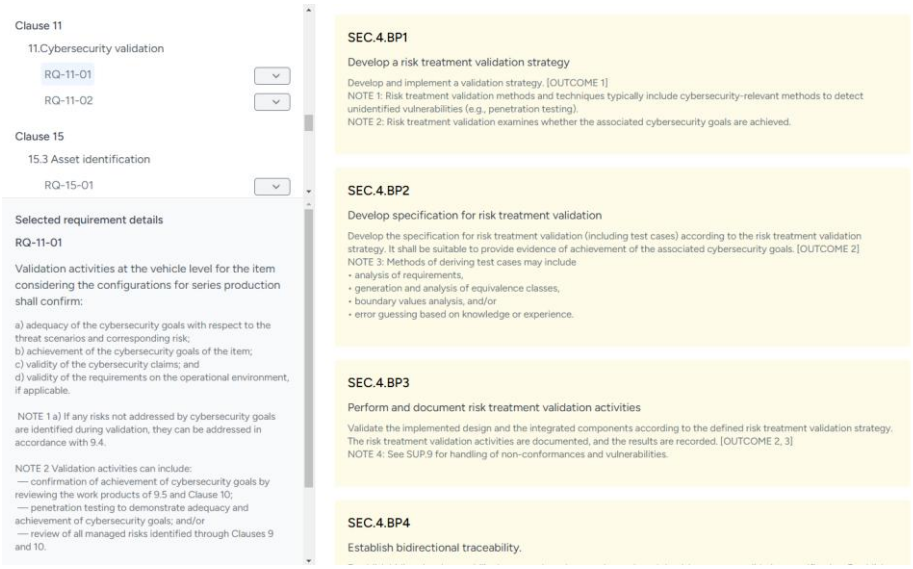


Fig. 41. Mapping of ISO 21434 Requirement RQ-11-01

Aligning with ISO RQ-11-01, the ASPICE for Cybersecurity base practices provide a structured approach through SEC.4.BP1 to SEC.4.BP6 to facilitate comprehensive risk treatment validation. SEC.4.BP1 focuses on developing and implementing a validation strategy that includes methods and techniques relevant to detecting unidentified vulnerabilities, such as penetration testing. This strategy examines whether the associated cybersecurity goals are achieved, directly supporting ISO's emphasis on confirming goal adequacy and achievement. SEC.4.BP2 involves developing the specification for risk treatment validation, including detailed test cases derived according to the validation strategy. This specification must provide evidence of the achievement of the cybersecurity goals, aligning with ISO's requirement to validate the cybersecurity goals and claims. SEC.4.BP3 requires performing and documenting the risk treatment validation activities. The implemented design and integrated components are validated according to the defined strategy, with all activities thoroughly documented and results recorded.

BUPT

This documentation is crucial for demonstrating compliance with cybersecurity goals and managing any identified vulnerabilities, as suggested by ISO's guidance on handling weaknesses during validation. SEC.4.BP4 emphasizes establishing bidirectional traceability between the cybersecurity goals and the risk treatment validation specification, as well as between the validation specification and the validation results. This traceability supports coverage, consistency, and impact analysis, ensuring that every cybersecurity goal is addressed by specific validation activities and that results can be traced back to their corresponding goals. This practice directly supports ISO's requirement to confirm the adequacy and achievement of cybersecurity goals and the validity of cybersecurity claims. SEC.4.BP5 focuses on ensuring consistency between the cybersecurity goals and the risk treatment validation specification. By maintaining consistency, organizations ensure that validation activities are aligned with the cybersecurity goals, fulfilling ISO's requirement to validate the adequacy of these goals concerning threat scenarios and risks. SEC.4.BP6 involves summarizing and communicating the risk treatment validation results to all affected parties. Effective communication ensures transparency and allows for informed decision-making regarding any residual risks or necessary actions, supporting ISO's emphasis on validating the requirements on the operational environment and addressing any risks not previously covered by cybersecurity goals.

In conclusion, the ASPICE for Cybersecurity base practices SEC.4.BP1 through SEC.4.BP6 provide a comprehensive framework that aligns closely with ISO 21434 Requirement RQ-11-01. By developing a robust validation strategy, specifying detailed validation activities, performing and documenting these activities, ensuring traceability and consistency, and communicating results effectively, organizations can confirm the adequacy and achievement of cybersecurity goals, validate cybersecurity claims, and verify operational environment requirements. This alignment ensures that the item meets the necessary cybersecurity standards, enhancing its resilience against cyber threats and contributing to the overall security posture of the automotive industry.

Mapping of ISO 21434 Requirement RQ-11-02 and ASPICE for Cybersecurity Base Practice SEC.1.BP1

ISO 21434 Requirement RQ-11-02 mandates that a rationale for the selection of validation activities must be provided. This requirement emphasizes the importance of justifying why specific validation methods and techniques have been chosen to confirm the adequacy and effectiveness of the cybersecurity measures implemented in the item. Providing a rationale ensures that the validation activities are appropriate for the identified risks and that they comprehensively address the cybersecurity goals and claims. It also promotes transparency and accountability, allowing stakeholders to understand the decision-making process behind the validation approach. In alignment with this ISO requirement, the ASPICE for Cybersecurity framework includes the practice of developing a risk treatment validation strategy, as outlined in SEC.4.BP1. This practice requires organizations to develop and implement a validation strategy designed to examine whether the associated cybersecurity goals are achieved. The accompanying notes specify that risk treatment validation methods and techniques typically include cybersecurity-relevant methods to detect unidentified vulnerabilities, such as penetration

BUPT

testing. By necessitating the development of a validation strategy, ASPICE inherently calls for a thoughtful selection of validation activities that are suited to the specific risks and goals of the project.

While ASPICE SEC.4.BP1 does not explicitly state that a rationale must be provided for the selection of validation activities, the process of developing a validation strategy implies the need for such a rationale. Organizations are expected to carefully consider which validation methods and techniques are most appropriate for confirming the achievement of cybersecurity goals. This involves assessing the risks, the nature of the item, the potential vulnerabilities, and the effectiveness of different validation approaches. Documenting this strategy effectively provides the rationale that ISO RQ-11-02 requires. In practice, when organizations develop their risk treatment validation strategy under ASPICE, they typically include justifications for their chosen validation activities. This might involve explaining why certain methods, such as penetration testing, are suitable for detecting specific vulnerabilities associated with the item, or why other methods may not be applicable. By documenting these decisions, organizations ensure that their validation activities are aligned with the identified risks and cybersecurity objectives, thereby fulfilling the intent of ISO RQ-11-02.

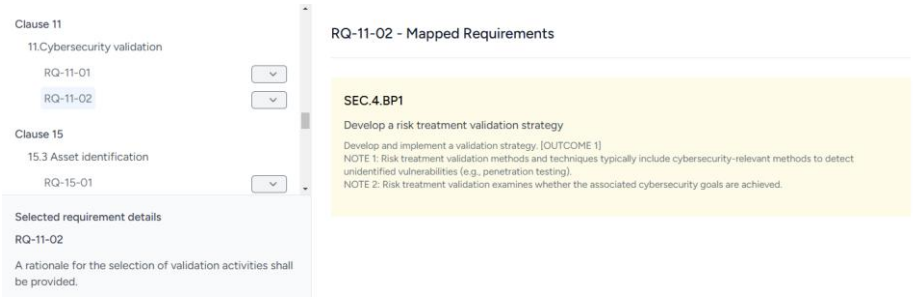


Fig. 42. Mapping of ISO 21434 Requirement RQ-11-02

In conclusion, ISO 21434 Requirement RQ-11-02 and the ASPICE for Cybersecurity practice of developing a risk treatment validation strategy are closely aligned. Both emphasize the importance of selecting appropriate validation activities to confirm the effectiveness of cybersecurity measures. While ASPICE does not explicitly require a documented rationale, the development of a comprehensive validation strategy inherently involves providing justification for the chosen validation methods and techniques. This alignment ensures that organizations can effectively validate their cybersecurity implementations and demonstrate compliance with industry standards, ultimately enhancing the security and resilience of automotive systems against cyber threats.

3.5 Mapping of Clause 15

Clause 15 of ISO/SAE 21434 focuses on the methods used to determine the extent to which road users can be impacted by a threat scenario. These methods, collectively

BUPT

known as Threat Analysis and Risk Assessment (TARA), are performed from the viewpoint of the affected road users. The clause outlines generic modules that can be systematically invoked at any point in the lifecycle of an item or component. These modules include asset identification (section 15.3), threat scenario identification (15.4), impact rating (15.5), attack path analysis (15.6), attack feasibility rating (15.7), risk value determination (15.8), and risk treatment decision (15.9).

Since these are generic modules, the work products defined in this clause are documented as parts of work products produced by other clauses. The objectives of Clause 15 are to identify assets, their cybersecurity properties, and their damage scenarios; to identify threat scenarios; to determine the impact rating of damage scenarios; to identify the attack paths that realize threat scenarios; to determine the ease with which attack paths can be exploited; to determine the risk values of threat scenarios; and to select appropriate risk treatment options for threat scenarios.

In this chapter, the requirements related to Clause 15 are mapped to the corresponding base practices in ASPICE for Cybersecurity. This mapping provides a structured framework for integrating the threat analysis and risk assessment activities prescribed by ISO/SAE 21434 with the process assessment model of ASPICE. By aligning these requirements and practices, organizations can systematically incorporate risk assessment methodologies throughout the product development lifecycle, ensuring that automotive systems are robust and secure against cyber threats.

Asset Identification (15.3)

Mapping of ISO 21434 Requirements RQ-15-01, RQ-15-02 and ASPICE for Cybersecurity Base Practices MAN.7.BP1, MAN.7.BP3

ISO 21434 Requirements RQ-15-01 and RQ-15-02 are foundational steps in the cybersecurity risk assessment process for automotive systems. RQ-15-01 mandates the identification of damage scenarios, which are potential adverse consequences resulting from cybersecurity breaches. These scenarios encompass the relationship between the functionality of the item (such as a vehicle component or system) and the adverse outcome, descriptions of harm to road users, and the relevant assets that could be affected. By identifying damage scenarios, organizations can understand how cyber threats might translate into real-world impacts, including safety hazards, financial losses, operational disruptions, and breaches of privacy. Building on this, RQ-15-02 requires the identification of assets with cybersecurity properties whose compromise could lead to a damage scenario. Assets are elements within the item that possess properties like confidentiality, integrity, and availability, which are crucial for maintaining cybersecurity. The identification process can involve analyzing the item definition, performing impact ratings, deriving assets from potential threat scenarios, or utilizing predefined catalogs of assets. This ensures a comprehensive understanding of all critical components that need protection to prevent the realization of damage scenarios.

BUPT

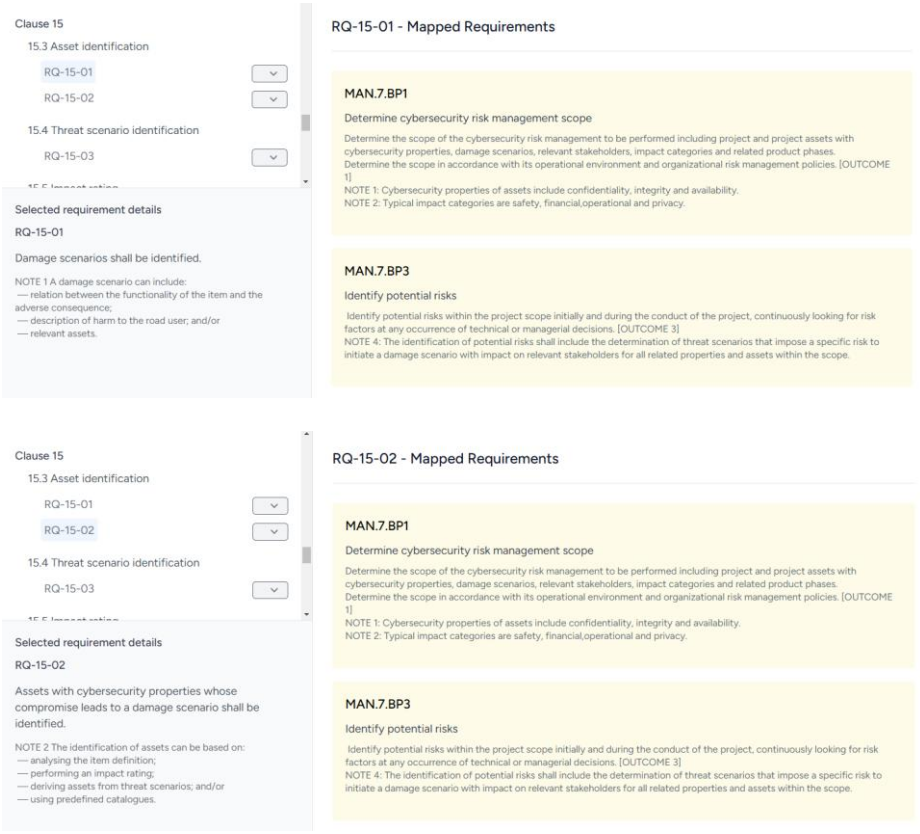


Fig. 43. Mapping of ISO 21434 Requirements RQ-15-01, RQ-15-02

In the context of ASPICE for Cybersecurity, these ISO requirements align closely with the practices outlined in MAN.7.BP1 and MAN.7.BP3. MAN.7.BP1 focuses on determining the scope of cybersecurity risk management. This involves defining the project scope to include assets with cybersecurity properties, damage scenarios, relevant stakeholders, impact categories (such as safety, financial, operational, and privacy impacts), and related product phases. The scope determination is conducted in accordance with the operational environment and the organization's risk management policies. By establishing this scope, organizations set the foundation for a targeted and effective risk management process. MAN.7.BP1 directly addresses the requirements of RQ-15-01 and RQ-15-02 by ensuring that damage scenarios and assets with cybersecurity properties are identified at the outset. By incorporating these elements into the scope, organizations acknowledge the potential adverse consequences and the critical assets that, if compromised, could lead to those consequences. This practice ensures that all relevant factors are considered in the risk management process, aligning with the ISO's emphasis on comprehensive identification.

MAN.7.BP3 emphasizes the ongoing identification of potential risks within the project scope. This involves continuously looking for risk factors during technical or

BUPT

managerial decisions throughout the project's lifecycle. The identification includes determining threat scenarios that pose specific risks capable of initiating damage scenarios impacting relevant stakeholders. By maintaining a continuous risk identification process, organizations can adapt to new threats, changes in the operational environment, or alterations in the system design that might introduce new vulnerabilities. This continuous approach in MAN.7.BP3 complements the ISO requirements by ensuring that the identification of damage scenarios and assets is not a one-time activity but an ongoing effort. As new information emerges or as the project evolves, the organization can update its understanding of potential risks and adjust its risk management strategies accordingly. This proactive stance aligns with ISO's emphasis on thorough and dynamic risk assessment practices.

In summary, ISO 21434's RQ-15-01 and RQ-15-02 focus on identifying potential damage scenarios and the assets whose compromise could lead to these scenarios, forming the basis of a robust cybersecurity risk assessment. ASPICE for Cybersecurity's MAN.7.BP1 and MAN.7.BP3 provide a structured approach to fulfilling these requirements by establishing the scope of risk management and ensuring continuous risk identification. Together, these practices enable organizations to comprehensively understand and manage cybersecurity risks, enhancing the security and resilience of automotive systems against cyber threats.

Threat Scenario Identification (15.4)

Mapping of ISO 21434 Requirement RQ-15-03 and ASPICE for Cybersecurity Base Practice MAN.7.BP3

ISO 21434 Requirement RQ-15-03 emphasizes the crucial step of identifying threat scenarios in the cybersecurity risk assessment process for automotive systems. According to this requirement, each threat scenario must include three key elements: the targeted asset, the compromised cybersecurity property of that asset (such as confidentiality, integrity, or availability), and the cause of the compromise of the cybersecurity property. This comprehensive approach ensures that organizations thoroughly understand how potential cyber threats can impact specific assets and the nature of those impacts. The requirement acknowledges that additional information can be associated with a threat scenario, such as related damage scenarios, technical interdependencies between assets, details about potential attackers, methods and tools they might use, and the attack surfaces they might exploit. It also suggests that the identification of threat scenarios can be conducted through group discussions or systematic approaches, utilizing frameworks like EVITA, TVRA, PASTA, or STRIDE. These methodologies help in systematically identifying and categorizing threats based on different factors like spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Furthermore, it is noted that a single damage scenario may correspond to multiple threat scenarios, and conversely, a threat scenario can lead to multiple damage scenarios. An example provided is the spoofing of Controller Area Network (CAN) messages to the braking Electronic Control Unit (ECU), which compromises the integrity of the messages and potentially leads to a loss of braking function integrity.

BUPT

In alignment with this ISO requirement, the ASPICE for Cybersecurity process MAN.7.BP3 focuses on the identification of potential risks within the project scope. This practice involves initially identifying risks and continuously monitoring for new risk factors throughout the project's duration, especially during technical or managerial decision points. The identification process explicitly includes determining threat scenarios that impose specific risks capable of initiating damage scenarios that impact relevant stakeholders. These threat scenarios consider all related properties and assets within the defined scope, ensuring a comprehensive assessment of potential cybersecurity risks.

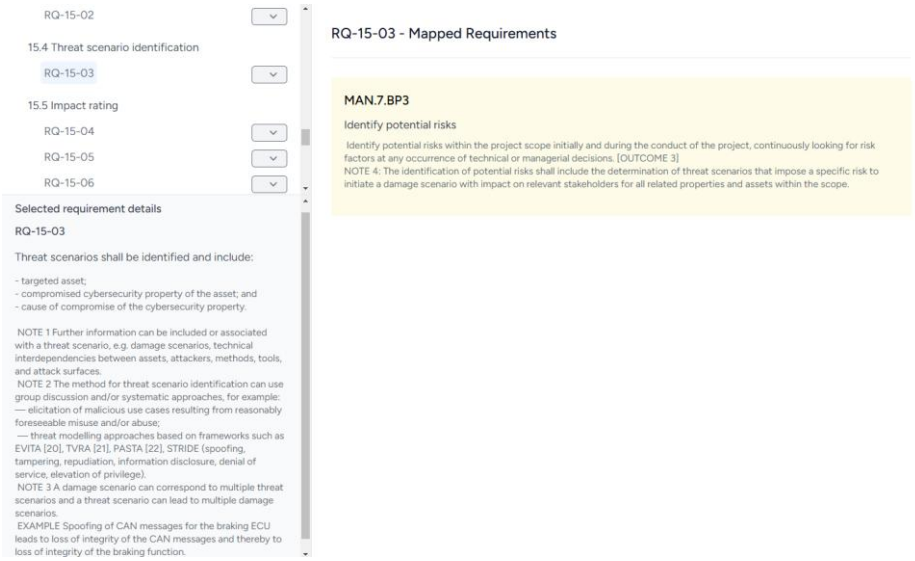


Fig. 44. Mapping of ISO 21434 Requirement RQ-15-03

The mapping between ISO RQ-15-03 and ASPICE MAN.7.BP3 is evident in their shared emphasis on systematically identifying threat scenarios as a fundamental component of cybersecurity risk management. Both standards recognize that understanding the specifics of how assets can be compromised, and the resulting impacts, is essential for developing effective mitigation strategies. By including elements such as the targeted asset, the compromised property, and the cause of compromise, organizations can gain detailed insights into potential vulnerabilities and threat vectors. Moreover, both ISO and ASPICE acknowledge the importance of using structured methods and frameworks to guide the identification of threat scenarios. The ISO requirement suggests utilizing established threat modeling approaches and encourages the inclusion of detailed information that can enhance the understanding of each threat scenario. Similarly, ASPICE MAN.7.BP3 implies the use of systematic risk identification processes that can be integrated into the project's risk management activities. The example provided in the ISO requirement, where spoofing CAN messages to the braking ECU leads to

BUPT

compromised message integrity and impacts the braking function, illustrates how a threat scenario can be detailed and directly linked to potential damage scenarios. This level of detail aligns with ASPICE's focus on understanding how threat scenarios can initiate damage scenarios affecting stakeholders, reinforcing the need for thorough analysis and documentation.

In conclusion, ISO 21434 Requirement RQ-15-03 and ASPICE for Cybersecurity practice MAN.7.BP3 are closely aligned in their objectives and methodologies. Both emphasize the systematic identification of threat scenarios, including detailed information about targeted assets, compromised properties, and causes of compromise. By integrating these practices, organizations can enhance their cybersecurity risk assessments, ensuring that all potential threats are identified, analyzed, and addressed effectively. This alignment facilitates the development of robust cybersecurity strategies that protect automotive systems against cyber threats and safeguard stakeholders' interests.

Impact rating (15.5)

Mapping of ISO 21434 Requirement RQ-15-04 and ASPICE for Cybersecurity Base Practice MAN.7.BP3

ISO 21434 Requirement RQ-15-04 mandates that damage scenarios must be assessed against potential adverse consequences for road users in four specific impact categories: safety, financial, operational, and privacy (abbreviated as S, F, O, P respectively). This requirement emphasizes the importance of evaluating how cybersecurity incidents could affect these critical areas, ensuring that organizations thoroughly consider the potential impacts on the well-being and interests of road users. The standard acknowledges that it does not provide relationships or weightings between different impact categories, allowing organizations the flexibility to prioritize them based on their context and risk management policies. Additionally, it permits the inclusion of additional impact categories if deemed necessary, with the recommendation that any such additions, along with their rationale, be shared within the supply chain in accordance with Clause 7 of the standard.

In the context of ASPICE for Cybersecurity, the practice of identifying potential risks, as outlined in MAN.7.BP3, closely aligns with this ISO requirement. This practice involves the initial and continuous identification of potential risks within the project scope, especially at points where technical or managerial decisions occur. It requires organizations to look for risk factors that could impact relevant stakeholders and to determine threat scenarios that impose specific risks capable of initiating damage scenarios. By considering all related properties and assets within the scope, this practice ensures a comprehensive assessment of potential cybersecurity risks and their impacts.

BUPT

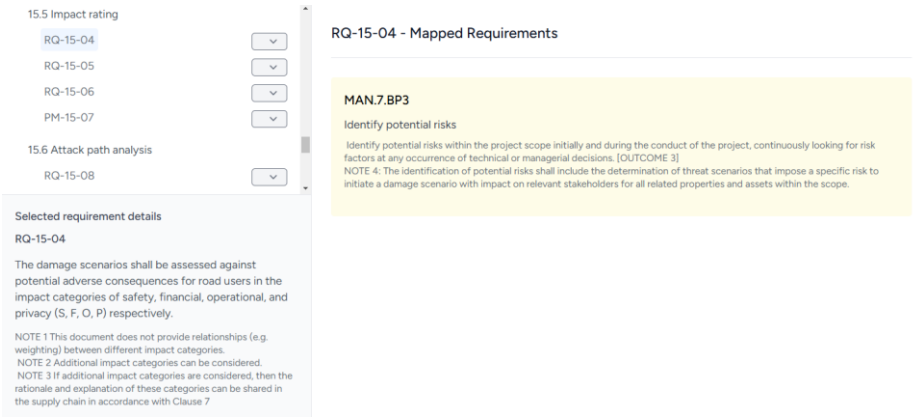


Fig. 45. Mapping of ISO 21434 Requirement RQ-15-04

The alignment between ISO RQ-15-04 and ASPICE MAN.7.BP3 is evident in their shared emphasis on assessing the impacts of damage scenarios on stakeholders. While ISO explicitly requires the assessment against the four impact categories of safety, financial, operational, and privacy, ASPICE encourages organizations to consider the impacts on relevant stakeholders without prescribing specific categories. However, the requirement in MAN.7.BP3 to consider all related properties and assets naturally encompasses these impact areas. By integrating the specific impact categories from ISO into the risk identification process of ASPICE, organizations can enhance the thoroughness of their assessments. In practice, when implementing MAN.7.BP3, organizations can incorporate the impact categories specified by ISO RQ-15-04 by systematically evaluating how each identified damage scenario could adversely affect safety, financial stability, operational continuity, and privacy. This involves analyzing the potential consequences of cybersecurity threats on the physical safety of road users, financial losses for the organization or stakeholders, disruptions to vehicle or system operations, and unauthorized access to or misuse of personal data. By doing so, organizations ensure that they address the critical areas where cybersecurity incidents could have the most significant repercussions. Moreover, both ISO and ASPICE recognize the importance of flexibility and adaptability in the risk assessment process. ISO allows for the consideration of additional impact categories if necessary and suggests sharing the rationale and explanations for these categories within the supply chain. Similarly, ASPICE's approach to risk identification is continuous and responsive, encouraging organizations to look for new risk factors and consider their impacts as the project progresses. This shared emphasis on adaptability ensures that organizations remain vigilant and responsive to emerging threats and changing circumstances.

In conclusion, ISO 21434 Requirement RQ-15-04 and ASPICE for Cybersecurity practice MAN.7.BP3 are closely aligned in their approach to assessing the potential impacts of damage scenarios resulting from cybersecurity threats. By explicitly incorporating the impact categories of safety, financial, operational, and privacy into the risk identification and assessment processes, organizations can ensure a comprehensive

BUPT

evaluation of how cybersecurity incidents could affect stakeholders. This alignment enhances the effectiveness of cybersecurity risk management, enabling organizations to develop more robust strategies to mitigate risks and protect both the organization and its users from adverse consequences. Ultimately, integrating these practices contributes to the development of secure and resilient automotive systems that prioritize the safety and interests of all stakeholders.

Mapping of ISO 21434 Requirements RQ-15-05, RQ-15-06, PM-15-07 and ASPICE for Cybersecurity Base Practice MAN.7.BP3

ISO 21434 Requirements RQ-15-05, RQ-15-06, and PM-15-07 focus on the critical task of impact rating in the cybersecurity risk assessment process for automotive systems. RQ-15-05 mandates that the impact rating of a damage scenario must be determined for each impact category using one of the following levels: severe, major, moderate, or negligible. This standardized scale allows organizations to consistently evaluate the potential consequences of cybersecurity incidents across different scenarios and impact categories, facilitating a uniform understanding of risk severity. RQ-15-06 specifies that safety-related impact ratings should be derived from ISO 26262-3:2018, clause 6.4.3. This clause in ISO 26262 provides a framework for assessing the severity of hazardous events in functional safety, which can be directly applied to evaluate the safety impacts of cybersecurity-related damage scenarios. Note 5 indicates that Table F.1 in Annex F of ISO 21434 can be used to map safety impact criteria to the standardized impact ratings, offering a practical tool for organizations to align their safety assessments with the cybersecurity impact rating process. Note 6 highlights that evaluations performed for functional safety purposes can be reused for this impact rating, promoting efficiency and consistency between safety and cybersecurity assessments. PM-15-07 allows organizations to omit further analysis in other impact categories if a damage scenario results in an impact rating and it can be reasonably argued that the impacts in other categories are less critical. For example, if a damage scenario has a safety impact rated as "severe," the organization may decide not to further analyze the financial impact of that scenario, assuming it would be less critical. This provision enables organizations to focus their resources on the most significant risks, streamlining the risk assessment process without compromising the thoroughness of the evaluation.

In the context of ASPICE for Cybersecurity, the practice MAN.7.BP3 involves identifying potential risks within the project scope, both initially and continuously throughout the project's duration. This practice emphasizes the importance of consistently looking for risk factors during technical or managerial decision-making processes. The identification of potential risks includes determining threat scenarios that impose specific risks capable of initiating damage scenarios, which impact relevant stakeholders across all related properties and assets within the scope.

BUPT

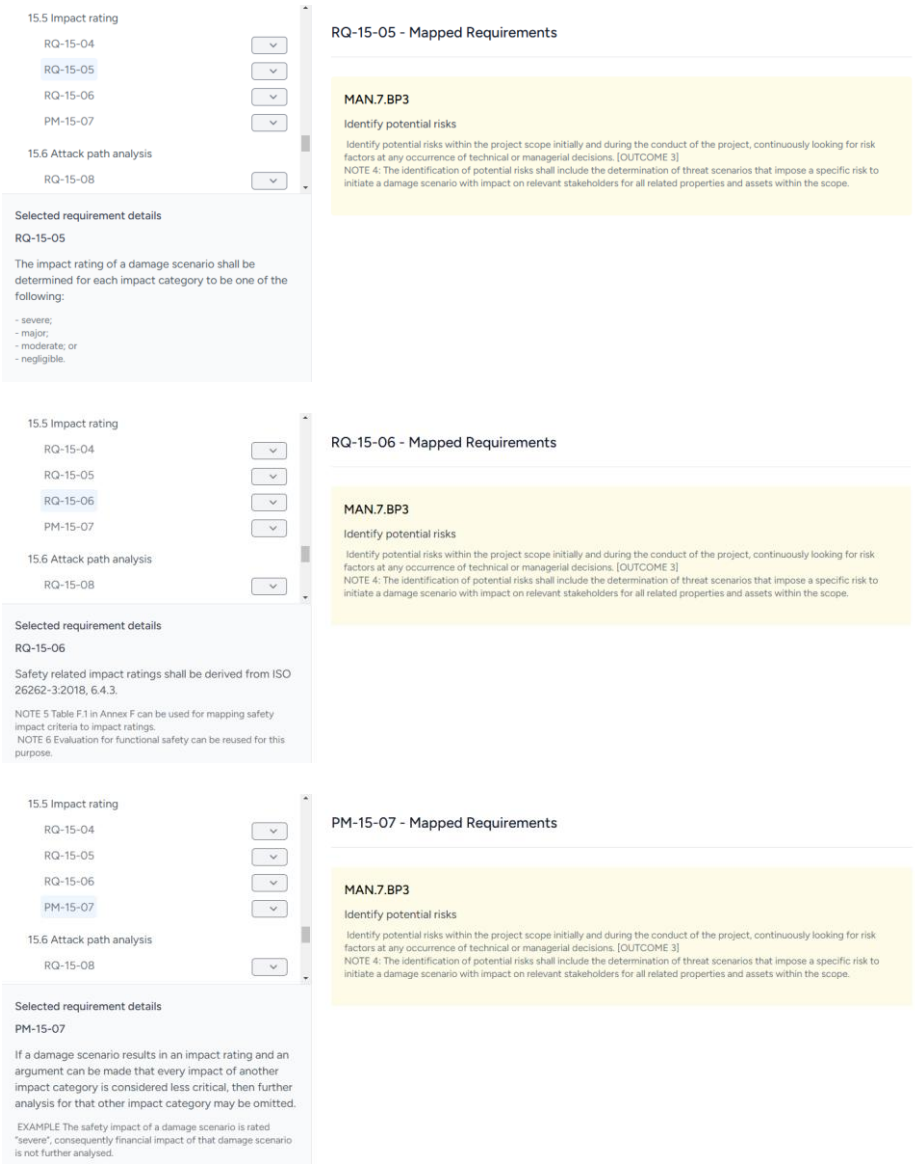


Fig. 46. Mapping of ISO 21434 Requirements RQ-15-05, RQ-15-06, PM-15-07

The alignment between these ISO requirements and the ASPICE practice is evident in their shared emphasis on systematically identifying and evaluating risks and their impacts. While ISO 21434 provides a detailed methodology for impact rating, including specific categories and severity levels, ASPICE's MAN.7.BP3 offers a framework for ongoing risk identification and assessment without prescribing exact rating scales or categories. Organizations implementing ASPICE can enhance their risk assessment processes by incorporating the impact rating scale defined in ISO RQ-15-05. By

BUPT

assigning standardized severity levels—severe, major, moderate, or negligible—to the impacts of identified damage scenarios, they can achieve a more precise and comparable evaluation of risks. Additionally, leveraging ISO 26262-3:2018 for safety-related impact ratings, as suggested in RQ-15-06, ensures consistency between functional safety and cybersecurity assessments. This integration allows for the reuse of existing evaluations, saving time and resources while maintaining a high level of accuracy. The provision in PM-15-07 for omitting further analysis in less critical impact categories can also be effectively integrated into the ASPICE risk assessment process. By focusing on the most critical impacts, organizations can allocate their resources more efficiently, ensuring that the most significant risks receive the necessary attention. This approach aligns with the continuous risk identification and prioritization emphasized in MAN.7.BP3, enabling organizations to maintain a dynamic and responsive cybersecurity risk management process.

In conclusion, ISO 21434 Requirements RQ-15-05, RQ-15-06, and PM-15-07 provide detailed guidance on determining impact ratings for damage scenarios in cybersecurity risk assessments, specifying both the categories to consider and the levels of severity to assign. The ASPICE for Cybersecurity practice MAN.7.BP3 complements these requirements by mandating the identification of potential risks and the assessment of their impacts on relevant stakeholders. By integrating the specific impact rating methodology from ISO 21434 into the ASPICE framework, organizations can enhance their risk assessment processes, ensuring a thorough, consistent, and standardized evaluation of cybersecurity risks and their potential consequences. This alignment ultimately contributes to the development of more secure and resilient automotive systems, better protecting stakeholders from the adverse effects of cybersecurity incidents.

Attack path analysis (15.6)

Mapping of ISO 21434 Requirements RQ-15-08, RQ-15-09 and ASPICE for Cybersecurity Base Practice MAN.7.BP5

ISO 21434 Requirements RQ-15-08 and RQ-15-09 focus on the critical process of analyzing threat scenarios to identify attack paths in the cybersecurity risk assessment of automotive systems. Requirement RQ-15-08 mandates that organizations must thoroughly analyze threat scenarios to identify attack paths, which are sequences of actions an attacker could take to realize a threat scenario. This analysis is essential for understanding how vulnerabilities could be exploited and for developing effective countermeasures to mitigate risks. Attack path analysis can be conducted using two primary approaches. The top-down approach involves deducing attack paths by systematically exploring the different ways a threat scenario could be realized, utilizing methods such as attack trees or attack graphs. This method allows for a comprehensive examination of potential attack vectors from the perspective of the threat scenario itself. Alternatively, the bottom-up approach builds attack paths from identified vulnerabilities, constructing possible paths an attacker might take starting from existing weaknesses in the system. This method is particularly useful when specific vulnerabilities have already been identified, allowing for targeted analysis of how these weaknesses could be exploited. The requirement notes that if a partial attack path does not lead to the realization

BUPT

of a threat scenario, the analysis of that partial path can be discontinued, enabling organizations to focus resources on more relevant attack paths.

Requirement RQ-15-09 stipulates that each attack path identified must be associated with the threat scenarios that can be realized by that attack path. This ensures a clear linkage between potential attack vectors and the specific threats they enable, facilitating a more targeted and effective risk assessment and mitigation process. The requirement acknowledges that in the early stages of product development, attack paths may be incomplete or imprecise due to the lack of detailed implementation information. As product development progresses and more information becomes available—particularly after conducting vulnerability analyses—attack paths should be updated to reflect the current understanding of potential security issues. An illustrative example provided in RQ-15-09 involves a threat scenario where spoofing of Controller Area Network (CAN) messages to the braking Electronic Control Unit (ECU) leads to a loss of integrity of both the CAN messages and the braking function. The attack path realizing this threat scenario involves several steps: first, the telematics ECU is compromised via the cellular interface; second, the gateway ECU is compromised through CAN communication from the compromised telematics ECU; and third, the gateway ECU forwards malicious braking request signals, resulting in unwanted rapid deceleration. This example demonstrates how a complex attack path can be broken down into specific stages, each of which can be analyzed for vulnerabilities and mitigated accordingly.

Aligning with these ISO requirements, the Automotive SPICE (ASPICE) for Cybersecurity process MAN.7.BP5 focuses on analyzing potential risks and evaluating them to determine the probability, consequence, and severity of risks. This practice involves a detailed analysis of potential risks based on the identified attack paths that realize threat scenarios. By assessing the ease with which these attack paths can be conducted, organizations can evaluate the likelihood of successful attacks and prioritize risks accordingly. ASPICE MAN.7.BP5 acknowledges the use of various techniques for evaluating metrics, rating, and scoring schemes to analyze the system. These techniques include functional analysis, simulation, Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), and Attack Tree Analysis (ATA). Such methods provide structured approaches to systematically assess the risks associated with identified attack paths, enabling organizations to quantify risks in terms of their probability and potential impact. This quantification is crucial for making informed decisions about where to allocate resources for risk mitigation.

BUPT



Fig. 47. Mapping of ISO 21434 Requirements RQ-15-08, RQ-15-09

The alignment between ISO RQ-15-08 and RQ-15-09 and ASPICE MAN.7.BP5 is evident in their shared emphasis on the importance of attack path analysis in the cybersecurity risk management process. Both frameworks recognize that understanding how threat scenarios can be realized through specific attack paths is essential for accurately assessing risks. By associating attack paths with threat scenarios, organizations can better understand the feasibility of attacks, the potential consequences, and the most effective points for implementing security controls. Moreover, the iterative nature of attack path analysis highlighted in ISO RQ-15-09 aligns with the continuous risk assessment approach advocated in ASPICE MAN.7.BP5. As products evolve and more information becomes available during development, organizations are encouraged to update their attack path analyses accordingly. This ensures that risk assessments remain current and

BUPT

relevant, allowing for timely adjustments to cybersecurity strategies as new vulnerabilities are identified or system configurations change.

In conclusion, ISO 21434 Requirements RQ-15-08 and RQ-15-09 and ASPICE for Cybersecurity practice MAN.7.BP5 are closely aligned in their approach to cybersecurity risk assessment. Both emphasize the necessity of analyzing threat scenarios to identify attack paths and assessing the risks associated with these paths based on their probability and potential impact. By integrating these practices, organizations can develop a comprehensive understanding of potential cybersecurity risks, enabling them to implement effective mitigation strategies. This alignment ultimately contributes to the development of secure and resilient automotive systems that are better equipped to withstand cyber threats and protect stakeholders.

Attack feasibility rating (15.7)

Mapping of ISO 21434 Requirements RQ-15-10, RC-15-11 - RC-15-14 and ASPICE for Cybersecurity Base Practice MAN.7.BP5

ISO 21434 Requirement RQ-15-10 mandates that for each identified attack path, an attack feasibility rating must be determined. This rating assesses how easily an attacker could exploit the attack path to realize a threat scenario, categorizing the effort required into four levels: High (the attack path can be accomplished utilizing low effort), Medium (the attack path requires medium effort), Low (the attack path requires high effort), and Very Low (the attack path requires very high effort). This classification helps organizations prioritize risks based on the ease of execution, allowing them to allocate resources effectively to mitigate higher-risk scenarios. The accompanying recommendations, RC-15-11 to RC-15-14, provide guidance on how to determine the attack feasibility rating. RC-15-11 suggests defining the attack feasibility rating method based on one of three approaches: an attack potential-based approach, a CVSS-based approach, or an attack vector-based approach. The selection of the appropriate method depends on the phase in the lifecycle and the information available. In the early stages of development, when detailed system information may be limited, an attack vector-based approach might be more suitable. As development progresses and more information becomes available, organizations might adopt a more detailed attack potential-based or CVSS-based analysis. If an attack potential-based approach is used, as per RC-15-12, the attack feasibility rating should be determined based on core factors including elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, and equipment required. These factors are derived from standards like ISO/IEC 18045, and guidelines are provided in Annex G.2 of ISO 21434. For a CVSS-based approach, RC-15-13 states that the rating should be determined based on the exploitability metrics of the base metric group, including attack vector, attack complexity, privileges required, and user interaction, with further guidance in Annex G.3. If an attack vector-based approach is chosen, as described in RC-15-14, the attack feasibility rating focuses on evaluating the predominant attack vector, referencing definitions from CVSS version 3.1. This method is particularly useful during early development stages when there is insufficient information to identify specific attack paths, and further guidance is available in Annex G.4.

BUPT

In the context of Automotive SPICE (ASPICE) for Cybersecurity, the practice MAN.7.BP5 involves analyzing potential risks and evaluating them to determine the probability, consequences, and severity of risks. This analysis is based on identified attack paths that realize a threat scenario and considers the ease with which these attack paths can be conducted. The practice acknowledges that different techniques may be used for evaluating metrics, rating, and scoring schemes to analyze a system, including functional analysis, simulation, Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), and Attack Tree Analysis (ATA). While ASPICE MAN.7.BP5 does not explicitly prescribe the specific methods for determining attack feasibility ratings as outlined in ISO 21434, the overall objectives are aligned. Both frameworks emphasize the importance of assessing the ease or difficulty with which an attacker could exploit vulnerabilities, which is crucial for accurate risk evaluation and prioritization. By integrating the attack feasibility rating methods from ISO 21434 into the ASPICE process, organizations can enhance their risk assessment practices. In practice, organizations implementing ASPICE can adopt the attack feasibility rating approaches recommended by ISO 21434 within their risk analysis activities. By doing so, they can systematically evaluate the likelihood of threat scenarios being realized through specific attack paths, considering factors such as required expertise, resources, and attack vectors. This integration allows for a more nuanced assessment of risks by accounting not only for the potential impact but also for the effort required by an attacker to exploit vulnerabilities.

Aligning the ASPICE risk analysis process with ISO 21434's attack feasibility ratings ensures a comprehensive and consistent approach to cybersecurity risk management. This alignment facilitates better prioritization of mitigation efforts, focusing resources on addressing the most feasible and potentially damaging attack paths. Ultimately, integrating these practices supports a more robust cybersecurity strategy, contributing to the development of secure and resilient automotive systems capable of withstanding cyber threats.

Risk value determination (15.8)

Mapping of ISO 21434 Requirements RQ-15-15, RQ-15-16 and ASPICE for Cybersecurity Base Practices MAN.7.BP4, MAN.7.BP5

ISO 21434 Requirements RQ-15-15 and RQ-15-16 focus on determining risk values for each identified threat scenario within the cybersecurity risk assessment process for automotive systems. Requirement RQ-15-15 mandates that organizations calculate the risk value for every threat scenario by considering both the impact of associated damage scenarios and the attack feasibility of corresponding attack paths. This comprehensive approach ensures that risk evaluation accounts for the potential consequences of a cyber incident as well as the likelihood of its occurrence. If a threat scenario corresponds to multiple damage scenarios or if an associated damage scenario affects more than one impact category (such as safety, financial, operational, or privacy), the standard allows for separate risk values to be determined for each impact rating. This enables a nuanced understanding of how a single threat can have varied effects across different areas. Additionally, when a threat scenario is linked to multiple attack paths, the attack feasibility

BUPT

ratings of these paths can be appropriately aggregated. For example, the highest attack feasibility rating among the attack paths might be assigned to the threat scenario to reflect the most accessible route an attacker could exploit. Requirement RQ-15-16 specifies that the risk value assigned to a threat scenario must be a numerical value between 1 and 5, inclusive, where a value of 1 represents minimal risk. This standardized scale facilitates consistent evaluation and comparison of risks across different scenarios and systems. The standard suggests methods for determining risk values, such as using risk matrices or risk formulas. These tools combine impact ratings and attack feasibility ratings to compute a single risk value, enabling organizations to prioritize risks effectively based on both severity and likelihood.

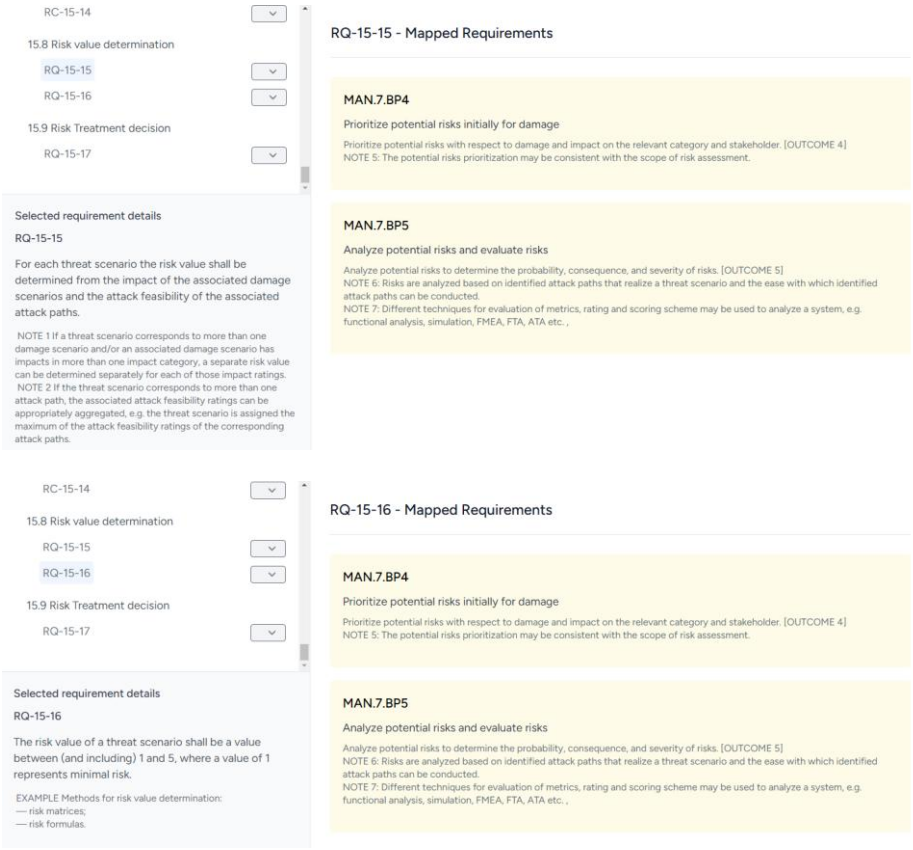


Fig. 48. Mapping of ISO 21434 Requirements RQ-15-15, RQ-15-16

In alignment with these ISO requirements, the Automotive SPICE (ASPICE) for Cybersecurity framework includes processes MAN.7.BP5 and MAN.7.BP4, which focus on analyzing and prioritizing potential risks. MAN.7.BP5 involves analyzing potential

BUPT

risks to determine their probability, consequences, and severity. This analysis is based on identified attack paths that realize a threat scenario and the ease with which these attack paths can be executed. The practice acknowledges that different techniques may be used for evaluating metrics, rating, and scoring schemes to analyze a system, including functional analysis, simulation, Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), and Attack Tree Analysis (ATA). By employing these techniques, organizations assess both the likelihood and impact of potential risks, which aligns with the ISO requirement to determine risk values from impact and attack feasibility. MAN.7.BP4 focuses on prioritizing potential risks with respect to damage and impact on relevant categories and stakeholders. This practice ensures that risks are not only identified but also ranked according to their potential to cause harm or disruption. By prioritizing risks based on their assessed severity and potential damage, organizations can allocate resources more effectively, addressing the most critical threats first. This prioritization is consistent with the scope of the risk assessment and supports strategic decision-making in cybersecurity risk management.

The alignment between ISO RQ-15-15 and RQ-15-16 and ASPICE MAN.7.BP5 and MAN.7.BP4 is evident in their shared emphasis on a systematic and quantitative approach to risk analysis and prioritization. Both frameworks require organizations to evaluate risks by considering the potential impact of damage scenarios and the feasibility of attacks. By assigning numerical values to risks and prioritizing them accordingly, organizations can develop targeted mitigation strategies that address the most significant threats to their systems. Integrating the ISO's risk value determination methodology into the ASPICE practices enhances the robustness of the cybersecurity risk assessment process. Organizations can adopt risk matrices or formulas to quantify risks, combining impact ratings with attack feasibility ratings to arrive at a risk value between 1 and 5. This quantitative assessment allows for objective comparison of risks and aids in making informed decisions about where to focus mitigation efforts.

By incorporating these practices, organizations ensure that their risk assessments are thorough, consistent, and aligned with industry standards. The synergy between ISO 21434 and ASPICE practices facilitates a comprehensive approach to cybersecurity risk management, enabling organizations to prioritize risks effectively and implement appropriate countermeasures. This alignment ultimately contributes to the development of secure and resilient automotive systems that protect stakeholders from potential cyber threats and maintain the integrity, safety, and reliability of automotive products.

Risk Treatment decision (15.9)

Mapping of ISO 21434 Requirement RQ-15-17 and ASPICE for Cybersecurity Base Practice MAN.7.BP6

ISO 21434 Requirement RQ-15-17 mandates that for each identified threat scenario, considering its assessed risk values, one or more appropriate risk treatment options must be determined. These options include avoiding the risk, reducing the risk, sharing the risk, or retaining the risk. This requirement emphasizes the necessity for organizations to make informed decisions on how to handle each risk based on its severity and the organization's risk management strategy. The accompanying note specifies that the

BUPT

rationales for retaining or sharing the risk must be recorded as cybersecurity claims and are subject to cybersecurity monitoring and vulnerability management as outlined in Clause 8 of the standard. This ensures that even when risks are not mitigated, they are acknowledged and managed appropriately throughout the system's lifecycle.

In alignment with ISO 21434 RQ-15-17, the Automotive SPICE (ASPICE) for Cybersecurity process MAN.7.BP6 focuses on defining risk treatment options for each identified risk or set of risks. This practice requires organizations to decide whether to accept, reduce, avoid, or share (transfer) the risks. By explicitly defining these options, ASPICE ensures that all risks are systematically addressed and that appropriate strategies are implemented to manage them effectively. The accompanying note in MAN.7.BP6 highlights that typically accepted and shared risks define cybersecurity claims, mirroring the ISO requirement's emphasis on documenting rationales for retaining or sharing risks as cybersecurity claims. These claims are crucial for ongoing risk management, monitoring, and vulnerability management activities.

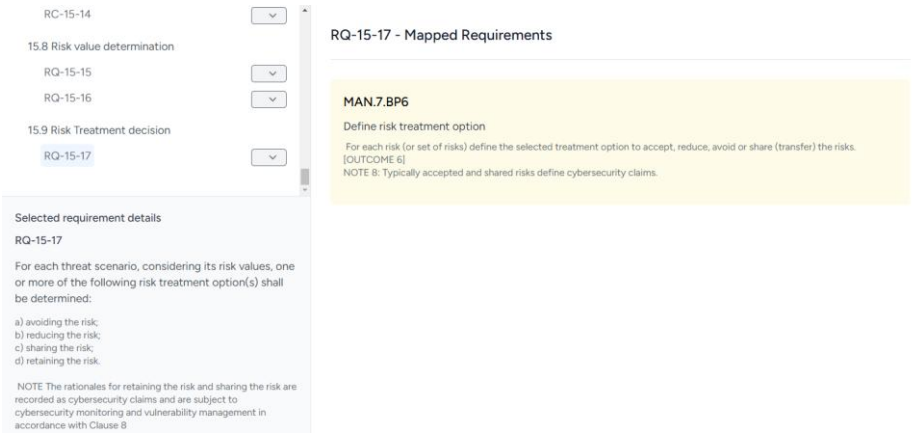


Fig. 49. Mapping of ISO 21434 Requirement RQ-15-17

Both ISO RQ-15-17 and ASPICE MAN.7.BP6 underscore the importance of a structured and transparent approach to risk treatment in the cybersecurity risk management process. They recognize that not all risks can be entirely eliminated and that organizations must make strategic decisions on how to handle each risk based on factors such as impact severity, likelihood of occurrence, feasibility of mitigation, and resource constraints. By defining clear risk treatment options and documenting the rationale behind them, organizations can ensure accountability and facilitate continuous improvement in their cybersecurity practices. The alignment between ISO 21434 and ASPICE in this context promotes consistency and coherence in the automotive industry's approach to cybersecurity risk management. Adhering to these standards enables organizations to effectively manage cybersecurity risks by ensuring that all potential threats are addressed in a manner consistent with organizational policies and industry best practices.

BUPT

This comprehensive and methodical approach contributes to the development of secure and resilient automotive systems, enhancing overall safety, reliability, and trust in automotive products amidst the evolving landscape of cyber threats.

BUPT

4 Web Application

The initial development of the Compliance Matrix in Excel was a significant step toward harmonizing the requirements of ISO/SAE 21434 [6] and ASPICE for Cybersecurityz. This matrix provided a structured approach to mapping the critical clauses of ISO/SAE 21434 (specifically clauses 7, 9, 10, 11, and 15) to the corresponding base practices of ASPICE for Cybersecurity. While the Excel-based matrix served as a valuable resource, its static nature and limitations in scalability and user accessibility highlighted the need for a more dynamic and user-friendly tool. To address these challenges, a web application was developed to transform the static Compliance Matrix into an interactive, accessible, and efficient platform. The web application aims to simplify the compliance mapping process, enhance collaboration among stakeholders, and provide real-time access to compliance data. By leveraging modern web technologies and intuitive design principles, the application addresses the limitations of the Excel matrix and offers a robust solution for organizations striving to meet the stringent requirements of both ISO/SAE 21434 and ASPICE for Cybersecurity.

One of the primary motivations for creating the web application was to facilitate a seamless and bidirectional mapping between ISO/SAE 21434 requirements and ASPICE base practices. In the complex landscape of automotive cybersecurity, organizations often grapple with understanding how the requirements of one standard correlate with those of another. The web application addresses this challenge by allowing users to navigate mappings from ISO requirements to ASPICE base practices and vice versa. This bidirectional capability empowers organizations to approach compliance from either standard, depending on their existing processes or strategic focus. The web application's user-friendly interface is designed to enhance accessibility and usability. Unlike the Excel matrix, which can become cumbersome with large datasets and complex mappings, the web application provides intuitive navigation and interactive features. Collaboration is a critical aspect of compliance management, often involving cross-functional teams that include cybersecurity experts, software engineers, quality assurance personnel, and project managers. The web application supports collaborative workflows by enabling multiple users to access and update compliance data in real-time. Role-based access controls ensure that sensitive information is protected while allowing team members to contribute effectively. This collaborative environment fosters better communication, reduces redundancies, and ensures that all stakeholders are aligned in their compliance efforts. Another significant advantage of the web application is its ability to centralize and manage documentation related to compliance activities. Users can upload, store, and organize documents such as policies, procedures, audit reports, and evidence of compliance directly within the application. This central repository simplifies document management, enhances traceability, and facilitates audit preparation. Auditors can be granted controlled access to relevant documentation, streamlining the audit process and building confidence in the organization's compliance posture.

The scalability of the web application is particularly important in the context of evolving industry standards and organizational growth. As compliance requirements change or expand, the application can be updated to incorporate new mappings,

BUPT

features, and functionalities without disrupting existing workflows. This adaptability ensures that the tool remains relevant and continues to meet the needs of organizations over time. From a technical perspective, the development of the web application involved careful consideration of performance, security, and reliability. Leveraging modern web development frameworks and cloud-based technologies, the application is designed to provide fast, responsive interactions while maintaining robust security measures to protect sensitive compliance data. Regular updates and maintenance ensure that the application adheres to best practices in cybersecurity and data protection.

The impact of the web application on organizations adopting it has been significant. By streamlining the compliance mapping process, reducing administrative overhead, and enhancing collaboration, organizations have reported improved efficiency and reduced costs associated with compliance management. The ability to quickly identify and address compliance gaps has led to better audit outcomes and a stronger overall cybersecurity posture. Additionally, the application's intuitive design and user-friendly features have contributed to higher user adoption rates and satisfaction.

In the context of the case studies presented in the following chapter, the web application played a pivotal role in facilitating the cost reductions achieved by the Tier 1 suppliers. By providing a dynamic platform for mapping non-conformances and managing compliance data, the suppliers were able to streamline their audit processes, allocate resources more effectively, and focus on strategic improvements rather than administrative tasks. Looking ahead, the web application serves as a foundation for further innovation and enhancement. Plans for future development include integrating advanced analytics to provide deeper insights into compliance trends, incorporating machine learning algorithms to predict potential compliance issues, and expanding the application's capabilities to support additional industry standards. These developments aim to provide organizations with even greater value, enabling them to navigate the complexities of automotive cybersecurity compliance with confidence and agility.

4.1 Development and Features of the Web Application

To enhance the usability and accessibility of the Compliance Matrix, a web application was developed using Laravel, a robust PHP framework known for its elegant syntax and powerful features. This application transforms the static Excel-based Compliance Matrix into an interactive and user-friendly platform, allowing organizations to efficiently manage compliance with ISO/SAE 21434 and ASPICE for Cybersecurity standards.

User Registration and Account Management

The web application enables users to create new accounts through a straightforward registration process. Upon successful registration, users gain access to features tailored to streamline compliance activities. User authentication ensures that only authorized personnel can access sensitive project information, maintaining the integrity and confidentiality of the compliance data.

BUPT

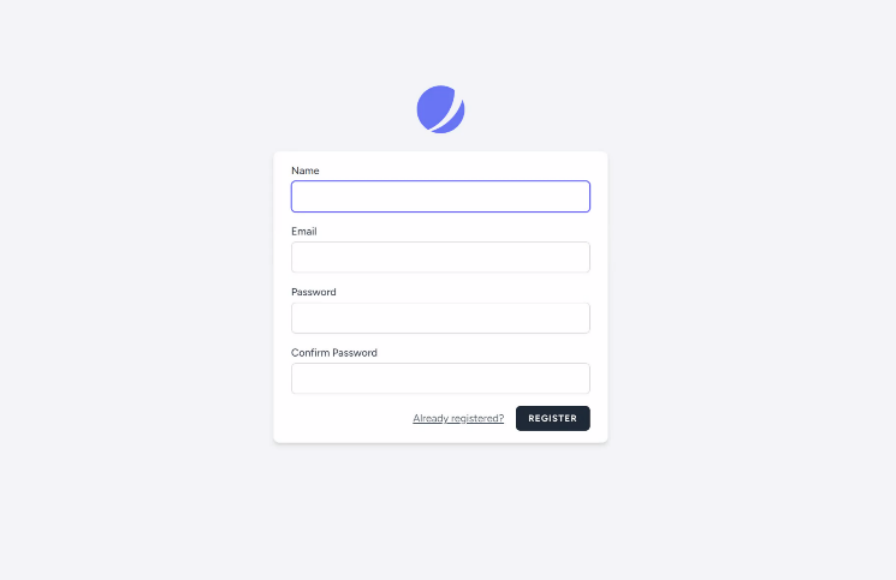


Fig. 50. Web Application User Registration

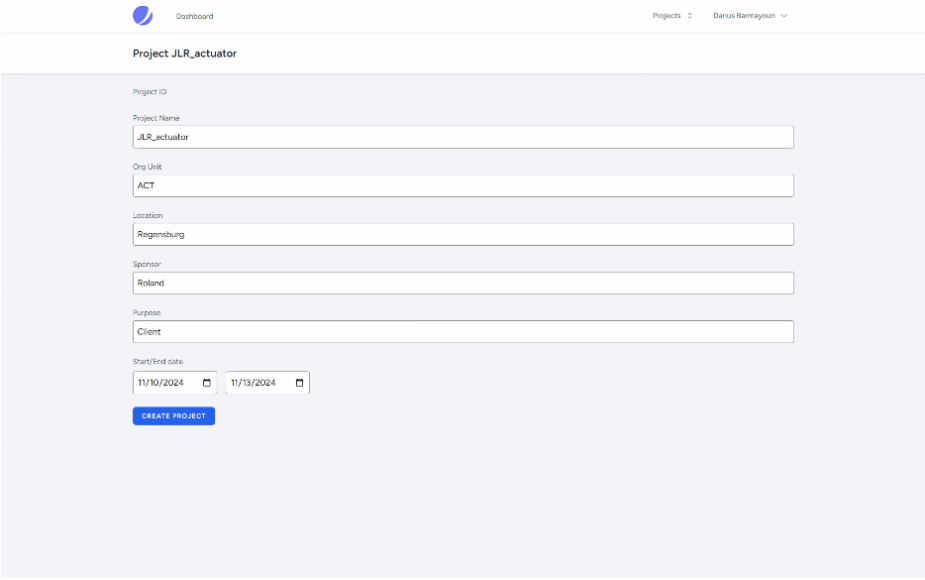


Fig. 51. Web Application Project Creation

Project Creation and Management

After logging in, users are presented with a list of all available projects within the tool or have the option to create a new one. When creating a new project, users can input

BUPT

essential project information, including the project name, description, and relevant details. They can also assign a responsible lead assessor and add other assessors involved in the project. This collaborative feature ensures that all team members are aligned and can contribute effectively to the compliance assessment process.

Dual Compliance Views: ISO-ASPICE and ASPICE-ISO

The application offers two primary views to accommodate different starting points for compliance assessments: the ISO-ASPICE view and the ASPICE-ISO view. Users can choose which audit or assessment they wish to initiate based on their organizational needs or strategic focus. In the ISO-ASPICE view, users begin with the ISO/SAE 21434 requirements. The interface is divided into three columns. The left column displays all the relevant ISO requirements for the project. The middle column shows the mapped ASPICE base practices corresponding to each ISO requirement. The right column allows users to add observations in the form of comments or identified weaknesses. This structured layout facilitates a comprehensive understanding of how ISO requirements align with ASPICE practices, aiding in the identification of compliance gaps and areas requiring attention.

Conversely, the ASPICE-ISO view starts with the ASPICE base practices. The columns are arranged similarly: the left column lists the ASPICE base practices applicable to the project; the middle column displays the corresponding ISO/SAE 21434 requirements mapped to each ASPICE practice; and the right column provides space for users to add observations, comments, or note weaknesses. Observations added in either view are automatically synchronized and visible in the corresponding view, ensuring consistency and facilitating a holistic approach to compliance management.

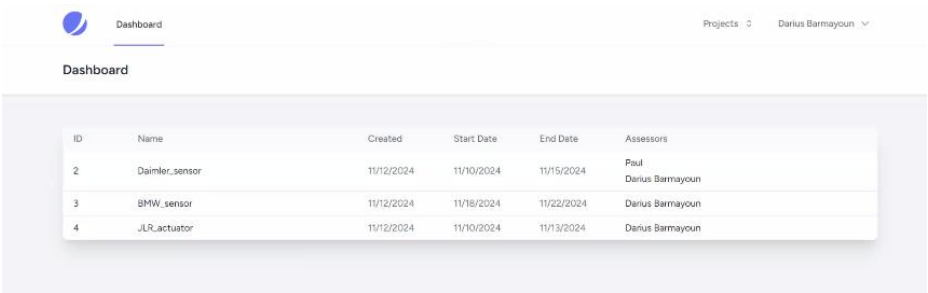


Fig. 52. Web Application Project List

Observations and Compliance Rating

The application allows users to document their findings and observations during the assessment process. Observations can be added as comments or noted weaknesses against each requirement or base practice, supporting thorough documentation and aiding in tracking compliance issues that need to be addressed. Each requirement or base practice can be rated using the NPLF scale, which stands for Not Achieved (N),

BUPT

Partially Achieved (P), Largely Achieved (L), and Fully Achieved (F). "Not Achieved" indicates that the requirement or practice has not been implemented or there is no evidence of its implementation. "Partially Achieved" means the requirement or practice has been implemented to some extent but lacks completeness or consistency. "Largely Achieved" signifies that the requirement or practice has been mostly implemented with minor gaps or areas for improvement. "Fully Achieved" denotes that the requirement or practice has been fully implemented, and there is comprehensive evidence of compliance. This rating system provides a clear and standardized method for assessing compliance levels, enabling organizations to prioritize remediation efforts and monitor progress over time.

Data Synchronization and Consistency

A key feature of the web application is the automatic synchronization of observations and ratings between the ISO-ASPICE and ASPICE-ISO views. When users add comments or identify weaknesses in one view, the information is seamlessly reflected in the corresponding elements of the other view. This ensures that all team members have access to the most up-to-date information, regardless of the starting point of their assessment, reducing the likelihood of data discrepancies or redundant efforts.

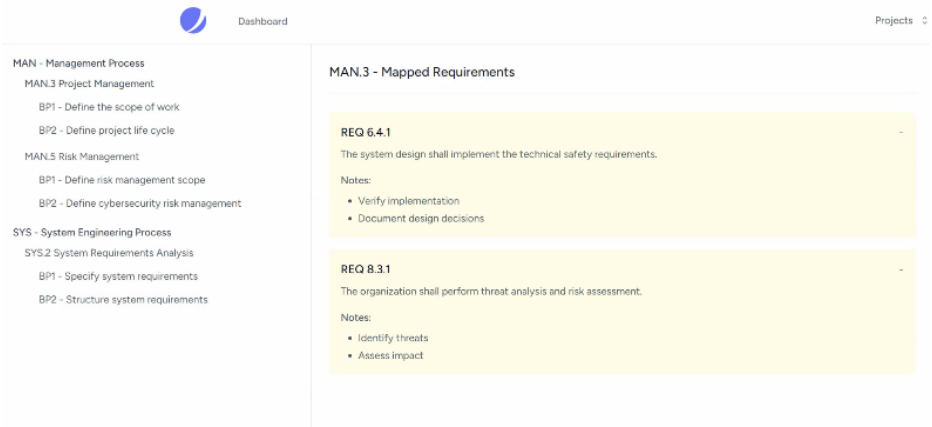


Fig. 53. Web Application ISO-ASPICE mapping

User Interface and Experience

The application is designed with an intuitive user interface that emphasizes ease of navigation and clarity of information. The layout organizes complex compliance data into manageable sections, allowing users to focus on specific requirements or practices without becoming overwhelmed. Search and filter functions enhance the user experience by enabling quick access to relevant information. Responsive design principles ensure that the application is accessible across various devices and screen sizes, accommodating users who may need to access the tool remotely or on different platforms.

BUPT

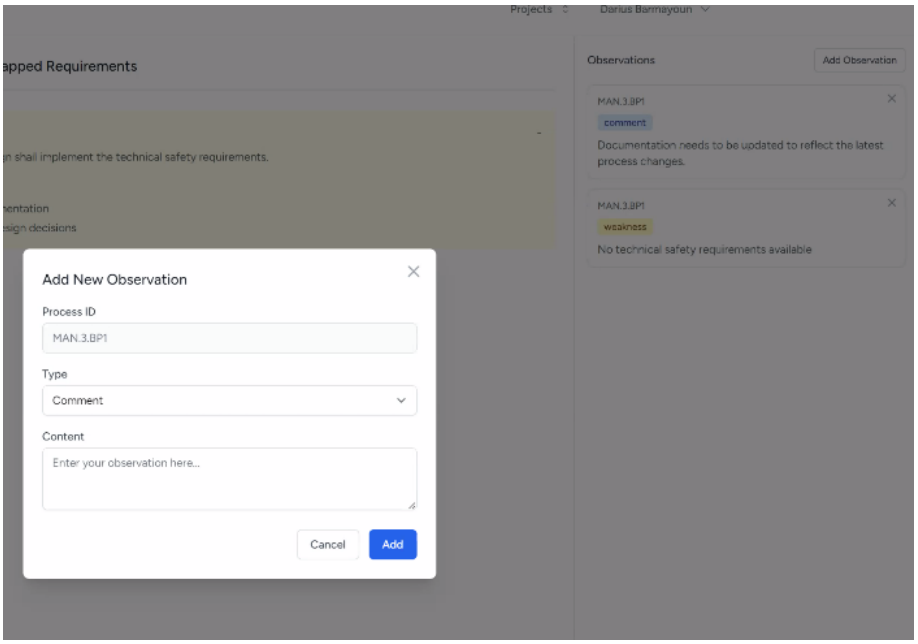


Fig. 54. Web Application Observations

Collaborative Features

Collaboration is facilitated through features that allow multiple users to work on the same project simultaneously. Role-based access controls enable administrators to assign permissions to different team members, ensuring that users have appropriate levels of access based on their roles and responsibilities. This collaborative environment supports teamwork and promotes a unified approach to compliance management.

4.2 Conclusion

The development of the web application represents a significant milestone in advancing compliance management within the automotive industry. By converting the static Excel-based Compliance Matrix into an interactive and user-friendly platform, the application effectively addresses the challenges associated with traditional compliance methods. It empowers organizations to navigate the complexities of ISO/SAE 21434 and ASPICE for Cybersecurity standards with greater ease, efficiency, and accuracy. The application's features ranging from user registration and project creation to dual compliance views and synchronized observations offer a comprehensive solution for managing compliance assessments. Users can seamlessly switch between the ISO-ASPICE and ASPICE-ISO views, allowing for flexibility in starting points and ensuring a thorough understanding of how the standards interrelate. The ability to add observations and rate compliance levels using the NPLF scale provides a standardized and

BUPT

transparent method for assessing compliance status, facilitating targeted remediation efforts and continuous improvement.

By fostering collaboration through real-time data synchronization and role-based access controls, the application enhances teamwork and ensures that all stakeholders are aligned in their compliance objectives. The intuitive user interface and responsive design make the tool accessible across various devices, accommodating the needs of diverse teams and enabling remote access when necessary. The web application not only streamlines the compliance process but also contributes to strengthening cybersecurity practices within organizations. By providing clear mappings between ISO requirements and ASPICE base practices, it helps organizations identify gaps, reduce redundancies, and implement effective controls to mitigate cybersecurity risks. The centralized platform for documentation and observations further aids in audit preparation and supports a proactive approach to compliance management.

In the subsequent chapters, the practical benefits and effectiveness of the web application will be demonstrated through two case studies involving Tier-1 suppliers. These organizations have utilized the application to prove compliance with ISO/SAE 21434 and ASPICE for Cybersecurity, achieving significant improvements in efficiency, cost reduction, and overall cybersecurity posture. The case studies will provide valuable insights into how the application functions in real-world scenarios, highlighting its role as an essential asset in the industry's compliance efforts. By bridging the gap between complex standards and practical implementation, the web application stands as a testament to the potential of innovative technological solutions in addressing industry challenges. It not only fulfills the immediate needs of compliance management but also contributes to a culture of continuous improvement and excellence in automotive cybersecurity.

BUPT

C. Case Studies and Financial Analysis

1 Case Study - A

This case study explores the practical application of a compliance matrix and accompanying web application designed to align ISO/SAE 21434 with ASPICE for Cybersecurity within a real-world automotive project. A Tier-1 supplier undertook the development of a cybersecurity-relevant component for a German Original Equipment Manufacturer (OEM), a task that demanded strict adherence to industry cybersecurity standards. During the ISO/SAE 21434 audit, multiple non-conformities were identified, revealing gaps in processes such as threat analysis, risk assessment, and documentation of cybersecurity goals and requirements. To address these challenges, the project team utilized the compliance matrix to map the ISO/SAE 21434 requirements to the corresponding base practices in ASPICE for Cybersecurity. This approach enabled a systematic analysis of each non-conformity, allowing the team to rectify deficiencies by aligning their processes with ASPICE practices like MAN.7 (Cybersecurity Risk Management) and SEC.1 and SEC.2. The web application enhanced this process by providing an interactive platform for navigating the mappings and rationalizations.

1.1 Case Study Introduction

In order to demonstrate the practical application and effectiveness of the compliance matrix developed between ISO/SAE 21434 and ASPICE for Cybersecurity, a comprehensive case study was conducted involving a Tier-1 supplier within the automotive industry. This supplier, recognized for its advanced engineering capabilities and commitment to quality, was engaged in a project that centered on the development of a cybersecurity-relevant component for a prominent German Original Equipment Manufacturer (OEM). The component in question was integral to the vehicle's critical systems and thus required adherence to stringent cybersecurity regulations to ensure its safe, secure, and reliable operation.

The automotive industry is witnessing an unprecedented convergence of technology and connectivity, leading to increased cybersecurity risks that can have severe implications for safety, privacy, and operational integrity. As such, automotive components, especially those with cybersecurity relevance, are subjected to rigorous standards and assessments to mitigate potential vulnerabilities. In this context, the Tier-1 supplier faced the dual challenge of not only meeting the technical specifications demanded by the OEM but also ensuring full compliance with industry cybersecurity standards, specifically ISO/SAE 21434 and ASPICE for Cybersecurity.

Recognizing the critical importance of adhering to these standards, the project was scheduled for both an ASPICE assessment—including the Add-on Module for Cybersecurity—and an ISO/SAE 21434 audit. The ASPICE assessment aimed to evaluate the maturity and capability of the supplier's software development processes, with a particular focus on cybersecurity practices. The ISO/SAE 21434 audit, on the other hand, was intended to assess the organization's adherence to the comprehensive cybersecurity

BUPT

engineering framework outlined by the standard, covering aspects such as risk assessment, threat analysis, requirements specification, implementation, verification, and validation.

During the ISO/SAE 21434 audit, multiple non-conformities were identified. These non-conformities highlighted areas where the project's processes and documentation did not fully align with the stringent requirements of the standard. Specific issues included gaps in the threat analysis and risk assessment processes, incomplete documentation of cybersecurity goals and requirements, insufficient evidence of cybersecurity validation activities, and a lack of clear assignment of responsibilities for cybersecurity tasks between the supplier and the OEM. These findings underscored the complexities inherent in complying with multiple, overlapping standards and the challenges organizations face in aligning their processes accordingly. The identification of non-conformities posed a significant risk to the project's timeline and the supplier's relationship with the OEM, necessitating prompt and effective corrective actions.

In response to these challenges, the project team decided to employ the compliance matrix and the accompanying web application developed as part of this work. The compliance matrix, which provides a detailed mapping between ISO/SAE 21434 requirements and ASPICE for Cybersecurity base practices, served as a crucial tool in addressing the identified non-conformities. By utilizing the matrix, the team was able to systematically analyze each non-conformity in the context of both standards, understanding how deficiencies in one area could be rectified by aligning with the corresponding practices in the other standard. The compliance matrix facilitated a more holistic understanding of the interrelations between the standards. It allowed the team to see how improvements in their processes could simultaneously satisfy multiple requirements, reducing duplication of effort and ensuring a more integrated approach to compliance. The web application enhanced this process by providing an interactive platform where the team could easily navigate between the standards, access rationalizations for each mapping, and track their progress in addressing the non-conformities. As the team worked through the non-conformities using the compliance matrix, they also prepared for the upcoming ASPICE assessment. By aligning their processes with the ASPICE base practices, they ensured that the necessary documentation, evidence, and process maturity were in place. This proactive approach not only addressed the immediate issues identified in the ISO audit but also positioned the team for success in the ASPICE assessment.

1.2 Identified non-conformances

During the ISO/SAE 21434 audit of the cybersecurity-relevant component developed by the Tier-1 supplier for the German OEM, several non-conformances were identified. These non-conformances highlighted gaps in the project's adherence to the stringent requirements of the standard and underscored areas needing immediate attention to ensure full compliance. This chapter details the specific non-conformances uncovered during the audit, their implications for the project, and how they were addressed using the compliance matrix and web application.

BUPT

The audit aimed to assess the supplier's cybersecurity engineering processes across various phases of the product lifecycle. It focused on key areas such as risk assessment, requirements management, design and implementation of cybersecurity controls, verification and validation activities, and management of distributed cybersecurity activities with the OEM. The findings revealed several non-conformances, which included incomplete threat analysis and risk assessment (TARA), insufficient documentation of cybersecurity goals and requirements, lack of evidence for cybersecurity validation activities, undefined responsibilities in distributed cybersecurity activities, inadequate attack path analysis and feasibility ratings, and missing risk treatment decisions and rationales.

One significant issue identified was the incomplete threat analysis and risk assessment (TARA). The audit revealed that the project's TARA did not fully adhere to the methodologies prescribed in Clause 15 of ISO/SAE 21434. Specifically, the project team had not comprehensively identified all assets with cybersecurity properties whose compromise could lead to damage scenarios, as required by asset identification in Clause 15.3. There was a lack of detailed threat scenarios, including targeted assets, compromised cybersecurity properties, and causes of compromise, as outlined in Clause 15.4. Additionally, the impact ratings for identified damage scenarios were not adequately determined across the required impact categories—safety, financial, operational, and privacy—as specified in Clause 15.5. Furthermore, attack paths realizing the threat scenarios were not thoroughly analyzed or documented, failing to meet the requirements of attack path analysis in Clause 15.6.

The implications of an incomplete TARA are significant. Potential cybersecurity risks may remain unidentified or inadequately assessed, leading to insufficient mitigation measures. This oversight could result in vulnerabilities that attackers might exploit, compromising the safety and integrity of the vehicle systems. To address this non-conformance, the team utilized the compliance matrix to map these requirements to the ASPICE for Cybersecurity process MAN.7 (Cybersecurity Risk Management), namely MAN.7.BP3 (Identify potential risks) and MAN.7.BP5 (Analyze potential risks and evaluate risks). By aligning with these base practices, the team enhanced their TARA processes to systematically identify all relevant assets and their cybersecurity properties, develop comprehensive threat scenarios with detailed descriptions, assign impact ratings based on standardized criteria, and conduct thorough attack path analyses to understand potential exploitation methods. The web application facilitated access to rationalizations and guidance on how to implement these practices effectively.

Another major issue was the insufficient documentation of cybersecurity goals and requirements. The audit found that the project lacked clear documentation of cybersecurity goals and derived cybersecurity requirements as per Clause 9 (Concept) of ISO/SAE 21434. The cybersecurity concept was not fully developed, and the traceability between identified risks and the specified cybersecurity measures was weak. Without well-defined cybersecurity goals and requirements, the development team might implement inadequate or misaligned security controls, leading to gaps in security measures and making the system vulnerable to cyberattacks. To rectify this non-conformance, the team referred to the compliance matrix mapping to ASPICE for Cybersecurity Base Practices SEC.1.BP1 (Derive cybersecurity goals and cybersecurity

BUPT

requirements), SEC.1.BP2 (Establish bidirectional traceability), and SEC.1.BP3 (Ensure consistency). By adopting these base practices, the team established clear cybersecurity goals derived from the TARA results, developed detailed cybersecurity requirements linked to the identified risks, ensured bidirectional traceability between the cybersecurity requirements and the cybersecurity goals, and between the cybersecurity goals and the threat scenarios. They also ensured consistency between these elements, verifying that the cybersecurity requirements effectively addressed the cybersecurity goals and the identified threats. The web application provided templates and examples to guide the documentation process, enhancing the quality and completeness of the cybersecurity requirements.

The audit also revealed a lack of evidence for cybersecurity validation activities. Clause 11 of ISO/SAE 21434 requires validation of cybersecurity measures at the vehicle level. However, the audit found insufficient evidence of such activities, including test plans, procedures, and results demonstrating that the implemented controls met the cybersecurity goals. Without proper validation, there is no assurance that the cybersecurity measures effectively mitigate the identified risks, potentially leaving residual vulnerabilities undetected before the product's release. Addressing this issue, the compliance matrix guided the team to align with ASPICE for Cybersecurity processes SEC.4.BP1 (Develop risk treatment validation strategy) and SEC.4.BP2 (Develop specification for risk treatment validation). By implementing these base practices, the team developed comprehensive validation strategies outlining how the cybersecurity controls would be validated. They then developed detailed specifications for risk treatment validation, including test cases suitable to provide evidence of achieving the associated cybersecurity goals. This approach ensured that the validation activities were systematically planned and executed. The team conducted the validation activities according to these specifications and documented the results, thereby fulfilling the requirements of Clause 11.

The audit further highlighted inadequate attack path analysis and feasibility ratings. The attack path analysis performed did not meet the detailed requirements of Clauses 15.6 and 15.7, and the attack feasibility ratings were not determined using a defined method. There was no evidence of using approaches like the attack potential-based or CVSS-based methods. Incomplete analysis of attack paths and inadequate feasibility ratings hinder accurate risk valuation, which may result in underestimating the likelihood of attacks and insufficient prioritization of mitigation efforts. By aligning with ASPICE's process MAN.7.BP5 (Analyze potential risks and evaluate risks), the team conducted comprehensive attack path analyses for each threat scenario and determined attack feasibility ratings using standardized methods recommended by ISO/SAE 21434, such as the attack potential-based approach. This allowed for accurate assessments of the effort required by potential attackers, enabling the team to update risk values accordingly and prioritize mitigation strategies effectively.

Finally, the audit found missing risk treatment decisions and rationales. For several identified risks, the project did not document the risk treatment decisions or provide rationales for retaining, reducing, avoiding, or sharing the risks, as required by Clause 15.9. Without documented risk treatment decisions and rationales, it is unclear how risks are managed, and this lack of transparency can lead to unmanaged risks and

BUPT

challenges during audits or assessments. Referencing ASPICE process MAN.7.BP6 (Define risk treatment option), the team documented risk treatment decisions for each threat scenario and provided rationales for the chosen options, including any cybersecurity claims for accepted or shared risks. They ensured that risk treatment strategies were aligned with the overall cybersecurity concept, enhancing transparency and accountability in their risk management processes.

1.3 Cost Reduction through the Use of the Compliance Matrix

The utilization of the compliance matrix in the project not only facilitated the alignment of ISO/SAE 21434 requirements with ASPICE for Cybersecurity base practices but also led to significant cost reductions during the subsequent ASPICE assessment by approximatively 52%. By proactively addressing the non-conformances identified during the ISO/SAE 21434 audit and mapping them to the relevant ASPICE base practices using the compliance matrix, the project team effectively closed gaps that might have otherwise resulted in additional findings during the ASPICE assessment. This strategic approach streamlined the assessment process, reduced the time and resources required, and ultimately contributed to cost savings for the Tier-1 supplier.

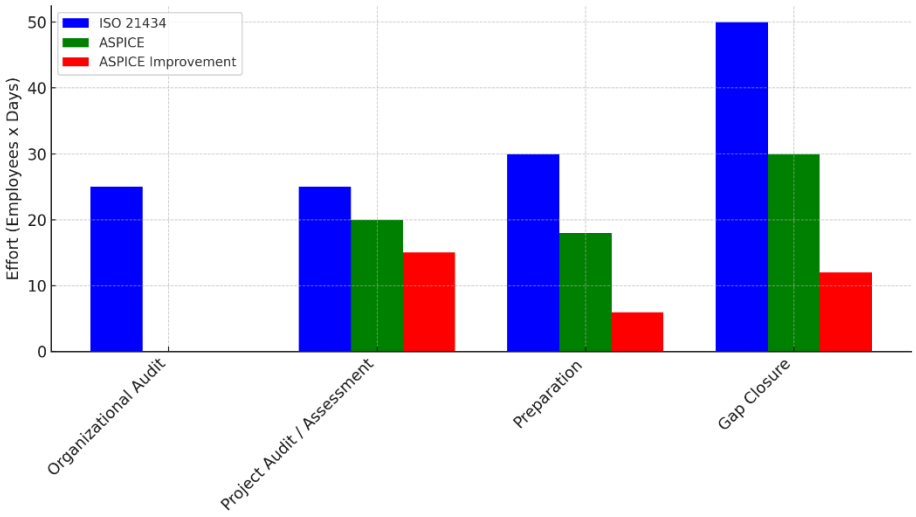
The project team conducted an ISO/SAE 21434 audit prior to the ASPICE assessment, during which non-conformances were identified and resolved. Each issue was mapped to corresponding ASPICE base practices using the compliance matrix. This proactive approach minimized duplicate efforts, allowing the team to prepare for the ASPICE assessment with many potential non-conformances already addressed. In each category, the effort required for the ASPICE assessment was substantially reduced, measured in terms of the number of employees involved and the number of days required to complete each task. For instance, the Project Audit effort was reduced from five employees over four days to five employees over three days due to the prior closure of ISO-related non-conformances. The Preparation Phase saw a reduction from six employees over three days to six employees over just one day. This reflects how the compliance matrix and early non-conformance closures enabled streamlined preparation, with much of the groundwork already completed during the ISO audit. In the Gap Closure Phase, what initially required six employees over five days for ISO gap closure was reduced to six employees over two days for ASPICE. This demonstrates the direct impact of the compliance matrix in addressing overlapping requirements and closing compliance gaps efficiently.

These numbers illustrate how a structured approach to compliance using the compliance matrix to systematically map and address requirements across both standards can lead to substantial cost and resource efficiencies. The compliance matrix served as a critical tool in this cost-saving endeavor by providing a clear mapping between ISO/SAE 21434 requirements and the ASPICE for Cybersecurity base practices. This enabled the project team to identify overlapping areas and address them comprehensively. The prior resolution of these issues meant that the ASPICE assessors encountered fewer non-conformances, which reduced the duration of the assessment and minimized the need for extensive corrective actions post-assessment.

BUPT

Table 5. Efforts reduction in case an ISO/SAE Audit was already conducted (Values expressed as Number of involved Employees x Number of Days)

	ISO 21434	ASPICE	ASPICE Improvemnt
Organizational Audit	5x5		
Project Audit / Assessment	5x5	5x4 ->	5x3
Preparation	6x5	6x3 ->	6x1
Gap closure	10x5	6x5 ->	6x2



By addressing the non-conformances identified during the ISO/SAE 21434 audit before the ASPICE assessment, the project team reaped several benefits. With many potential non-conformances already resolved, ASPICE assessors required less time to review and evaluate the project's compliance. This reduction in assessment time translated directly into lower costs associated with assessor fees and resource allocation. Proactively closing gaps avoided the need for extensive rework that would have been necessary if issues were discovered during the ASPICE assessment. Resources could be focused on enhancing processes and documentation rather than addressing a large number of non-conformances, contributing to overall cost savings. A clearer understanding of compliance status allowed project management to plan more effectively, reducing uncertainties and potential delays that often lead to increased costs.

The compliance matrix played an active role in achieving these cost reductions by providing clear traceability between the standards, facilitating comprehensive documentation, supporting training and awareness, and enhancing communication with

BUPT

assessors. By mapping ISO/SAE 21434 requirements to ASPICE base practices, the team could understand how addressing specific ISO non-conformances would impact ASPICE compliance, allowing for targeted improvements that served both standards. The guidance offered by the compliance matrix helped develop documentation that satisfied both ISO/SAE 21434 and ASPICE requirements, reducing the likelihood of documentation-related non-conformances during the ASPICE assessment.

Furthermore, the compliance matrix served as an educational tool for the project team, increasing awareness and understanding of the standards, which reduced errors and omissions that could lead to non-conformances. The availability of evidence demonstrating compliance with both standards facilitated smoother communication with ASPICE assessors, building confidence and trust.

While the compliance matrix significantly reduced the number of potential non-conformances, it is important to acknowledge that other non-conformances could still be identified during the ASPICE assessment. This is because not all ASPICE base practices have direct mappings to ISO/SAE 21434 requirements. Some ASPICE practices address areas not explicitly covered by ISO/SAE 21434, and thus, compliance with ISO does not guarantee full compliance with ASPICE. The project team was prepared for this possibility and remained committed to continuous improvement. The use of the compliance matrix did not eliminate the need for a thorough ASPICE assessment but rather enhanced the team's readiness by addressing overlapping areas in advance. This proactive approach minimized surprises during the assessment and allowed the team to focus on the specific ASPICE practices that required attention.

Quantifying the exact cost savings achieved through the use of the compliance matrix involves considering several factors. The ASPICE assessment was completed in a shorter timeframe than initially projected, leading to lower assessor fees and less disruption to the project schedule. Fewer non-conformances meant that the team spent less time and resources on corrective actions after the assessment, which often involve rework, additional documentation, and potential delays. The alignment of processes with both standards increased operational efficiency, reducing waste and improving productivity. Demonstrating compliance with both standards and effective cybersecurity management enhanced the supplier's reputation, potentially leading to increased business opportunities and revenue. While precise figures may vary, the overall impact on cost reduction was significant and positively influenced the project's budget and timeline.

For the Tier-1 supplier, the successful use of the compliance matrix provided strategic value beyond immediate cost savings. Demonstrating a proactive approach to compliance and cybersecurity management reinforced trust with the Original Equipment Manufacturer (OEM), potentially leading to long-term partnerships and preferred supplier status. Showcasing the ability to efficiently manage compliance with complex standards positions the supplier as an industry leader, attracting new customers and projects. The processes and lessons learned from this project can be applied to future projects, multiplying the cost-saving benefits over time.

In conclusion, the use of the compliance matrix in aligning ISO/SAE 21434 requirements with ASPICE for Cybersecurity base practices significantly contributed to cost reductions during the ASPICE assessment. By proactively addressing non-conformances identified in the ISO audit and mapping them to ASPICE practices, the project

BUPT

team minimized the potential for additional findings, reduced assessment duration, and optimized resource allocation. While acknowledging that some non-conformances may still be identified due to unmapped ASPICE practices, the overall impact was a streamlined assessment process with tangible cost savings. This case underscores the practical benefits of the compliance matrix as a tool for not only achieving compliance but also enhancing efficiency and reducing costs. For the Tier-1 supplier, these advantages translate into competitive strength, improved relationships with OEMs, and a foundation for continued success in managing cybersecurity within the automotive industry.

BUPT

2 Case Study – B

2.1 Case Study Introduction

In the rapidly evolving automotive industry, cybersecurity has become a paramount concern for Original Equipment Manufacturers (OEMs) and their suppliers. The increasing integration of advanced electronics, connectivity features, and autonomous driving capabilities in vehicles has expanded the potential attack surface for cyber threats. As a result, ensuring robust cybersecurity measures throughout the automotive supply chain is not just a regulatory requirement but also a critical component of maintaining brand reputation and customer trust.

This case study examines the proactive approach taken by a Tier 1 supplier collaborating with a prominent German OEM to enhance their cybersecurity posture. The Tier 1 supplier had previously conducted an Automotive Software Process Improvement and Capability dEtermination (ASPICE) assessment to evaluate and improve their software development processes. Recognizing the interconnected nature of software quality and cybersecurity, the supplier sought to align their existing processes with the ISO/SAE 21434 standard, which provides a comprehensive framework for automotive cybersecurity engineering. To achieve this alignment efficiently, the supplier utilized the Compliance Matrix Web Tool to map the non-conformances identified during the ASPICE assessment to the corresponding requirements in ISO/SAE 21434. This strategic use of the compliance matrix enabled the supplier to leverage the work already done during the ASPICE assessment, thus avoiding duplication of efforts and resources. By identifying the overlaps and gaps between the two standards, the supplier was able to address cybersecurity requirements more comprehensively while optimizing their resource allocation. The decision to map ASPICE non-conformances to ISO/SAE 21434 requirements was driven by several factors. First, both standards emphasize the importance of systematic processes and continuous improvement in managing complex automotive systems. While ASPICE focuses on software development capability, ISO/SAE 21434 extends this focus to encompass cybersecurity considerations throughout the product lifecycle. The overlap between the standards presents an opportunity for organizations to create synergies in their compliance efforts. Second, the German OEM required its suppliers to demonstrate compliance with both ASPICE and ISO/SAE 21434 standards. By aligning their processes with both standards concurrently, the Tier 1 supplier aimed to meet the OEM's expectations more effectively. This alignment not only facilitated smoother collaboration with the OEM but also positioned the supplier as a forward-thinking partner committed to the highest standards of quality and security.

Throughout this case study, we will explore how the Tier 1 supplier implemented the mapping process using the Compliance Matrix Web Tool. Moreover, this case study serves as an illustrative example for other organizations in the automotive industry seeking to harmonize their compliance efforts. By sharing the experiences and insights gained by the Tier 1 supplier, we aim to provide practical guidance on leveraging existing assessments to meet multiple standards. This approach not only streamlines compliance activities but also fosters a culture of continuous improvement and proactive

BUPT

risk management. The integration of ASPICE assessment findings with ISO/SAE 21434 requirements exemplifies a strategic approach to managing complex compliance landscapes. As cybersecurity threats continue to evolve, such proactive measures are essential for organizations to safeguard their products, protect consumer data, and maintain competitive advantage in the global automotive market. This case study underscores the importance of collaboration, innovation, and strategic planning in achieving these goals.

2.2 Identified non-conformances

During the ASPICE assessment conducted by the Tier 1 supplier collaborating with the German OEM, several non-conformances were identified across various base practices. These non-conformances highlighted areas where the supplier's processes did not fully align with the expectations set forth by the ASPICE framework. Recognizing the critical importance of addressing these gaps not only for ASPICE compliance but also for meeting the requirements of ISO/SAE 21434, the supplier utilized the Compliance Matrix Web Tool to map these non-conformances to the corresponding ISO standards. This strategic mapping facilitated a more comprehensive remediation approach, ensuring that corrective actions would enhance compliance with both ASPICE and ISO/SAE 21434, thereby strengthening the organization's overall cybersecurity posture.

One of the key non-conformances was identified in the area of supplier evaluation, specifically relating to the ASPICE base practice that requires organizations to evaluate potential suppliers by collecting information about their capabilities and assessing this information against established criteria. This base practice mandates documenting the results and short-listing preferred suppliers, ensuring that the evaluation process is thorough and systematic. The non-conformance arose because the supplier lacked a formalized process for evaluating the cybersecurity capabilities of potential suppliers. There was insufficient evidence that the organization systematically collected and analyzed information regarding suppliers' cybersecurity management systems, previous cybersecurity assessment reports, or their adherence to relevant cybersecurity standards. This deficiency was mapped to ISO/SAE 21434 requirements RQ-07-01 and RC-07-02. Requirement RQ-07-01 stipulates that the capability of a candidate supplier to develop and perform post-development activities in accordance with ISO/SAE 21434 must be evaluated. This evaluation supports supplier selection and can be based on the supplier's capability to conform to the standard or on previous implementations of other national or international cybersecurity standards. Additionally, RC-07-02 suggests that suppliers should provide a record of their cybersecurity capability to support the customer's evaluation. This record may include evidence of the organization's cybersecurity management practices, continual cybersecurity activities, incident response capabilities, and summaries of previous cybersecurity assessment reports. By mapping the ASPICE non-conformance to these ISO/SAE 21434 requirements, the supplier recognized the necessity of enhancing their supplier evaluation processes to incorporate comprehensive cybersecurity assessments. This led to the development of new evaluation criteria that specifically addressed the cybersecurity capabilities of potential suppliers. The organization implemented procedures to collect detailed information about suppliers'

BUPT

cybersecurity management systems, previous assessment outcomes, and their ability to comply with ISO/SAE 21434. This alignment not only rectified the ASPICE non-conformance but also ensured that the supplier's selection process was robust, reducing the risk of cybersecurity vulnerabilities originating from third-party components or services.

Another significant non-conformance was found in the domain of customer-supplier agreement management. The ASPICE base practices ACQ.4.BP2 and ACQ.4.BP5 require organizations to use defined joint interfaces for the exchange of all agreed information and to act to correct deviations when agreed objectives are not achieved. This includes negotiating changes to objectives and documenting them in agreements. The non-conformance emerged due to inadequate communication protocols between the customer and supplier when dealing with unclear, infeasible, or conflicting requirements. There was a lack of formal mechanisms to ensure that both parties were promptly notified and could take appropriate actions to resolve such issues. This issue was mapped to ISO/SAE 21434 requirement RQ-07-07, which mandates that if requirements are unclear, not feasible, or conflict with other cybersecurity requirements or requirements from other disciplines, both the customer and supplier must notify each other so that appropriate decisions and actions can be taken. By aligning with this ISO requirement, the supplier took steps to enhance their communication processes. They established clear protocols for issue escalation, ensuring that any ambiguities or conflicts in requirements were immediately communicated to the relevant stakeholders. This improved collaboration facilitated timely resolution of issues, minimizing the potential impact on project timelines and cybersecurity risk.

In the area of cybersecurity requirements allocation, a non-conformance was identified related to the ASPICE base practice SEC.2.BP2, which involves allocating cybersecurity requirements to one or more elements of the architectural design. The non-conformance indicated that the supplier did not consistently allocate defined cybersecurity requirements to specific system or software components within the architectural design. This gap posed a risk that certain components might not receive the necessary cybersecurity protections, potentially leading to vulnerabilities in the final product. This deficiency was mapped to ISO/SAE 21434 requirement RQ-10-02, which requires that defined cybersecurity requirements be allocated to components of the architectural design. By recognizing this alignment, the supplier undertook a thorough review of their architectural design processes. They implemented procedures to ensure that all cybersecurity requirements were systematically allocated to the appropriate components, with clear documentation and traceability. This involved cross-functional collaboration between system architects, cybersecurity experts, and software engineers to validate that each requirement was addressed adequately. The enhancement of this process not only resolved the ASPICE non-conformance but also strengthened the overall security architecture of the product.

A further non-conformance was detected in the development of a risk treatment validation strategy. The ASPICE base practice SEC.4.BP1 requires organizations to develop and implement a validation strategy that examines whether the associated cybersecurity goals are achieved. This includes utilizing cybersecurity-relevant methods to detect unidentified vulnerabilities, such as penetration testing. The non-conformance

BUPT

occurred because the supplier did not provide a clear rationale for the selection of validation activities within their strategy. There was a lack of documented reasoning behind the chosen methods and techniques, which could undermine the effectiveness of the validation process. This issue was mapped to ISO/SAE 21434 requirement RQ-11-02, which states that a rationale for the selection of validation activities must be provided. In response, the supplier revised their risk treatment validation strategy to include comprehensive justifications for each selected validation activity. They assessed the specific risks associated with their product and identified validation methods that were most effective in addressing those risks. The rationale considered factors such as the potential impact of identified threats, the feasibility of different validation techniques, and the resources available. By providing this detailed rationale, the supplier enhanced the credibility and effectiveness of their validation efforts, ensuring that the cybersecurity goals were met and that unidentified vulnerabilities were more likely to be detected and addressed.

Throughout this process of mapping ASPICE non-conformances to ISO/SAE 21434 requirements, the supplier leveraged the Compliance Matrix Web Tool to facilitate accurate and efficient alignment. This tool enabled them to identify direct correspondences between the two standards, ensuring that corrective actions were comprehensive and strategically targeted. By addressing the non-conformances in a manner that satisfied both ASPICE and ISO/SAE 21434, the supplier not only improved their immediate compliance status but also established more robust and integrated processes for managing cybersecurity risks. The resolution of these non-conformances had several positive outcomes for the supplier. It enhanced their overall cybersecurity management system by embedding cybersecurity considerations more deeply into their processes. It also improved collaboration and communication with both suppliers and customers, fostering stronger relationships and trust. Additionally, by proactively addressing these issues, the supplier positioned themselves as a responsible and forward-thinking partner, potentially opening up new business opportunities and reinforcing their reputation in the industry. Therefore, the identification and mapping of non-conformances during the ASPICE assessment to ISO/SAE 21434 requirements played a pivotal role in enhancing the Tier 1 supplier's processes and cybersecurity posture. By utilizing the Compliance Matrix Web Tool, the supplier was able to systematically address gaps in their practices, ensuring compliance with critical industry standards. This strategic approach not only rectified specific deficiencies but also contributed to the development of a more resilient and secure product, ultimately benefiting both the supplier and the OEM. The case exemplifies the value of integrated compliance efforts and the importance of continuous improvement in the face of evolving cybersecurity challenges in the automotive industry.

2.3 Cost Reduction through the Use of the Compliance Matrix

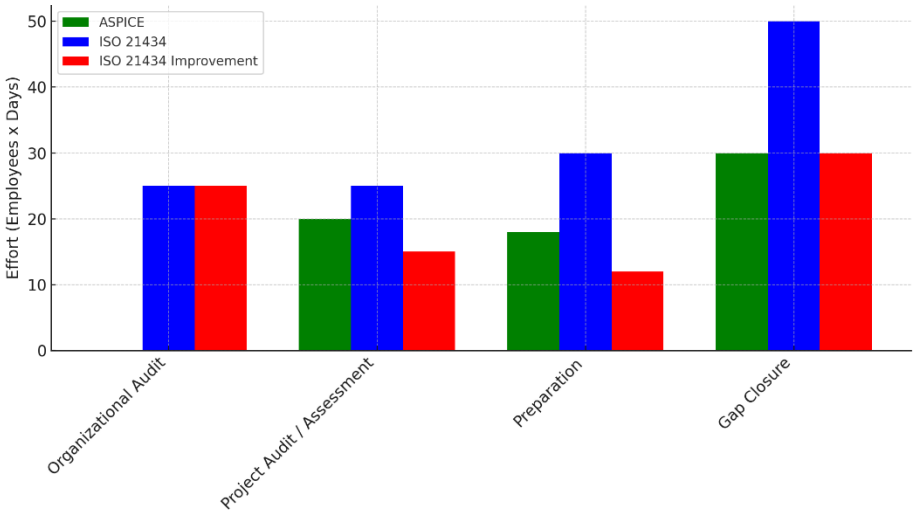
The strategic utilization of the Compliance Matrix Web Tool by the Tier 1 supplier not only facilitated the effective mapping of non-conformances from the ASPICE assessment to ISO/SAE 21434 requirements but also resulted in a 37% cost reductions during the subsequent ISO 21434 audit. By leveraging the work already completed during the

BUPT

ASPICE assessment, the supplier was able to streamline the ISO audit process, thereby optimizing resource allocation and reducing overall expenditure. This chapter explores the cost-saving benefits realized through this approach, highlighting the quantitative reductions in effort and resources across various phases of the ISO audit. The ISO 21434 audit encompasses several critical phases, including the organizational audit, project audit/assessment, preparation, and gap closure. Typically, these phases require substantial investment in terms of personnel and time. However, the prior completion of the ASPICE assessment provided a foundation upon which the supplier could build, especially by mapping the identified non-conformances to the corresponding ISO requirements using the compliance matrix. This mapping enabled the supplier to preemptively address potential issues, thus reducing the workload and resources needed for the ISO audit.

Table 6. Efforts reduction in case an ASPICE Assessment was already conducted (Values expressed as Number of involved Employees x Number of Days)

	ASPICE	ISO 21434	ISO 21434 Improvemnt
Organizational Audit		5x5 ->	5x5
Project Audit / Assessment	5x4	5x5 ->	5x3
Preparation	6x3	6x5 ->	6x2
Gap closure	6x5	10x5 ->	10x3



In the case of the organizational audit, there was no reduction in effort, remaining at five employees over five days. This is because the ASPICE assessment primarily

BUPT

focuses on software development processes and does not extensively cover organizational aspects related to cybersecurity management systems, policies, and governance structures required by ISO 21434. Consequently, the organizational audit necessitated a full evaluation to ensure compliance with the standard's requirements in this domain.

However, significant reductions were observed in other phases of the audit. The project audit/assessment phase saw a reduction from five employees over five days to five employees over three days. This decrease was achieved by leveraging the non-conformance mappings from the ASPICE assessment. Since the supplier had already identified and begun addressing issues related to project-specific cybersecurity processes, the ISO auditors could expedite their evaluation, focusing primarily on areas not covered by ASPICE or where additional ISO-specific requirements existed.

The preparation phase experienced a reduction from six employees over five days to six employees over two days. The compliance matrix facilitated this by providing a clear roadmap of the necessary documentation and evidence required for the ISO audit. With the mappings in place, the supplier's team could efficiently gather and organize the relevant materials, reducing the time spent on preparation. The familiarity gained during the ASPICE assessment also meant that the team was already well-versed in the processes and requirements, further streamlining the preparation efforts.

Similarly, the gap closure phase was reduced from ten employees over five days to ten employees over three days. By preemptively mapping and addressing the non-conformances identified during the ASPICE assessment, the supplier minimized the number of additional findings during the ISO audit. This proactive approach meant that fewer gaps needed to be closed post-audit, thereby reducing the resources required for remediation activities. The team could focus on addressing the remaining gaps more effectively, ensuring that all ISO requirements were met in a timely manner.

These quantitative reductions demonstrate how the strategic use of the compliance matrix can lead to substantial cost savings. By mapping ASPICE non-conformances to ISO 21434 requirements, the supplier effectively reduced duplication of effort and avoided redundant assessments. This not only saved time and resources but also allowed the supplier to allocate their personnel more efficiently across other critical project activities. The cost savings achieved through this approach extended beyond mere reductions in man-days. By shortening the duration of the ISO audit phases, the supplier also reduced the potential for project delays that could arise from prolonged audit activities. This helped maintain project timelines and ensured that deliverables to the OEM were met as scheduled, which is crucial in the competitive automotive industry where time-to-market can significantly impact market share and profitability. Moreover, the reduction in audit time translated to lower fees associated with external auditors. Since auditors typically charge based on the duration and complexity of the audit, minimizing the time required for each phase directly reduced the financial expenditure on audit services. Another critical aspect of the cost reduction was the improved readiness and efficiency of the supplier's team. The prior experience gained from the ASPICE assessment, and the use of the compliance matrix enhanced the team's understanding of the standards and the expectations of the auditors. This led to more effective communication during the audit, fewer misunderstandings, and quicker resolution of any issues that arose. The team's familiarity with the mapped requirements meant that

BUPT

they could provide accurate and comprehensive responses to auditor inquiries, further streamlining the audit process. The proactive identification and remediation of non-conformances contributed to a higher level of confidence among the auditors regarding the supplier's commitment to cybersecurity. This positive perception can influence the auditors to adopt a more collaborative approach, focusing on continuous improvement rather than penalizing non-compliance. Such a relationship can be beneficial for future audits and assessments, potentially leading to even greater efficiencies and cost savings over time.

The cost reduction achieved also had strategic implications for the supplier's relationship with the OEM. Demonstrating the ability to efficiently comply with ISO 21434 requirements showcased the supplier's commitment to cybersecurity and quality, reinforcing trust with the OEM. This could lead to preferential treatment in future projects, opportunities for deeper collaboration, and a stronger competitive position in the market. The methodologies and practices developed during this process can be institutionalized within the supplier's organization. By integrating the compliance matrix into their standard operating procedures, the supplier can replicate these cost-saving benefits across multiple projects and audits. This institutional knowledge becomes a valuable asset, enhancing the organization's overall capability in managing compliance and cybersecurity risks. This case illustrates the tangible benefits of integrating compliance efforts across multiple standards using tools like the compliance matrix. It demonstrates that proactive planning, efficient use of resources, and strategic alignment of processes can lead to substantial cost savings while enhancing compliance and cybersecurity posture. For organizations operating in the increasingly complex and regulated automotive industry, such approaches are not just advantageous but essential for maintaining competitiveness and ensuring the security and integrity of their products.

BUPT

3 Financial Analysis

3.1 Introduction

This chapter provides a detailed Cost-Benefit Analysis (CBA) centered around a specific case study in which the integrated compliance matrix was deployed to streamline assessment activities related to ISO/SAE 21434 and ASPICE for cybersecurity. In previous sections of this thesis, the theoretical underpinnings, practical functionalities, and qualitative advantages of the web-based compliance matrix were discussed at length. Now, the focus shifts to a quantitative examination of its economic and operational impact. By fostering an environment that encourages rapid adaptability and proactive security measures, the automotive industry can enhance the protection of its assets and maintain consumer trust [74]. The scenario under review involves a Tier 1 supplier located in Bavaria, Germany, that has already completed an ISO/SAE 21434 assessment using the web application. Having established a robust cybersecurity baseline through that initial assessment, the supplier subsequently planned and conducted an ASPICE for cybersecurity assessment. Traditionally, such assessments would require the project team to revisit a broad set of compliance obligations, prepare extensive documentation anew, and engage in lengthy interviews, often duplicating efforts already undertaken during the ISO/SAE 21434 phase. Many efforts have been made to simultaneously comply with key automotive cybersecurity standards. However, in some cases, these attempts have led to an increase in the "cost of quality" due to redundancy and overlap [75]. However, by relying on the integrated compliance matrix, the supplier was able to reuse much of the previously gathered evidence, easily identify any remaining gaps, and align the necessary activities to meet ASPICE criteria with significantly reduced manual work.

In essence, the compliance matrix serves as a structured interface that maps the relationships and overlaps between ISO/SAE 21434 and ASPICE requirements. This mapping not only provides clarity about what has already been fulfilled but also highlights precisely where additional effort is needed. As a result, preparation times for the subsequent assessment are shortened, the number of interviews and clarification sessions with assessors can be minimized, and any deficiencies discovered can be addressed more efficiently. All these improvements ultimately reflect a reduction in person-hours and related costs. While the qualitative benefits of such a matrix—improved transparency, streamlined processes, and better resource allocation—are clear, a robust economic argument requires quantified evidence. The CBA presented in this chapter compares the initially planned (or baseline) effort and costs for the ASPICE assessment (i.e., what would have been the case without using the integrated compliance solution) against the actual results achieved when the integrated matrix and web application were employed. Specifically, three key improvement areas will be highlighted:

- Reduced Preparation Effort: Instead of preparing from scratch for ASPICE compliance, the project team can directly leverage the outcomes of the ISO/SAE 21434 assessment. By doing so, tasks that would have normally required extensive

BUPT

document searches, artifact creation, or re-verification of cybersecurity measures are minimized.

- Lower Interview and Assessment Overheads: Assessors rely heavily on clear, well-structured evidence and concise reporting. With the compliance matrix, much of this groundwork is already laid out, reducing the hours spent in interviews and clarification sessions. This not only cuts labor costs but also shortens the overall assessment timeline, freeing resources for other mission-critical tasks.
- Accelerated Gap Closure and Continuous Improvement: When non-compliances or improvement areas are identified, the integrated matrix provides immediate guidance on how to address them by referencing both ISO/SAE 21434 and ASPICE requirements in parallel. This guidance speeds up the process of implementing corrective measures, lowering the effort needed post-assessment and ensuring that the project's cybersecurity posture matures more quickly.

By quantifying the time saved and extrapolating it into financial terms, the CBA will illuminate how the integrated compliance matrix adds tangible value. The analysis will draw upon actual recorded hours, rates, and project data, ensuring that the resulting conclusions rest on an empirical foundation. Furthermore, careful attention will be given to the assumptions, variables, and calculations underlying the CBA, thereby enhancing the credibility and reproducibility of the findings.

The chapter will begin by outlining the methodological approach to the CBA, detailing the data sources and assumptions used. Following that, the results of the analysis—expressed in terms of effort reduction, cost savings, and improved efficiency—will be presented and interpreted. In doing so, this chapter aims to bridge the gap between conceptual benefits and measurable financial outcomes, thereby providing a solid, data-backed business case for adopting the integrated compliance matrix as a standard operational tool. Ultimately, the insights gained here reinforce the proposition that integrating ISO/SAE 21434 and ASPICE compliance efforts through a single web-based platform can significantly streamline the assessment process. Beyond theoretical value, this chapter shows how such harmonization leads to real, demonstrable cost savings and productivity gains—key metrics that decision-makers require when evaluating new tools, methodologies, or strategic approaches in complex and highly regulated development environments.

3.2 Methodological Approach

This section outlines the methodology employed to conduct the Cost-Benefit Analysis (CBA) for evaluating the economic impact of utilizing the integrated compliance matrix between ISO/SAE 21434 and ASPICE for cybersecurity. It begins by establishing the theoretical underpinnings and standard practices of CBA, followed by a detailed explanation of the data sources and the methods used to gather and interpret relevant information from the case study. By adhering to recognized frameworks and ensuring data traceability, the analysis aims to produce credible and reproducible findings that can support informed decision-making.

BUPT

Theoretical Framework of CBA.
The benefit-cost ratio (BCR) is a profitability metric used in cost-benefit analysis to assess the feasibility of cash flows generated by an asset or project [76]. Its primary goal is to determine whether the net benefits of a proposed project, policy, or intervention outweigh its total costs. By converting diverse inputs ranging from labour hours and resource expenditures to time saved and potential risk reductions into comparable monetary terms, CBA provides a structured method for judging the economic desirability of an action. While often associated with public sector decision-making, the underlying principles of CBA are equally applicable in private sector contexts, where managers and stakeholders must choose how best to allocate limited resources among competing initiatives. At its core, the theoretical underpinnings of CBA rest on several key principles and assumptions:

Rational Decision-Making Under Resource Constraints. CBA assumes that decision-makers aim to use resources efficiently by selecting options that yield the greatest net social or organizational benefit. Underlying this concept is the idea that both public entities and private firms operate in environments of scarce resources—be they financial capital, personnel, or time—and must therefore prioritize investments based on their expected returns or improvements in organizational welfare.

Comprehensive Identification of Costs and Benefits. The starting point of any CBA is a thorough mapping of all relevant costs and benefits. Costs typically include direct expenses such as capital investments, labour, materials, training, licensing, and maintenance. They may also encompass indirect costs like administrative overhead, opportunity costs (the benefits of the next best alternative foregone), or even potential future liabilities arising from delayed implementation or compliance failures. Benefits, in contrast, are positive outcomes that enhance the value proposition of the project or action under review. These can be direct revenue gains, labour hour savings, reduced consultancy fees, or averted penalties. In a compliance context, such as evaluating cybersecurity standards, benefits could also appear as efficiency gains, minimized rework, accelerated project timelines, and improved readiness for subsequent audits. Although some benefits are tangible and easily expressed in monetary terms, others—such as reputational enhancement, knowledge accumulation, or lowered long-term risk—are intangible and harder to quantify. The theoretical framework of CBA acknowledges that while quantification is ideal, well-documented qualitative assessments can also be incorporated to enrich the analysis.

Monetization and Common Units of Measurement. A defining feature of CBA is its insistence on translating diverse costs and benefits into a single metric—most commonly a monetary unit—to facilitate direct comparison. By expressing both gains and losses in currency terms, CBA overcomes the challenge of evaluating heterogeneous factors. For example, saved person-hours are multiplied by the appropriate hourly rate to yield a financial measure of time savings. Reduced audit complexity might translate into fewer paid consultancy days, again yielding tangible cost reductions. This

BUPT

monetization ensures that decision-makers can assess trade-offs clearly, treating each option's cumulative benefit and cost profile as comparable "portfolios" of value.

Net Metrics of Economic Performance. Once all costs and benefits have been identified, monetized, and, if necessary, discounted, the analysis proceeds to aggregate them into summary measures. Common metrics include:

- Benefit-Cost Ratio (BCR): The ratio of total benefits to total costs. A BCR greater than 1.0 indicates that benefits outweigh costs [76]. The theoretical literature supports the use of these metrics as intuitive, standardized indicators of economic viability, simplifying complex arrays of inputs into manageable decision criteria. The formula for cost-benefit analysis under BCR is:

  BCR = ∑ PV of Benefits (cash inflows) / ∑ PV of costs (cash outflows).

- Net Present Value (NPV): The difference between the present value of total benefits and the present value of total costs [76]. A positive NPV suggests that benefits exceed costs, making the project potentially desirable.

  NPV = ∑ PV of benefits (cash inflows) – ∑ PV of costs (cash outflows)

Risk, Uncertainty, and Sensitivity Analysis. Real-world conditions are rife with uncertainties. Variables such as labour rates, number of compliance assessment cycles, and complexity of regulatory requirements may not be known with precision. Recognizing this, the theoretical framework of CBA encourages sensitivity and scenario analyses. By adjusting key parameters and assumptions, the analyst can gauge the robustness of the conclusions. For example, if varying employee hourly rates by ±10% does not meaningfully change the NPV or BCR, the outcome is considered stable and reliable. Conversely, if small parameter changes drastically alter conclusions, decision-makers are alerted to the need for further data refinement or cautious implementation.

Decision-Making Under the CBA Framework. Ultimately, the theoretical goal of CBA is to inform choices in a rational and transparent manner. Armed with clear measures of net economic advantage, stakeholders can evaluate whether to adopt, modify, or reject a given project. In organizational settings, the fundamental logic—selecting projects that maximize the net economic benefit—supports strategic resource allocation, fosters accountability, and encourages continuous improvement.

In applying this theoretical framework to the integrated compliance matrix scenario, the primary objective is to measure the cost savings and efficiency gains realized by streamlining two cybersecurity compliance processes. Although the core CBA concepts remain unchanged—identifying and quantifying benefits, comparing them to costs, and presenting results in accessible metrics—the specifics are tailored to a context where assessment preparation times, interview durations, and gap closure activities have direct financial implications. By grounding the subsequent analysis in these well-established theoretical principles, the forthcoming evaluation can produce credible,

BUPT

transparent, and actionable results that support informed decision-making and strategic planning.

Data Sources and Collection Methods.
The Cost-Benefit Analysis (CBA) conducted within this research is fundamentally reliant on accurate, consistent, and contextually relevant data. Without reliable input values—ranging from planned and actual labour hours to financial parameters such as hourly rates—any economic evaluation would lack credibility. This section provides a detailed account of how the data supporting the CBA were sourced, what types of information were collected, how these data were validated, and the roles various stakeholders played in compiling and interpreting these inputs.

Data Origination and Tools Used. A key element of the case study under analysis was the planning and execution of both ISO/SAE 21434 and ASPICE for cybersecurity assessments. The project management activities related to these assessments were carried out using a digital project planning tool called Float. This tool is commonly employed to schedule tasks, allocate resources, track progress, and document changes in planned versus actual effort. The decision to use Float as the primary data repository was driven by its integration into the engineering organization's established project management practices. Since Float was already routinely updated by the project management team, it represented a single, consistent source of truth for understanding scheduled tasks, assigned personnel, and recorded work durations. Within Float, project managers responsible for both system-level and software-level tasks meticulously recorded timelines and deliverables for each assessment phase. Activities related to ISO/SAE 21434 and ASPICE compliance—such as preliminary document reviews, interview sessions with engineers, evidence compilation, and remediation of gaps—were assigned dedicated time slots and responsible persons. By comparing initial estimates (planned) to final records (actual), it became possible to determine discrepancies, sources of inefficiency, and the extent to which the integrated compliance matrix reduced preparatory work.

Types of Data Collected.

5. Planning and Scheduling Information: At the core of the analysis were the time-based data captured in Float. For both the ISO/SAE 21434 and ASPICE for cybersecurity assessments, the project management team established baseline (planned) timelines that reflected the anticipated effort required for various assessment activities. This included the scheduling of interviews with key subject matter experts, allocation of time for document reviews, and setting aside blocks of work hours for performing pre-assessment checks or post-assessment remediation. Recording these planned values provided a reference scenario against which actual performance could be measured.
6. Interview Sessions' Duration and Frequency: A significant portion of compliance assessments involves interviews and discussions with stakeholders who possess domain-specific knowledge—system architects, software developers, quality

BUPT

assurance personnel, and cybersecurity engineers. Float was used to plan these sessions in advance, estimating their duration based on previous assessments or industry benchmarks. After the interviews took place, the actual durations were logged. By comparing the planned interview lengths with actual durations, the analysis could reveal whether the integrated compliance matrix reduced the time needed for clarifications and additional inquiries, thus contributing to efficiency gains.

7. Pre-Assessment and Post-Assessment Activities: Achieving compliance is not limited to the assessment event itself. It involves a series of preparatory tasks before the formal assessment begins (e.g., collating documentation, mapping requirements to artifacts, identifying initial gaps) and follow-up tasks afterwards (e.g., implementing improvement measures, closing identified gaps, finalizing compliance reports). Float's records included these pre- and post-assessment activities as discrete tasks, each with an estimated timeframe and a responsible individual or team. Capturing both planned and actual durations of these tasks allowed for a nuanced understanding of where time savings occurred across the entire compliance lifecycle, not just during the formal assessment interviews.
8. Hourly Rates and Financial Parameters: Converting saved labour hours and reduced interview times into monetary values necessitated the collection of financial parameters. The project's internal accounting and human resources teams provided fully burdened hourly rates for employees based on their roles and seniority levels. Similarly, for external assessors and consultants, contract agreements were reviewed to determine standard daily or hourly rates. These financial metrics were then linked to time-saving data from Float, yielding quantifiable cost reductions. Such cost parameters provided the economic dimension that transformed raw time savings into meaningful indicators like reduced project costs, improved return on investment, and shortened payback periods.

3.3 Identification of Costs

When conducting a Cost-Benefit Analysis (CBA), one of the most fundamental steps involves accurately identifying and quantifying all cost elements associated with the introduction and utilization of new tools or methodologies. In this assessment scenario, we focus on a specialized compliance tool that integrates ISO/SAE 21434 and ASPICE requirements to reduce effort and enhance process efficiency. As previously discussed, using the tool has been shown to significantly cut down on both preparation and execution time. However, any new resource—even one that reduces overall costs—must be transparently accounted for in terms of its own direct expenses.

Subscription Costs

The primary cost associated with the tool under consideration is its annual subscription fee. For each employee granted access, a yearly charge of 150 EURO applies. Within the context of this particular assessment and project, an average of 15 employees from various disciplines and functional areas (system engineers, software developers, quality assurance staff, and cybersecurity specialists) are granted access to the tool. These

BUPT

individuals actively use the tool to prepare for and support both the ISO/SAE 21434 and ASPICE compliance audits. They rely on it for centralized documentation, streamlined cross-referencing of standards, and targeted gap analysis, all of which contribute to a more efficient assessment process.

Given that no other recurring or one-time costs are associated with implementing the tool (e.g., no hardware acquisitions, no significant IT support overheads, no extended training sessions beyond initial onboarding), the subscription fee stands as the sole cost element linked directly to utilizing the integrated compliance matrix solution. This simplicity in cost structure is advantageous for the organization, as it ensures predictability and straightforward budgeting. Calculating the subscription cost for this scenario is direct:

15 employees × 150 EURO per year = 2,250 EURO in total subscription fees per annum.

It is worth noting that this 2,250 EURO investment is a small fraction compared to the savings in person-hours and external consulting costs when using the tool. As subsequent sections will demonstrate, the efficiency gains more than compensate for this expense, yielding a positive net outcome that justifies the subscription fee.

Hourly Rates of Employees and Assessors

Beyond the subscription costs, the evaluation of cost reduction hinges on monetizing the time saved. Both the internal project staff and external assessors represent a significant cost driver, as their labor costs are directly tied to hourly rates. By reducing preparation times, interview durations, and post-assessment gap resolution efforts, the tool effectively decreases the total number of person-hours required for an assessment. To translate these saved hours into tangible financial benefits, we must first establish baseline hourly rates. The team contributing to the assessments comprises 15 employees with varying roles and expertise. These individuals bring different levels of seniority, technical skill, and organizational responsibilities. As a result, their fully burdened hourly rates, which factor in wages, benefits, and overhead, tend to vary (See Table 7).

Table 7. Hourly Rates of all Roles involved in project assessments

Role	Hourly Rate
Cybersecurity Manager	33.17 €
Software Developer	37.98 €
Process Manager	36.06 €
Project Manager	40.00 €
QA Manager	30.77 €
Risk Manager	32.21 €

BUPT

Software Project Lead	38.46 €
SW Architect	40.87 €
SW Requirements Engineer	26.44 €
SYS Architect	43.27 €
System Project Lead	38.46 €
Test Manager	36.06 €
Software Tester	33.17 €

In addition to internal staff, the assessment typically involves two external assessors who conduct formal audits, verify compliance with the relevant standards, and issue findings that guide improvements. External assessors often command higher hourly rates due to their specialized expertise, independence, and accreditation. Their costs can represent a substantial portion of the assessment's total expenditure, especially when multiple interviews, evidence reviews, and follow-up sessions are required (See Table 8). By leveraging the integrated tool, it is possible to decrease the total hours that these external experts must spend on the project, thereby realizing substantial savings.

Table 8. Hourly Rates of Assessors

Role	Hourly Rate
Lead Assessor	55 €
Co-Assessor	50 €

Rationale for Hourly Rate Transparency
Adopting a transparent approach to disclosing hourly rates and the workforce composition ensures that the subsequent calculations of cost savings are easily understood and validated. Decision-makers gain confidence in the CBA's conclusions when they can verify that realistic labor rates and team structures were used. Moreover, having clear visibility into the baseline cost structure allows the organization to perform sensitivity analyses. For example, if labor costs rise due to wage increases or if a different composition of roles is needed for future assessments, the established baseline and detailed hourly rate data enable straightforward recalculations.

3.4 Assessment Efforts and Costs

In order to build a coherent and evidence-based business case for the integrated compliance tool discussed in this study, it is essential to examine the estimated efforts and costs associated with conducting both ISO/SAE 21434 and ASPICE for cybersecurity

BUPT

assessments. These assessments, while closely related in content and objective, differ in scope, complexity, and temporal distribution of activities. The following sections present detailed insights into the levels of effort (measured in working hours) and the corresponding costs (expressed in Euros) depicted in Table 10, grounded in both industry benchmarks and lessons learned from previous compliance audits. The effort data serve as a baseline to compare pre- and post-tool implementation scenarios, while the cost calculations rely upon the hourly rates and resource distributions introduced in the preceding chapters.

ISO/SAE 21434 Assessment Efforts and Costs.
The ISO/SAE 21434 standard sets forth a structured framework for addressing cybersecurity throughout the automotive engineering lifecycle. Adhering to this standard involves not only meeting technical requirements but also ensuring that the organizational and procedural infrastructures support robust cybersecurity measures. As such, the time and resources invested in this standard's assessments typically span multiple phases: preparation, execution of the actual ISO/SAE 21434 assessment, and subsequent findings closure.

Effort Estimation and Cost Calculation. The total effort required to achieve ISO/SAE 21434 compliance in this case study amounted to approximately 1841 hours. These hours encompass a range of activities, including preliminary documentation reviews and initial gap closure; detailed interviews with engineers and managers; and the closure of non-compliances or improvement areas identified during the audit. Such an effort level aligns with industry benchmarks for full-scale cybersecurity assessments in complex automotive projects, where multiple stakeholders, interconnected systems, and evolving technical requirements contribute to the overall labor intensity. A typical breakdown reveals that preparation activities can account for the largest segment of effort. Preparation tasks typically include assembling necessary evidence, mapping existing processes to ISO/SAE 21434 clauses, and drafting initial compliance reports. The actual assessment phase involves in-depth auditor interviews, verification of evidence, and traceability checks between cybersecurity requirements and the implemented measures. Finally, the findings closure phase, performed after the main audit, entails addressing identified gaps, documenting corrective actions, and re-verifying compliance.

Preparation Phase. The preparation phase is the most labor-intensive and costly part of the ISO/SAE 21434 assessment. It is during this phase that the necessary groundwork is laid to ensure that the organization is fully prepared for the formal audit. Preparation activities include a detailed review of relevant documents, the identification and closure of any gaps in compliance, and the alignment of internal processes with the requirements set out in ISO/SAE 21434. The primary goal is to ensure that all documentation and processes are in place before the formal assessment begins, reducing the likelihood of non-compliance findings during the audit itself.

The preparation phase requires a substantial commitment of time, amounting to a total of 960 hours. This phase is especially intensive due to the complexity of the tasks

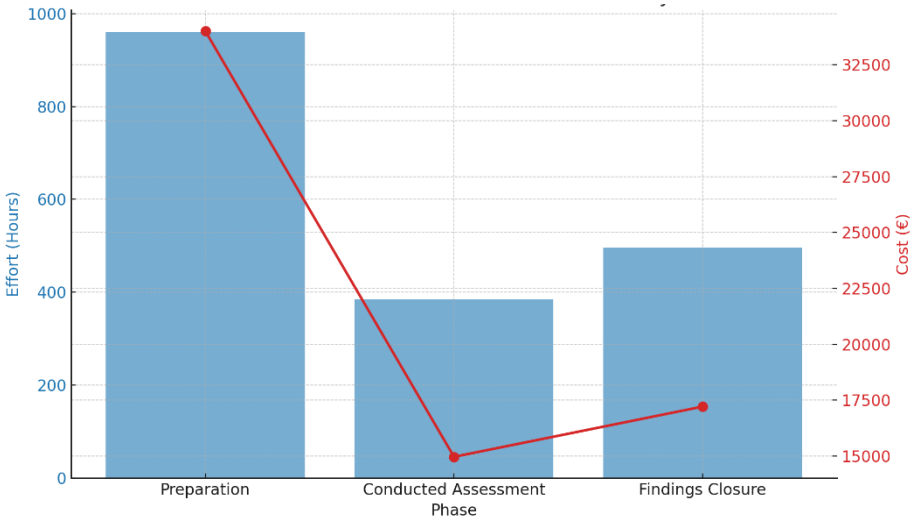
BUPT

involved, which range from reviewing compliance questionnaires to conducting gap analyses and revising internal documentation to address identified shortcomings. Given the critical nature of this phase, a large portion of the overall cost of the assessment is tied to preparation activities. The cost for this phase was €34,005.76 (See Table 9), which reflects the labor-intensive nature of the tasks and the expertise required to ensure that the organization is fully prepared for the audit. This includes the involvement of system engineers, cybersecurity experts, and documentation specialists, each contributing their specific knowledge to make sure that all requirements are met ahead of the actual assessment.

This phase is crucial for setting a strong foundation for the subsequent assessment. Its significance is reflected in the extensive effort and cost allocated to it. By addressing potential issues before the formal audit, the organization increases the likelihood of a smoother and more efficient assessment, thereby mitigating the risk of non-compliance and the associated costs of remediation.

Table 9. ISO/SAE 21434 Assessments Efforts and Costs based on Phases

Phase	Effort	Cost
Preparation	960 h	34,005.76 €
Conducted Assessment	385 h	14,970.49 €
Findings Closure	496 h	17,216,00 €
Total	**1,841 h**	**66,192.25 €**



BUPT

Assessment Phase. The assessment phase is the formal audit process in which external assessors evaluate the organization's compliance with ISO/SAE 21434. During this phase, the auditors review the processes, controls, and documentation that were prepared in the previous phase to ensure that they meet the cybersecurity requirements outlined in the standard. This phase involves structured interviews, evidence verification, and a detailed review of the organization's cybersecurity practices and policies. The purpose is to identify whether the necessary measures have been implemented to safeguard automotive systems and data against cybersecurity threats.

While the conducted assessment phase is less time-consuming than the preparation phase, it still requires a significant investment of effort. A total of 385 hours were dedicated to this phase, as auditors conducted in-depth evaluations, reviewed artifacts, and engaged with internal teams to verify the implementation of the ISO/SAE 21434 requirements. The financial cost for this phase amounted to €14,970.49 (See Table 9). This cost reflects the involvement of both internal personnel and external assessors who contribute their expertise in auditing, verifying compliance, and ensuring that all cybersecurity measures are adequately implemented.

Although the conducted assessment is not as resource-intensive as preparation, it is still a critical part of the compliance process. The cost and effort invested in this phase reflect the high level of scrutiny and the need for expert input during the audit. The external assessors' role, in particular, is crucial, as they bring an independent perspective to the process and ensure that all aspects of the standard are thoroughly evaluated. The relatively lower cost and effort compared to preparation highlight the efficiency gains achieved through proper pre-assessment preparation.

Findings Closure Phase. Once the formal assessment is completed, the findings closure phase is initiated. This phase focuses on addressing any gaps or non-conformities identified during the assessment. During findings closure, the organization works to implement corrective actions, ensure compliance, and finalize the assessment documentation. This phase also involves a review of the effectiveness of the corrective actions taken and ensuring that all requirements have been met to the satisfaction of the assessors. The closure phase is crucial for ensuring that the organization is fully compliant and can finalize its certification or achieve the desired level of compliance.

The findings closure phase required a total of 496 hours of effort. This phase typically involves revisiting processes, conducting additional reviews, and ensuring that all corrective actions have been successfully implemented. The cost for findings closure amounted to €17,216 (See Table 9), reflecting the time and resources needed to resolve any issues identified during the assessment. This phase requires significant input from both internal teams and external assessors to ensure that all gaps are addressed and compliance is achieved.

The dual-axis chart provides a clear visualization of the effort (measured in hours) and the corresponding cost (in euros) associated with different phases of the ISO/SAE 21434 assessment. The blue bars represent the effort required for each phase, illustrating the number of hours dedicated to activities such as preparation, assessment, and findings closure. Meanwhile, the red line with markers indicates the associated cost in euros, allowing for a comparative analysis of resource allocation and financial

BUPT

expenditure. This visualization effectively highlights the relationship between time investment and cost across the assessment phases, offering valuable insights into the distribution of effort and financial impact.

While the findings closure phase is less resource-intensive than the preparation phase, it is still a significant investment in terms of time and financial resources. The work done during this phase is essential for ensuring that the organization meets all requirements and that the final report is ready for submission. It ensures that any issues discovered during the assessment are fully resolved and that the organization is ready for official certification or compliance approval.



Fig. 55. ISO/SAE 21434 Assessments Total Costs

Summary of ISO/SAE 21434 Efforts and Costs. The ISO/SAE 21434 assessment required a total of 1,841 hours of effort across all three phases, with a total cost of €66,192.25 as depicted in Figure 55. The preparation phase accounted for the largest share of both the effort and the cost, reflecting the significant time and resources needed to prepare the organization for the assessment. The conducted assessment phase, while shorter in duration, still required a substantial investment due to the detailed review and verification processes involved. Finally, the findings closure phase was necessary to ensure that all issues identified during the assessment were addressed, and that full compliance with ISO/SAE 21434 was achieved. These figures provide a clear picture of the resource requirements for an ISO/SAE 21434 assessment. The preparation phase stands out as the most resource-intensive, both in terms of time and cost, while the conducted assessment and findings closure phases, though less resource-heavy, remain essential for ensuring that all compliance requirements are met. Understanding these cost and effort breakdowns is critical for evaluating the efficiency of the ISO/SAE 21434 process and serves as a baseline for assessing the impact of tools or methodologies aimed at streamlining the assessment process.

BUPT

Table 10. ISO/SAE 21434 Assessments Efforts and Costs based on Phases

Phase	Effort (Hours)	Cost (€)
Preparation ISO/SAE 21434	960	34005,76
Questionnaire Review	240	8501,44
Gap Closure	360	12752,16
Documentation Review	360	12752,16
ISO/SAE 21434 Assessment	385	14970,49
Space for Open Questions	25,5	954,51
Kick-Off	17	636,34
Final Presentation	25,5	954,51
Consolidation	20	1050
9 Concept	72	2845,98
7 Distributed Cybersecurity Activities	82	1262,68
11 Validation	118	4430,92
10 Product Development	75	2835,55
Findings Closure ISO/SAE 21434	496	17216
Implementation Review	112	3930,72
Findings Closure	264	9034,56
Final Report Analysis	120	4250,72
Total	**1841**	**66192,25**

ASPICE for Cybersecurity Planned Assessment Efforts and Costs.
The ASPICE (Automotive SPICE) for Cybersecurity assessment is a critical process for evaluating the maturity of a project's cybersecurity practices within the automotive software and systems development lifecycle. This assessment is divided into three main phases: Preparation, Conducted Assessment, and Findings Closure. Each phase involves specific activities that require significant investment in terms of effort and associated costs. In this chapter, we provide a detailed breakdown of the planned efforts, measured in hours, and the corresponding costs, expressed in euros, for each of these three phases. The data presented is derived from project planning tools and reflects the organization's internal estimates, offering a comprehensive view of the resources allocated for each phase.

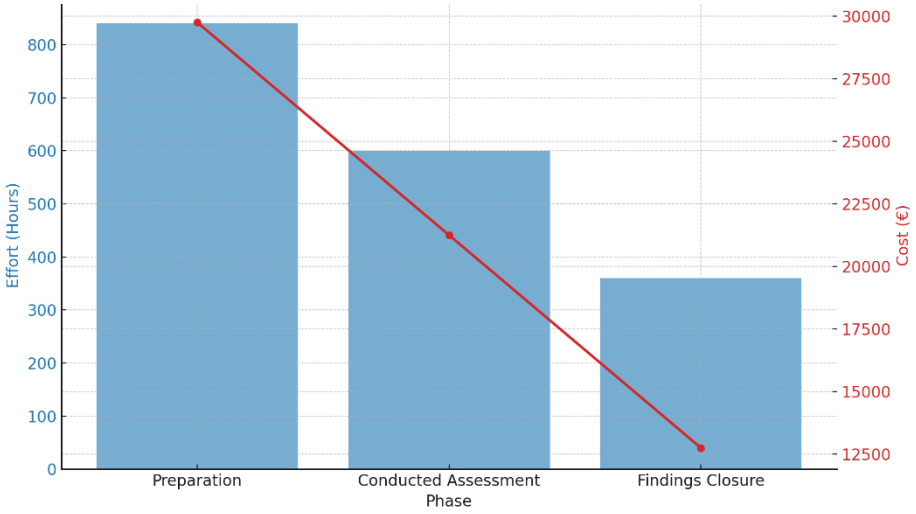
Preparation Phase. The preparation phase is a crucial part of the ASPICE for Cybersecurity assessment process. It sets the groundwork for a smooth and efficient formal

BUPT

audit. During this phase, the organization reviews its existing cybersecurity measures, identifies any gaps in compliance, and ensures that all necessary documentation is in place before the actual assessment begins. This phase is critical because it minimizes the likelihood of finding significant non-conformities during the formal audit and helps streamline the entire process. The preparation phase includes several activities such as reviewing the ASPICE for Cybersecurity questionnaires, closing any identified gaps in compliance, and conducting an extensive review of all relevant documentation. These activities are essential for aligning the organization's processes with ASPICE requirements and ensuring that all cybersecurity practices meet the necessary standards. The organization dedicates significant effort during this phase to ensure that all aspects of the cybersecurity framework are well-documented, up to date, and aligned with the requirements of the ASPICE standard. For this phase, the organization planned a total of 840 hours of effort, reflecting the extensive nature of the tasks involved. This phase requires a financial investment of €29,755.04 (See Table 11).

Table 11. Planned ASPICE for Cybersecurity Assessments Efforts and Costs based on Phases

Phase	Effort	Cost
Preparation	840 h	29,755.04 €
Conducted Assessment	600 h	21,253.60 €
Findings Closure	360 h	12,752.16 €
Total	**1,726 h**	**62,368.94 €**



BUPT

The blue bars in the graph represent the effort required for each phase, measured in hours, illustrating the time allocated for preparation, assessment, and findings closure. The red line with markers represents the cost in euros associated with each phase, showing how financial resources are distributed throughout the assessment process. The significant costs reflect the involvement of various internal teams, including cybersecurity experts, systems engineers, and other specialists, who worked together to review and refine existing practices, ensure documentation compliance, and address any gaps in the current processes. The preparation phase is the most resource-intensive part of the ASPICE for Cybersecurity assessment due to the thorough review and alignment of organizational processes with the standard's requirements.

Assessment Phase. The assessment phase is where the actual auditing takes place. During this phase, external assessors evaluate the project's compliance with ASPICE for Cybersecurity Base Practices. The goal is to verify that cybersecurity is integrated into the used processes, that risk treatment measures are in place, and that these measures are effective in mitigating potential cybersecurity risks. This phase involves formal audits, evidence verification, interviews with key personnel, and a detailed review of cybersecurity practices across different areas of the organization.

During the assessment phase, several activities are carried out, including an in-depth review of cybersecurity implementation at both the system and software levels, and an assessment of how cybersecurity requirements are elicited at both levels. These activities are aimed at ensuring that the used processes and practices comply with the required ASPICE for Cybersecurity Base Practices. The assessors also evaluate the project's management practices, ensuring that cybersecurity is effectively integrated into project workflows.

This phase required a planning of 600 hours of effort (See Table 11), reflecting the intensive work involved in auditing the organization's practices, verifying evidence, and engaging with relevant personnel. The financial cost for this phase is planned to amount to €21,253.60. The conducted assessment phase, while less time-consuming than the preparation phase, still required substantial effort and financial resources due to the complexity of the tasks and the need for expert input from external assessors. The cost reflects the time invested by assessors to conduct interviews, review documentation, and verify that all cybersecurity measures are properly implemented and aligned with the ASPICE for Cybersecurity framework as well as the cost of the team members taking part at interview sessions.

Findings Closure Phase. The findings closure phase focuses on addressing any gaps or non-conformities identified during the conducted assessment. After the formal audit, the project team must implement corrective actions to address any issues raised and ensure full compliance with the ASPICE for Cybersecurity. This phase involves revisiting processes, updating documentation, and making necessary changes to meet the requirements of the audit. The findings closure phase is essential for ensuring that the organization achieves full compliance and that any weaknesses identified during the assessment are resolved. Key activities in the findings closure phase include the review and implementation of corrective actions. The project team works to ensure that any

BUPT

gaps identified during the conducted assessment are addressed, and that all necessary improvements are implemented.

This phase requires on average 360 hours of effort (See Table 11), which reflects the work involved in addressing the identified gaps and implementing corrective actions. The financial cost for this phase was planned with €12,752.16. Although this phase requires fewer resources than the preparation phase, it remains crucial for ensuring that all findings from the assessment are addressed and that the organization achieves compliance with the ASPICE for Cybersecurity standard.

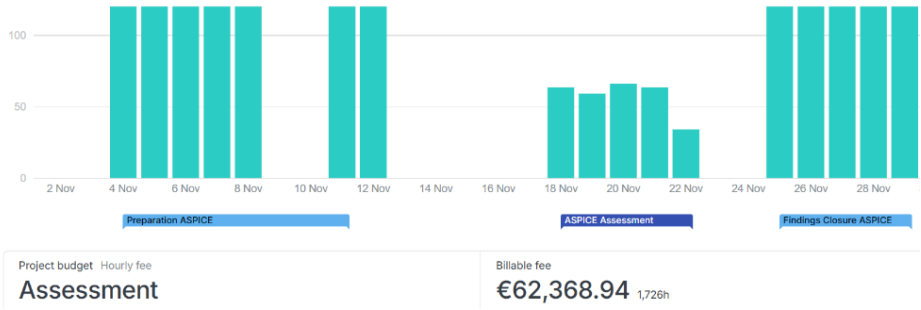


Fig. 56. Planned ASPICE for Cybersecurity Assessments Costs

Summary of ASPICE for Cybersecurity Efforts and Costs. The total effort for the ASPICE for Cybersecurity assessment was planned with 1,726 hours, with a total cost of €62,368.94. The preparation phase accounted for the largest share of both effort and cost, with 840 hours and €29,755.04, respectively. The conducted assessment phase required 600 hours and €21,253.60, while the findings closure phase took 360 hours and €12,752.16 (See Figure 56). The preparation phase is the most resource-intensive part of the assessment process, accounting for nearly half of the total planed time and cost. This phase is critical for ensuring that the project team is well-prepared for the formal assessment and minimizes the risk of non-conformities. The conducted assessment and findings closure phases, while less resource-intensive, are equally important in ensuring that the organization achieves full compliance with the ASPICE for Cybersecurity standard.

Understanding the planned efforts and costs in each of these phases provides valuable insight into where resources are allocated and how the process unfolds. This analysis also serves as a baseline for future comparisons, particularly in evaluating the impact of the Web Application Compliance Matrix to streamline the ASPICE for Cybersecurity assessment process and reduce associated efforts and costs.

BUPT

Table 12. Planned ASPICE for Cybersecurity Assessments Efforts and Costs based on Phases

Phase	Effort (Hours)	Cost (€)
Preparation ASPICE	840	29755,04
Questionnaire Review	240	8501,44
Gap Closure	240	8501,44
Document Review	360	12752,16
Findings Closure ASPICE	600	21253,6
Implementation Review	120	4250,72
Gap Closure	360	12752,16
Final Report Analysis	120	4250,72
ASPICE Assessment	286	11360,3
Space for open questions	42,5	1590,85
SEC.4 - Risk Treatment Validation	16	612,88
SEC.3 - Risk Treatment Verification	16	612,88
SEC.2 - Cybersecurity Implementation (SYS)	16	659,04
SEC.2 - Cybersecurity Implementation (SW)	18	720,58
SEC.1 - Cybersecurity Requirements Elicitation (SYS)	14	538,8
SEC.1 - Cybersecurity Requirements Elicitation (SW)	14	538,8
MAN.7 - Cybersecurity Risk Management	18	706,26
MAN.3 - Project Management	14	577,5
Kick Off	25,5	954,51
Final Presentation	34	1272,68
Consolidation	22	1155
ACO.4 - Supplier Monitoring	18	708,26
ACO.2 - Supplier Request and Selection	18	708,26
Total	**1726**	**62368,94**

3.5 ASPICE for Cybersecurity Assessment Effort and Cost Improvement

In this chapter, we present the actual efforts and costs associated with the ASPICE for Cybersecurity assessment, comparing them to the planned efforts and costs discussed in the previous chapter. The analysis aims to highlight the improvements in efficiency and cost reduction achieved through the use of the compliance tool and the integrated compliance matrix between ISO/SAE 21434 and ASPICE for Cybersecurity. By leveraging the mapping from ISO requirements to ASPICE base practices in the tool, the project team was able to streamline many of the assessment activities, significantly reducing the time and resources typically required for preparing for the assessment, conducting the assessment itself, and addressing the final gap closure after the assessment.

The project team had already gone through the ISO/SAE 21434 assessment, which was conducted using the compliance tool, and had performed the gap closure at the end of that audit. This previous experience with the ISO assessment gave the team a clear understanding of what to expect during the ASPICE assessment. As a result, the

BUPT

preparation time for the ASPICE audit was notably shorter, as much of the foundational work had already been completed. The tool, with its integrated compliance matrix, allowed the team to quickly identify areas of overlap between ISO/SAE 21434 and ASPICE requirements, reducing the need for redundant work and simplifying the documentation and evidence review process.

During the ASPICE assessment, the efficiency gains became even more evident. The tool's compliance matrix made it easier to trace and validate requirements across both ISO and ASPICE frameworks. This alignment reduced the time needed for interviews, evidence collection, and discussions with assessors. The project team was already familiar with the cybersecurity practices and processes being assessed, as these had been established during the ISO/SAE 21434 assessment. Consequently, the number of clarifications required during the ASPICE assessment was minimized, allowing the team to focus on more critical aspects of the evaluation rather than revisiting basic processes. This resulted in a faster assessment process and fewer resources required for the actual audit.

The final phase, which involves addressing any identified gaps and conducting gap closure after the assessment, also saw significant improvements. As the project team had already performed gap closure during the ISO assessment, the number of outstanding issues identified during the ASPICE assessment was reduced. Additionally, the compliance tool facilitated quicker identification and resolution of remaining gaps, further speeding up the gap closure process. The team could directly map the findings to the previously completed ISO/SAE 21434 compliance activities, ensuring that the corrective actions were both efficient and aligned with the established cybersecurity practices. This reduced the time required for the gap closure phase and contributed to overall cost savings.

Comparison of Actual Efforts vs. Planned Efforts

The total actual effort for the ASPICE for Cybersecurity assessment amounted to 813.2 hours (See Figure 57), while the planned effort was 1,726 hours. This reflects a reduction of 912.8 hours, or about 52.9% in total effort. The substantial decrease in effort highlights the efficiency gains achieved through the use of the compliance tool, which facilitated a quicker and more streamlined assessment process.

The Preparation Phase required 360 hours of actual effort (See Figure 57), compared to the planned 840 hours. This reduction of 480 hours represents a 57.1% decrease in effort. The reduction in time is primarily attributed to the compliance tool’s ability to quickly map the requirements from ISO/SAE 21434 to ASPICE for Cybersecurity, which eliminated the need for extensive gap analysis and documentation review. The team was already familiar with many of the requirements from the ISO/SAE 21434 assessment, and the tool’s support allowed them to focus on the specific differences between the two standards, reducing redundant work.

BUPT

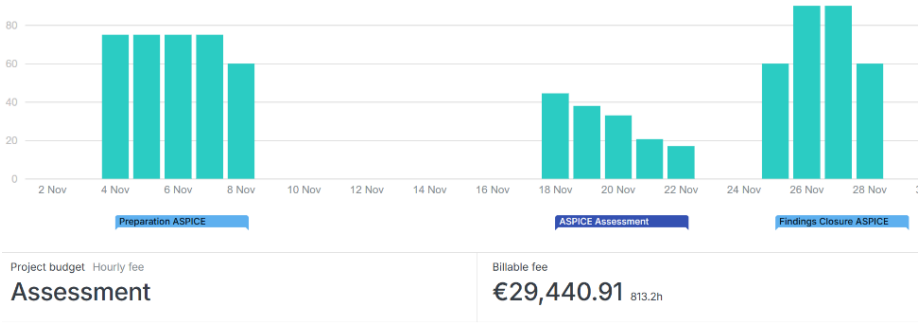


Fig. 57. Actual ASPICE for Cybersecurity Assessments Costs

Table 13. Actual ASPICE for Cybersecurity Assessments Efforts and Costs based on Phases

Phase	Effort (Hours)	Cost (€)
Preparation ASPICE	360	12752,16
Findings Closure ASPICE	300	10662,8
ASPICE Assessment	153,2	6081,95
Total	813,2	29440,91

The Conducted Assessment Phase required 153,2 hours (See Figure 57) of actual effort, compared to the planned 286 hours. This is a reduction of 46,4%. The decrease in effort during this phase was made possible by the tool's ability to quickly identify relevant documentation, processes, and requirements. The team had already completed much of the groundwork during the ISO/SAE 21434 assessment, so fewer resources were required for interviews, evidence review, and other assessment activities. Additionally, the compliance matrix streamlined the process of cross-referencing ISO/SAE 21434 and ASPICE requirements, reducing the need for back-and-forth discussions and clarifications.

The Findings Closure Phase required 300 hours (See Figure 57) of actual effort, compared to the planned 600 hours. This is a reduction of 50%. The large decrease in effort for findings closure is largely attributed to the fact that many of the identified gaps had already been addressed during the ISO/SAE 21434 gap closure process. The compliance tool also made it easier for the team to identify and close the remaining gaps quickly, further reducing the time and resources required.

Comparison of Actual Costs vs. Planned Costs

The total actual cost for the ASPICE for Cybersecurity assessment was €29,440.91 (See Figure 57), compared to the planned cost of €62,368.94. This results in a cost reduction of €32,928.03, or about 52.8%. The significant cost reduction reflects the efficiency improvements achieved in all phases of the assessment, which were made possible by the compliance tool's ability to streamline preparation, conducting the assessment, and findings closure activities.

The Preparation Phase incurred an actual cost of €12,752.16 (See Figure 57), compared to the planned €29,755.04. This is a reduction of €17,002.88, or 57.1% in cost.

BUPT

This reduction is in line with the decrease in effort, as the tool's ability to quickly identify relevant requirements and gaps significantly reduced the amount of time spent on preparation activities.

The Conducted Assessment Phase incurred an actual cost of €6,061.95 (See Figure 57), compared to the planned €11,360.30. This represents a reduction of €5,298.35, or 46,6%. The significant decrease in cost for the conducted assessment reflects the efficiency gains realized during the assessment phase. The project team's familiarity with the processes from the ISO/SAE 21434 assessment, combined with the tool's support, allowed the assessment to be conducted more efficiently, with fewer resources required.

The Findings Closure Phase incurred an actual cost of €10,626.80 (See Figure 57), compared to the planned €21,253.60. This is a reduction of €10,626.80, or 50%. This reduction in cost is primarily due to the fact that many of the corrective actions had already been completed during the ISO/SAE 21434 assessment, and the tool enabled the team to quickly identify and address the remaining gaps. As a result, the time and resources spent on the findings closure phase were significantly reduced, leading to substantial cost savings.

Table 14. Summary of Improvements

Phase	**Planned Effort (Hours)**	**Actual Effort (Hours)**	**Effort Reduction (%)**	**Planned Cost (€)**	**Actual Cost (€)**	**Cost Reduction (%)**
Preparation	840	360	**57.1**	29755.04	12752.16	**57.1**
Conducted Assessment	286	153.2	**46.4**	11360.3	6061.95	**46.6**
Findings Closure	600	300	**50**	21253.6	10626.8	**50**
Total	1726	813.2	**52.9**	62368.94	29440.91	**52.8**

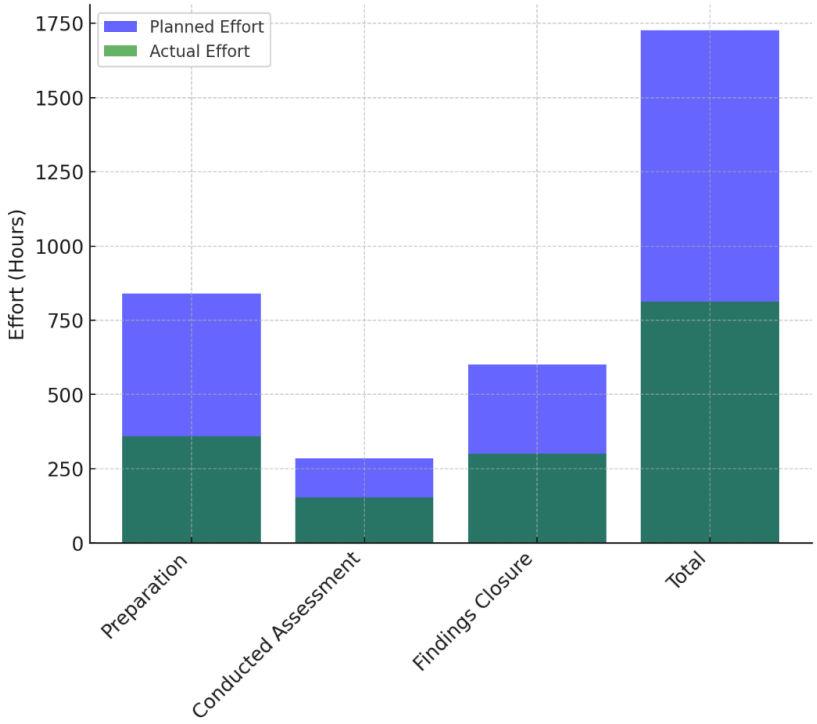
Summary of Improvements

As depicted in Table 14 and Figure58, the overall effort for the ASPICE for Cybersecurity assessment decreased by 912.8 hours, or 52.9%, while the cost was reduced by €32,928.03, or 52.8%. The most significant reductions were in the preparation and findings closure phases, with 57.1% less effort and cost in preparation, and 50% less effort and cost in findings closure. The conducted assessment phase saw a reduction of 46.4% in effort and 46.6% in cost. These reductions demonstrate the effectiveness of the compliance tool in enhancing the efficiency of the ASPICE for Cybersecurity assessment process. By enabling the project team to quickly align ISO/SAE 21434 requirements with ASPICE for Cybersecurity, the tool eliminated redundant work and allowed the team to focus on the essential tasks. This streamlined approach resulted in substantial time and cost savings, ultimately making the ASPICE assessment process far more efficient and cost-effective.

BUPT

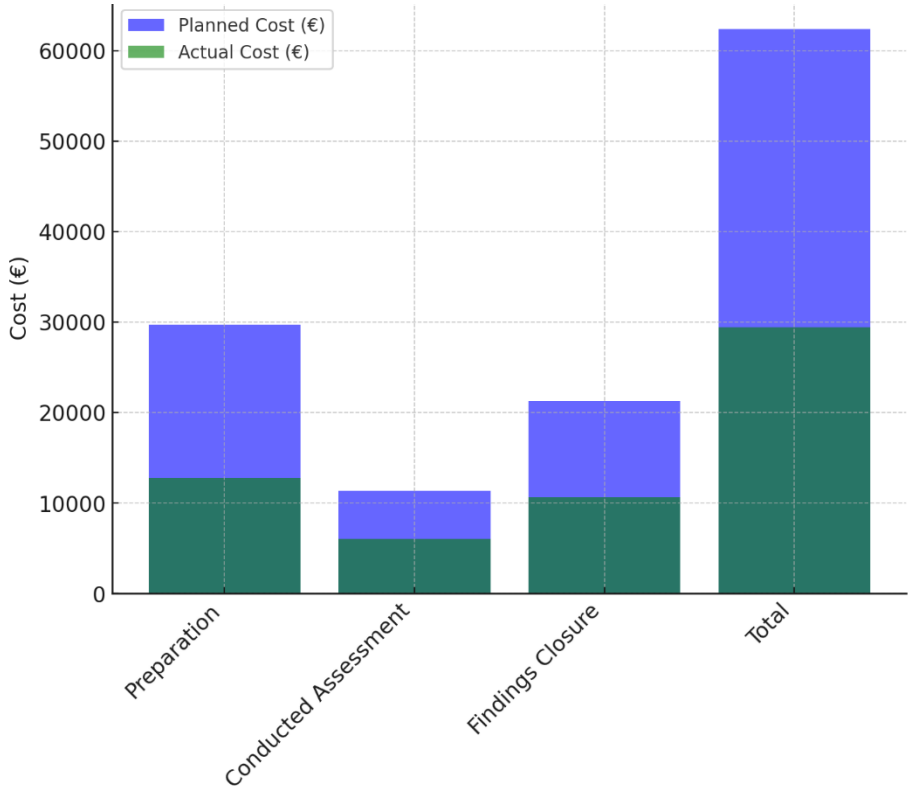
In conclusion, the compliance tool played a crucial role in achieving these significant improvements in the ASPICE for Cybersecurity assessment. The ability to reduce both the effort and cost by over 50% in key phases of the assessment underscores the value of integrating such tools into the compliance process. In the following chapter, we will explore the broader implications of these improvements and how they contribute to the overall success of the cybersecurity compliance strategy in the automotive industry.

Fig. 58. Planned vs. Actual effort in hours



BUPT

Fig. 59. Planned vs. Actual costs in EURO



3.6 Identification of Benefits

The implementation of the compliance tool in the ASPICE for Cybersecurity assessment process has yielded a broad range of benefits for the organization and project team, significantly impacting operational efficiency, financial performance, and intangible aspects such as knowledge development and team culture. These benefits, while measurable in terms of time and cost savings, also contribute to long-term improvements in the company's ability to conduct assessments, manage compliance, and foster innovation. By streamlining processes, enhancing collaboration, and supporting continuous learning, the tool has positioned the organization for greater success in meeting industry standards and maintaining a competitive edge. In this chapter, we explore these benefits in depth, focusing on operational, financial, and intangible benefits.

BUPT

Operational Benefits

The operational benefits provided by the compliance tool are profound, as it addresses several critical aspects of the assessment process, including workflow optimization, resource allocation, and documentation management. These improvements contribute to smoother, faster, and more efficient operations, enabling the team to complete assessments in less time and with fewer resources.

One of the most significant operational benefits of the compliance tool is its ability to streamline the gap analysis and documentation review process. In the past, these tasks often involved significant manual effort and time-consuming activities, such as reviewing large volumes of documentation, identifying discrepancies between different standards, and performing repeated iterations to close gaps. With the compliance tool, the team can quickly map the requirements of ISO/SAE 21434 to ASPICE for Cybersecurity, allowing them to immediately identify areas where the standards overlap and where gaps exist. This automated mapping significantly reduces the need for extensive manual reviews and ensures that the process is both faster and more accurate.

The tool also enhances cross-functional collaboration within the project. In large projects, multiple teams and departments often have a role to play in the assessment process. The compliance tool provides a shared platform where engineers, managers, and assessors can collaborate more effectively. This centralized access to the compliance matrix and relevant documentation ensures that all stakeholders are working from the same information, which reduces the risk of misunderstandings and errors. By fostering better collaboration and providing a unified approach to managing the assessment, the tool helps the organization avoid delays caused by miscommunication or lack of alignment.

As a result of these efficiencies, the organization can expect faster turnaround times for assessments. With reduced preparation time, streamlined documentation reviews, and fewer resources needed for the assessment itself, the organization can complete compliance assessments in significantly shorter timeframes. This not only accelerates the compliance process but also frees up resources that can be allocated to other value-added activities, such as product development or cybersecurity improvements.

Financial Benefits

The financial benefits of using the compliance tool are perhaps the most immediately obvious, as the tool has directly led to substantial cost reductions in the ASPICE for Cybersecurity assessment process. These savings stem from reduced resource allocation, shorter assessment timelines, and more efficient use of personnel.

The total cost reduction across all phases of the assessment is remarkable. The tool's ability to reduce the effort required for preparation, conducting the assessment, and closing out findings has led to an overall 52.8% reduction in cost. This is primarily due to the time savings achieved in each phase, which results in fewer resources being required for the assessment process. For example, the preparation phase saw a reduction of 57.1% in both effort and cost, while the conducted assessment phase experienced a 46.6% cost reduction. The findings closure phase, which is typically resource-intensive, saw the largest decrease in cost, with a 50% reduction in the resources required.

BUPT

These financial savings are not limited to direct labour costs. Assessor fees were also significantly reduced, as the tool made the entire process more efficient. By enabling internal teams to complete much of the preparatory work and reducing the need for extensive clarification during the assessment, the tool minimized the time external assessors needed to spend on the project. This directly resulted in lower costs for the conducted assessment phase, as external assessors could focus their efforts on the critical aspects of the audit rather than spending time on administrative tasks or repeated follow-ups.

Moreover, the reduced cost of findings closure is a key financial benefit. Traditionally, the findings closure phase could involve lengthy iterations to address non-conformities and close gaps identified during the assessment. However, due to the use of the compliance tool, many of these gaps had already been addressed during the ISO/SAE 21434 assessment, and the remaining gaps were identified and closed much more efficiently. This led to a 50% cost reduction for the findings closure phase, further contributing to the overall financial savings.

Additionally, the tool's efficiency in managing compliance tasks has far-reaching implications for future assessments. With the time and costs associated with compliance reduced, the organization can more effectively allocate resources to other critical projects, such as enhancing cybersecurity measures, improving internal processes, or investing in product development. This ensures that the organization can achieve better value for money while maintaining high standards of compliance and security.

Intangible Benefits

While the operational and financial benefits of the compliance tool are clearly measurable, the intangible benefits it offers are equally important. These benefits extend beyond immediate cost savings and efficiency improvements to enhance the long-term capabilities and culture of the organization.

One of the most valuable intangible benefits of the compliance tool is its role in enhancing the knowledge and skills of engineers and managers. By using the tool, team members gain a deeper understanding of the relationship between ISO/SAE 21434 and ASPICE for Cybersecurity. The tool provides a clear, visual mapping between the two standards, which helps engineers and managers better comprehend the nuances of both frameworks. This experience equips the team with a deeper understanding of how these standards relate to the development and implementation of secure, compliant systems. As the team becomes more familiar with the compliance requirements, they are better positioned to incorporate them into their daily workflows and to make proactive decisions that support compliance in future projects. Moreover, the tool functions as an educational resource. Engineers and managers can use it to improve their understanding of cybersecurity requirements and to learn how to apply these standards in practice. As the tool serves as both a compliance aid and a learning tool, it accelerates the team’s ability to adapt to evolving cybersecurity standards, ensuring that the organization is always ahead of the curve in terms of expertise.

The tool also promotes a culture of collaboration and continuous improvement. By providing a shared platform for compliance tracking and gap closure, it encourages team members from different departments to work together. This collaborative

BUPT

environment fosters the exchange of ideas, knowledge, and best practices, ensuring that everyone is aligned and working towards the same goals. Over time, this collaboration builds stronger teams and enhances the overall organizational culture.

In addition, the reliability and accuracy provided by the tool contribute to a more transparent and trustworthy compliance process. The ability to easily trace compliance gaps and map them to corrective actions enhances the credibility of the organization's cybersecurity practices. This transparency helps build trust among stakeholders, including internal teams, external auditors, and customers, who can rely on the accuracy and completeness of the assessment process. The tool also enables continuous feedback. As teams use the compliance tool across multiple projects, they can track the progress of compliance initiatives and learn from past experiences. This iterative feedback process allows the organization to constantly refine and improve its approach to compliance, ensuring that it remains efficient, up-to-date, and adaptable in the face of changing standards and regulations.

Conclusion

The compliance tool has provided significant operational, financial, and intangible benefits to the organization. Operationally, it has streamlined the assessment process, reduced redundant work, and facilitated better collaboration. Financially, it has led to substantial cost savings by reducing the time and resources required for preparation, assessment, and findings closure. Intangibly, the tool has enhanced the knowledge of engineers and managers, promoted a culture of continuous improvement, and fostered trust and transparency in the compliance process.

The comparison between the planned and actual costs for the combined ISO/SAE 21434 and ASPICE for Cybersecurity assessments demonstrates significant financial benefits driven by the use of the compliance tool. The planned costs for the entire assessment process amounted to €128,561.19 (See Figure 60 and Table 15), while the actual costs were €95,633.16 (See Figure 61 and Table 16), reflecting a substantial cost reduction of €32,928.03, or approximately 25.6%.

This reduction in costs can be attributed to the operational efficiencies realized throughout both the preparation and assessment phases. The preparation phase saw a notable reduction in both effort and cost, with the tool facilitating quicker alignment of ISO/SAE 21434 and ASPICE requirements, thereby minimizing the need for repetitive documentation reviews and gap analysis. The conducted assessment phase also benefited from the tool's ability to streamline evidence collection and cross-referencing, significantly reducing the time and resources required for interviews and review activities. Finally, the findings closure phase saw the most substantial savings, with many gaps having already been addressed during the ISO assessment, leading to a more efficient gap closure process. Overall, the compliance tool has enabled the organization to achieve substantial cost savings across all phases of the assessment process, making future assessments more financially efficient while maintaining high standards of compliance. These savings will not only allow for better resource allocation in future projects but also ensure that the organization can continue to meet increasingly stringent cybersecurity requirements in a cost-effective manner.

BUPT

As the organization continues to use the compliance tool, these benefits will compound over time, making future assessments more efficient and cost-effective while also building a stronger, more knowledgeable workforce. By aligning ISO/SAE 21434 and ASPICE for Cybersecurity, the tool supports both immediate compliance needs and long-term strategic goals, ultimately ensuring that the organization remains a leader in the automotive cybersecurity space.

Table 15. Overall Planned Costs and Efforts

Phase	Effort (Hours)	Cost (€)
Preparation ISO/SAE 21434	960	34005,76
Preparation ASPICE	840	29755,04
ISO/SAE 21434	385	14970,49
Findings Closure ISO/SAE 21434	496	17216
Findings Closure ASPICE	600	21253,6
ASPICE Assessment	286	11360,3
Total	**3567**	**128561,2**



Fig. 60. Overall Planned Costs

BUPT

Table 16. Overall Actual Costs and Efforts

Phase	Effort (Hours)	Cost (€)
Preparation ISO/SAE 21434	960	34005,76
Preparation ASPICE	360	12752,16
ISO/SAE 21434	385	14970,49
Findings Closure ISO/SAE 21434	496	17216
Findings Closure ASPICE	300	10626,8
ASPICE Assessment	153,2	6061,95
Total	**2654,2**	**95633,16**

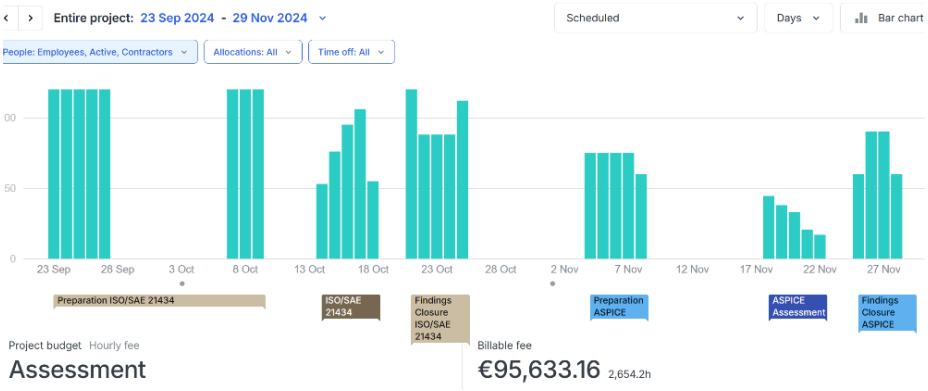


Fig. 61. Overall Actual Costs

3.7 Aggregation of Costs and Benefits for the ASPICE Assessment

In this chapter, we focus on the costs and benefits associated with the implementation of the compliance tool specifically for the ASPICE for Cybersecurity assessment. The compliance tool's value is primarily derived from its cost-saving benefits, which stem from improving the efficiency of the assessment process. The tool streamlines several tasks, reduces redundancies, and speeds up the process, thereby significantly cutting down the resources required for completing the assessment. In this analysis, we will aggregate the costs and benefits of using the compliance tool, calculate the Net Present Value (NPV), Benefit-Cost Ratio (BCR), and Return on Investment (ROI), and evaluate its financial impact on the organization.

BUPT

Total Cost Savings and Benefits

The introduction of the compliance tool results in substantial cost savings for conducting the ASPICE for Cybersecurity assessment. These savings are achieved through a reduction in the time and resources required to prepare for the assessment, conduct the assessment itself, and close the findings. The cost savings are primarily driven by the tool's ability to quickly map the requirements of ISO/SAE 21434 to ASPICE, streamline documentation review processes, and enable faster gap closure.

To quantify the financial benefits, we examine the costs before and after the tool's implementation. The initial costs for performing the ASPICE for Cybersecurity assessment were €62,368.94. After the tool was implemented, the costs were reduced to €29,440.91, which includes the savings resulting from reduced preparation time, fewer resources needed for assessment activities, and more efficient findings closure. The total cost savings achieved by implementing the tool are calculated as:

$$\textbf{Cost Savings} = 62{,}368.94 - 29{,}440.91 = \textbf{32,928.03 EURO}$$

The cost of implementing the tool is the annual subscription fee, which is €2,250. This represents the only additional cost associated with the tool. When we factor in this subscription fee, the total cost of the ASPICE assessment, after the tool's implementation, becomes:

$$\textbf{Total Cost After Tool} = 29{,}440.91 + 2{,}250 = \textbf{31,690.91 EURO}$$

Thus, the overall financial impact of implementing the tool is clear: the total cost after implementing the tool is €31,690.91, a significant reduction from the initial €62,368.94. This demonstrates the tool's ability to generate a huge return on investment (ROI) by drastically reducing the costs of conducting the assessment.

Net Present Value (NPV)

NPV evaluates the actual net economic benefit of a project. While the BCR indicates the ratio of benefits to costs, NPV calculates the absolute net economic gain [77]. In this context, the NPV measures the value generated by implementing the compliance tool, considering the costs of the tool and the savings it produces. A positive NPV indicates that the investment in the tool is profitable and provides a return greater than its initial cost. The formula for NPV is as follows:

$$NPV = \frac{\text{Benefits}}{(1+r)^t} - \text{Total Costs}$$

BUPT

Where:

- Benefits = €32,928.03 (cost savings),
- Total Costs = €2,250 (annual subscription fee),
- r = 10% (discount rate),
- t = 0 (time period, since the benefits are realized immediately).

Substituting these values into the NPV formula:

NPV = 32,928.03 − 2,250 = 30,678.03 EURO

Thus, the NPV for the ASPICE for Cybersecurity assessment is €30,678.03. This positive NPV indicates that the compliance tool generates a net gain of €30,678.03, after accounting for the tool's annual subscription cost. This clearly demonstrates the financial benefits of implementing the tool, as the savings far outweigh the tool's cost, leading to a strong return on investment (ROI).

Benefit-Cost Ratio (BCR)
The BCR offers a single metric that can help decide whether to accept or reject a project. In a budget-constrained environment, it serves as a tool for ranking and prioritizing projects within the available budget [77]. A BCR greater than 1 indicates that the benefits outweigh the costs, while a BCR less than 1 suggests that the costs exceed the benefits. In this case, we will calculate the BCR to understand how much value the organization gains for every euro spent on the compliance tool. The formula for BCR is:

$$BCR = \frac{\text{Total Benefits}}{\text{Total Costs}}$$

Where:

- Benefits = €32,928.03 (cost savings),
- Total Costs = €2,250 (annual subscription fee).

Substituting these values into the formula:

BCR = 32,928.03 / 2,250 = 14.65

The BCR for the ASPICE for Cybersecurity assessment is 14.65, which means that for every euro spent on the tool, the organization receives €14.65 in benefits. This extremely high BCR highlights the exceptional return on investment generated by the

BUPT

tool. It shows that the tool is not only cost-effective but also generates substantial value, making it a highly profitable investment for the organization.

Return on Investment (ROI)
In addition to NPV and BCR, the Return on Investment (ROI) is another key financial metric that calculates the percentage return on the investment made in the compliance tool. ROI measures the profit relative to the cost of the investment and provides an understanding of how efficiently the organization is using its resources. The formula for ROI is:

$$ROI = \frac{\text{Benefits} - \text{Costs}}{\text{Costs}} \times 100$$

Where:

- Benefits = €32,928.03 (cost savings),
- Costs = €2,250 (annual subscription fee).

Substituting the values into the formula:

ROI = ((32,928.03 - 2,250) / 2,250) x 100 = 1367.9%

Thus, the ROI for the ASPICE for Cybersecurity assessment is 1367.9%, meaning that for every euro spent on the tool, the organization earns €13.68 in savings. This exceptionally high ROI underscores the outstanding profitability of implementing the tool.

Conclusion of Financial Analysis
The aggregation of costs and benefits for the ASPICE for Cybersecurity assessment clearly shows that the compliance tool offers exceptional financial value:

- **The NPV of €30,678.03 demonstrates that the tool generates significant net value, well beyond the costs associated with its implementation.**
- **The BCR of 14.65 indicates that the organization receives more than €14.65 in benefits for every euro spent on the tool, underscoring the outstanding return on investment.**
- **The ROI of 1367.9% indicates that the tool provides a massive financial return, with a €13.68 return for every €1 invested.**

These findings clearly confirm that the compliance tool is a highly profitable investment for the organization. It not only reduces the cost of conducting the ASPICE for Cybersecurity assessment but also streamlines the overall process, enabling faster and

BUPT

more efficient assessments. The tool's cost-effectiveness and high ROI make it an invaluable asset for improving compliance processes, saving both time and resources while ensuring that the organization meets the necessary cybersecurity standards.

In conclusion, the compliance tool provides a clear financial benefit, particularly in the context of ASPICE for Cybersecurity assessments, making it an essential tool for organizations aiming to optimize their compliance processes while maintaining high standards of cybersecurity. With a positive financial impact, the tool will continue to deliver significant cost savings and efficiency improvements, contributing to the long-term success and sustainability of the organization's compliance efforts.

3.8 Risks of Cost Estimation

Cost estimation is a critical process in any project, as it serves as the foundation for budget planning and financial decision-making. In the context of compliance assessments, such as ASPICE for Cybersecurity and ISO/SAE 21434 assessments, accurate cost estimation becomes even more important due to the complex nature of the assessments and the financial resources involved. However, there are several risks associated with cost estimations, particularly when the assessments are conducted in locations with high labor costs, such as Bavaria, Germany. Moreover, variations between actual costs and planned costs further complicate the accuracy of these estimations. This chapter discusses the risks involved in cost estimation for these assessments, taking into account factors such as the location of employees, their experience, and the potential discrepancies between planned and actual costs. In published papers, the difficulty of cost estimation in the automotive industry is often attributed to the need for high-quality data and information. Challenges that hinder this process, including a lack of resources and difficulties in acquiring and validating information are continuously identified [78].

Impact of Location on Cost Estimation

One of the most significant risks to cost estimation in this scenario is the location of the employees involved in the assessments. The Bavarian region of Germany is known for its high labor costs compared to other countries, especially in Eastern Europe or Southeast Asia, where labor costs for similar tasks might be significantly lower. This geographic factor can cause cost estimates to be skewed, especially when compared to assessments conducted in lower-cost regions. When conducting cost estimations for the project, these labor cost differences need to be accounted for. If the initial cost estimations were based on general industry benchmarks that do not factor in these regional discrepancies, the actual costs of the project would likely be higher than expected. For instance, the same tasks performed by employees in Germany could be more expensive than if performed by workers in Poland, Romania, or India, where hourly rates are considerably lower.

In the context of the ASPICE for Cybersecurity and ISO/SAE 21434 assessments, the high labor costs in Germany could lead to a risk of underestimating costs when comparing the planned assessment to the actual outcome. Even if the initial budget is set based on industry standards, the actual cost might exceed the estimates due to the

BUPT

geographic location of the personnel involved in the assessment. Therefore, failing to account for these regional differences may lead to unexpected financial pressure on the project.

Impact of Experience and Team Expertise

Another risk to consider in cost estimation is the experience and expertise of the team members conducting the assessments. As with any professional service, more experienced individuals can often complete tasks more efficiently than those with less experience. In the case of the ISO/SAE 21434 and ASPICE for Cybersecurity assessments, members of the project team who are already familiar with the ISO/SAE 21434 standard or have previous experience participating in ASPICE assessments can complete the required tasks more quickly and accurately, thus reducing the overall effort and associated costs.

However, the complexity of the task and the experience of the team members create potential risks in estimating the actual time required for each phase of the assessment. For example, some team members may have extensive prior experience with ISO/SAE 21434 but be less familiar with ASPICE for Cybersecurity, leading to longer preparation times or additional hours spent on understanding the nuances of the assessment. Similarly, experienced team members may overestimate their ability to handle certain tasks or assume that previous experiences will lead to similar outcomes, potentially leading to inaccurate cost projections. Moreover, less experienced members may need additional support, training, or oversight, which could increase the overall time and cost of the project.

The learning curve is another factor that must be considered. Even experienced team members may face a learning curve when dealing with new processes or requirements that are unique to the specific assessment. For example, while many of the team members may be familiar with ISO/SAE 21434, they may not have worked extensively with ASPICE for Cybersecurity, leading to increased time and costs during the assessment phase as they become familiar with the standards.

Discrepancies Between Planned and Actual Costs

One of the most significant risks in cost estimation is the potential discrepancy between planned costs and actual costs. The actual cost of the assessment can differ from the planned budget due to several factors, including unanticipated challenges during the assessment, the complexity of the documentation review, or the need for additional resources to complete the project. Even when proper risk management strategies and detailed cost estimates are in place, the unpredictability of the project and the various external factors can cause the actual costs to exceed the initial projections.

In the case of the ASPICE for Cybersecurity and ISO/SAE 21434 assessments, unforeseen complications during the assessment process, such as a lack of documentation, unexpected gaps in the compliance processes, or the discovery of additional issues, could lead to higher costs than anticipated.

Additionally, project scope changes or changes in the team composition during the assessment can lead to discrepancies between planned and actual costs. For example, if

BUPT

the scope of the assessment is expanded to include more processes, therefore more stakeholders or additional documentation, it would require additional resources, which was not initially anticipated. Similarly, if key team members are unavailable or if new team members with less experience are brought in, the time required to conduct the assessment may increase, leading to cost overruns.

The Role of Experience in Planning

While experience can reduce the uncertainty in cost estimation, it can also introduce a risk of overconfidence. In cases where team members have previously participated in similar assessments, there may be a tendency to underestimate the time required or assume that previous experience will easily translate into cost savings. This overconfidence bias may cause underestimation of required effort, particularly if the project faces new or more complex requirements than those encountered in prior assessments.

Moreover, experienced team members may focus on familiar processes and overlook new challenges or changes in the standards, potentially missing hidden costs or risks. Therefore, despite the team's experience with similar assessments, the planning stage should be approached with caution to ensure all variables are accounted for and that expectations align with the reality of the project's requirements.

Conclusion. Cost estimation for the ASPICE for Cybersecurity and ISO/SAE 21434 assessments is a complex and inherently risky process. The location of the employees, with the high labor costs in Germany, poses a significant challenge in providing accurate cost estimates, particularly when compared to lower-cost regions. Similarly, the experience of the team members plays a critical role in determining the accuracy of cost estimations, as overconfidence or underestimation of effort can skew the planned versus actual costs. Discrepancies between planned and actual costs are inevitable, due to the unpredictable nature of the project, scope changes, and unforeseen challenges. Thus, while the compliance tool provides significant cost savings, it is essential to recognize that cost estimations for complex compliance assessments involve a variety of risks and uncertainties that must be managed carefully. By factoring in location-specific labor costs, the experience levels of team members, and the potential for scope changes, organizations can better anticipate and mitigate the risks of cost estimation for such assessments, leading to more effective financial planning and project execution.

3.9 Financial Analysis Conclusion

In conclusion, the cost-benefit analysis presented in this chapter provides a comprehensive understanding of the financial impact and efficiency improvements brought by the implementation of the compliance tool for the ASPICE for Cybersecurity assessment. By comparing the planned costs against the actual costs and assessing the resulting cost savings, it is evident that the tool delivers a substantial return on investment (ROI). The reduction in both effort and costs, as well as the positive financial outcomes highlighted by the Net Present Value (NPV) and Benefit-Cost Ratio (BCR), underscores the

BUPT

significant value the tool provides to organizations conducting these complex compliance assessments.

The tool's introduction notably reduces the time and resources required at each phase of the assessment, from preparation to findings closure. The cost savings, driven by the tool's efficiency in mapping standards, streamlining documentation review, and accelerating gap closure, contribute to a drastic reduction in the total cost of the assessment. When the annual subscription fee for the tool is factored into the overall cost, the remaining net savings demonstrate that the tool is a highly cost-effective investment for organizations undertaking regular ASPICE assessments. The positive NPV of €30,678.03 and the exceptionally high BCR of 14.65 indicate a massive return for every euro spent on the tool, proving that the tool not only reduces costs but also enhances value creation across the organization.

While the ROI of 1367.9% further validates the financial advantages of the compliance tool, it is essential to also recognize the risks involved in cost estimation. The high labor costs associated with conducting assessments in regions like Bavaria, Germany, add a layer of complexity when estimating both the planned and actual costs. These regional differences in labor costs, alongside the experience and expertise of the team members, influence the overall financial outcomes. In particular, the use of highly skilled personnel can result in faster completion of tasks, contributing to cost reductions, but could also lead to underestimation of time requirements due to overconfidence in their capabilities. Additionally, scope changes, unforeseen complications, and external factors like market shifts or regulatory updates can affect the accuracy of cost projections. Hence, even though the analysis reveals substantial savings, organizations must also remain vigilant about potential cost discrepancies and adjust their expectations accordingly.

Despite these challenges, the tool's value remains clear. The efficiency gains, cost reductions, and improved assessment timelines validate its role in supporting compliance initiatives, particularly in highly regulated and technically demanding industries such as automotive cybersecurity. The substantial cost reduction and positive ROI ensure that organizations using the tool for ASPICE for Cybersecurity assessments will continue to reap financial rewards, even when considering implementation costs.

In summary, the implementation of the compliance tool for the ASPICE for Cybersecurity assessment represents a sound financial investment, offering clear cost savings and a strong return on investment. It not only enhances the efficiency and speed of the assessment process but also optimizes financial resources by reducing unnecessary costs and improving resource allocation. By providing significant cost reductions and efficiency improvements, the tool supports long-term sustainability in compliance efforts, ensuring that organizations can meet regulatory requirements while maximizing operational performance and cost efficiency. Therefore, the compliance tool proves to be an essential part of the modern compliance landscape, demonstrating both short-term benefits and long-term financial advantages that contribute to the organization's overall success in navigating complex regulatory environments.

BUPT

D. Scientific Contribution

The complexity of ensuring compliance with various standards in the automotive industry, especially in the context of cybersecurity, has long been a challenge for organizations striving to meet regulatory and industry requirements. Another key challenge for Original Equipment Manufacturers (OEMs) under UNECE R155 is effectively communicating cybersecurity requirements and fostering a cybersecurity mindset throughout the entire supply chain. This intricate task requires a holistic approach to ensure that all stakeholders understand and apply the necessary cybersecurity measures [74]. As the automotive sector embraces more sophisticated software-driven technologies, the need for well-defined compliance frameworks has never been greater. Two prominent standards, ASPICE for Cybersecurity and ISO/SAE 21434, are central to addressing these requirements. Both of these standards play critical roles in ensuring that automotive software development projects meet the stringent demands for cybersecurity. However, organizations often face significant challenges in aligning these frameworks, especially when dealing with complex projects.

This thesis makes a significant contribution by introducing a compliance matrix that bridges the gap between ASPICE for Cybersecurity and ISO/SAE 21434, offering a structured, clear, and accessible approach for organizations to ensure compliance across both frameworks simultaneously. In a related study, a model for integrating various key standards in automotive was proposed, highlighting common requirements and practices to enhance the cybersecurity implementation process [75]. While existing methods for assessing compliance typically rely on separate evaluation processes for each standard, this matrix allows for a more integrated and efficient approach. This integration, however, would have been incomplete without the development of a user-friendly web-based tool that supports the compliance matrix, providing a practical solution to real-world problems in the automotive industry. The contribution of this work lies not only in the creation of the compliance matrix itself but also in the development of a web tool designed to enhance usability and accessibility. The tool improves upon traditional methods, such as Excel-based matrices, which have been widely used but are often inefficient and cumbersome. By moving to a web-based platform, this thesis offers a more dynamic and scalable approach, ensuring that the matrix can be applied flexibly across different projects, while being easily updated in response to evolving standards and practices. The development of the tool addresses a longstanding gap in the industry for a compliant, adaptable, and scalable solution that facilitates the integration of multiple cybersecurity standards.

Moreover, this work contributes to academic knowledge by advancing the understanding of how different compliance frameworks can be integrated and implemented in a practical setting. The methodology used to design and implement the compliance matrix and tool presents a new approach to compliance management in the automotive industry, offering valuable insights into how cybersecurity standards and software development processes can be aligned in a meaningful and efficient way. By focusing on the practical application of these frameworks, the research contributes not only to the development of tools but also to the broader academic discussion on integrated compliance systems and the challenges of aligning multiple cybersecurity standards.

BUPT

Through the development of both the compliance matrix and the web tool, this thesis responds to a crucial need in the automotive industry for more streamlined, efficient, and accessible ways to manage compliance with complex cybersecurity standards.

1 Development of a Compliance Matrix for ASPICE for Cybersecurity and ISO/SAE 21434

One of the primary contributions of this thesis is the development of a compliance matrix that integrates two critical standards in the automotive industry, ASPICE for Cybersecurity and ISO/SAE 21434. The increasing complexity of modern automotive systems, combined with the growing need to ensure cybersecurity across various software and hardware components, has made compliance with these frameworks an essential part of the industry. However, the complexity and overlap between ASPICE for Cybersecurity and ISO/SAE 21434 have historically made it challenging for organizations to streamline their compliance efforts, often resulting in duplicated work, confusion, and inefficiencies. Inconsistencies, along with a lack of connectivity and correlation between standards, have created challenges for practitioners working to ensure secure vehicle development [75]. The compliance matrix represents a significant step forward in simplifying and enhancing the process of achieving compliance with both standards. The matrix was developed as a structured, easy-to-navigate tool that helps professionals and organizations efficiently manage and align the requirements of ASPICE for Cybersecurity and ISO/SAE 21434. By directly mapping the overlapping requirements of both standards, the matrix serves as a guide to identifying and implementing the requirements where the frameworks intersect, thereby reducing redundancy and improving overall efficiency.

There has been considerable research focused on ISO 26262, paper that contribute to the development of a terminological framework necessary for systematizing the commonalities and variabilities within ISO 26262 and SAE J3061 [69]. Or even papers focusing on Cost Reduction by Mutual Integration between Automotive SPICE and IATF 16949:2016 [79].

1.1 Addressing the Need for Integration

The primary challenge that the compliance matrix addresses is the need for better integration between two essential standards, both of which are crucial for ensuring cybersecurity within automotive systems. The automotive industry has made significant efforts in designing and producing safe and secure connected and automated vehicles [80]. ISO/SAE 21434 provides a framework for managing cybersecurity risks throughout the automotive lifecycle, including the identification of threats, risk analysis, and the design of cybersecurity controls. On the other hand, ASPICE for Cybersecurity is specifically focused on integrating cybersecurity practices into the project and process context of automotive software development part. By integrating security measures early in the development process, companies can substantially lower costs and strengthen the resilience of their systems [74]. The overlap between these frameworks

BUPT

means that many activities are required in both standards yet managing them separately often leads to inefficiencies. This integration is particularly valuable as organizations face increasing pressure to meet both standards, without dedicating excessive time or resources. By utilizing the compliance matrix, professionals can easily see where the two frameworks overlap, what activities can be combined, and where they need to implement separate solutions to fulfill specific requirements of each standard. Therefore, this thesis can also lead towards continuous compliance, a new terminology emerging in the research area. A continuous compliance approach enables organizations to regularly update the necessary documentation and resources to maintain compliance with standards. This ensures that organizations are well-prepared to update their certification whenever required, in accordance with the schedules set by certification authorities [81]. The need of integration between ISO/SAE 21434 and various other standards used in the automotive industry is highlighted in multiple research papers. The ISO/SAE 21434 standard has laid the foundation for automotive cybersecurity and can be applied alongside other standards, such as ISO 26262 and ISO PAS 21488 [82].

1.2 Key Features of the Compliance Matrix

The compliance matrix developed in this thesis is not only theoretical but designed to be an actionable and practical tool. One of its key features is its focus on practicality and user accessibility. Rather than presenting the compliance requirements in an abstract or overly technical manner, the matrix provides a clear structure that allows users to easily understand how each requirement of the ISO/SAE 21434 and ASPICE for Cybersecurity standards is related. The matrix directly links the specific activities and processes required by both standards, helping users identify common actions that meet the criteria for both frameworks. Additionally, the matrix helps identify gaps in compliance, areas where requirements may not align, or where additional steps may be needed to satisfy one framework without necessarily duplicating effort. For example, it is common that both ISO/SAE 21434 and ASPICE for Cybersecurity require cybersecurity risk management activities, but they may differ in their specific methods or documentation requirements. The matrix enables users to pinpoint these differences and determine how to approach the gap between the two standards. In this way, the matrix does not just reduce redundancies but also enables a more effective allocation of resources in compliance efforts, focusing attention on areas where real discrepancies exist between the frameworks. Another valuable aspect of the matrix is that it goes beyond simply showing overlap; it also highlights areas where one standard provides a deeper level of detail or requires activities that the other does not explicitly cover. This allows organizations to ensure that all requirements are properly addressed without overcomplicating the compliance process or missing critical elements. Through this detailed comparison, organizations can confidently ensure they are meeting the full scope of both frameworks, saving time and reducing the risk of non-compliance.

BUPT

1.3 Theoretical and Practical Implications

The development of this compliance matrix has both theoretical and practical implications in the field of cybersecurity and automotive software development. From a theoretical perspective, the matrix contributes to the growing body of research on the integration of cybersecurity standards within the automotive sector. As the industry faces increasing challenges in balancing cybersecurity needs with software development processes, the matrix offers a novel solution that advances understanding in the area of standards alignment. It represents a systematic approach to addressing the challenges of cross-framework compliance and illustrates how multiple regulatory and industry standards can be harmonized to reduce redundancy and improve operational efficiency.

From a practical standpoint, the matrix offers immediate value to organizations in the automotive industry that are navigating the complexities of compliance. By providing a tool that directly supports the integration of two essential standards, the matrix helps organizations meet cybersecurity requirements more efficiently, freeing up resources to focus on other critical aspects of product development and cybersecurity risk mitigation. In practice, the matrix can be used in a variety of settings. It can serve as a reference point for compliance assessments, helping project teams navigate the complexities of both ASPICE and ISO/SAE 21434. It can also be used to identify and prioritize activities, ensuring that the most critical compliance requirements are met first. The matrix is designed to be dynamic and flexible, accommodating changes in both standards as they evolve. This adaptability ensures that organizations will not need to redo their compliance assessments each time a new version of one or both of the standards is released, making the matrix a long-term tool for continuous compliance management.

1.4 Limitations and Areas for Future Research

While the compliance matrix provides significant value, it is important to acknowledge that its application and effectiveness are not without limitations. It is important to note that we are attempting to introduce a more open strategy into a longstanding, experienced, and closed industry [83], as outlined in a research article discussing a new rating method for cybersecurity. The matrix is a tool for mapping the requirements of ASPICE for Cybersecurity and ISO/SAE 21434, but its effectiveness relies on how accurately and consistently the frameworks are applied in practice. The implementation of these standards within an organization is highly dependent on team expertise, the specific context of the development project, and organizational readiness to adopt such a matrix-based approach. Furthermore, while the matrix has been designed to address the intersection of two key standards, there is potential for extending its use to other cybersecurity standards in the automotive or broader engineering domains. By continuing to develop and refine the matrix, future work could offer even more comprehensive solutions for multi-standard compliance management. Even if no Artificial Intelligence methodologies have been used in the development of the matrix, the established connections between the two standards can be used in training Artificial Intelligence based tools that can further be used towards process improvement. The integration of AI in vehicle

BUPT

security holds significant promise, and the proposed solutions require comprehensive testing to ensure their effectiveness [84].

2 Development of a Web-Based Tool to Support the Compliance Matrix

A key contribution of this thesis is the development of a web-based tool designed to support the compliance matrix between ASPICE for Cybersecurity and ISO/SAE 21434. While the compliance matrix itself provides an essential framework for integrating the overlapping requirements of these two standards, it was crucial to offer a practical, user-friendly tool that could effectively support its implementation in real-world scenarios. This web-based tool was developed with the intention of improving the efficiency, scalability, and user experience in conducting compliance assessments, making it easier for professionals to navigate, track, and manage the complex requirements of both frameworks.

The development of this tool addresses several critical challenges faced by organizations when managing compliance processes. The first challenge is the inherent complexity and scale of both the ASPICE for Cybersecurity and ISO/SAE 21434 standards. These contain a large number of requirements, work products, and processes that need to be meticulously documented, tracked, and validated. Given the detailed nature of these frameworks, traditional methods such as Excel-based matrices or manual tracking systems are not ideal solutions. These methods are often cumbersome, error-prone, and lack the flexibility needed to handle updates, user collaboration, and real-time reporting. The web-based tool solves these challenges by offering a more efficient and scalable solution for compliance management.

2.1 Addressing the Need for Digital Transformation in Compliance

According to recent observations, global automotive sales executives are consistently confronted with various ideas, theories, and "tornado business models," all claiming to drive economic value. Among these emerging business trends that have already impacted the leading automotive industry are digitalization and connectivity [85]. The development of the web-based tool is rooted in the growing need for digital transformation in compliance management. Compliance management is a complex, time-intensive, and costly process that would greatly benefit from enhanced confidence, automation, and systematic reuse [70]. As automotive organizations face increasing pressure to comply with stringent cybersecurity standards and software development processes, it becomes crucial to use digital tools that not only streamline compliance activities but also allow for more efficient collaboration and real-time tracking. It has been highlighted that many small and medium-sized enterprises (SMEs) lack digital transformation strategies, which could have a significant impact on the automotive sector [86]. The web-based tool enables professionals to move beyond static, offline solutions, and offers a more dynamic and interactive approach to meeting compliance requirements. The digital nature of the tool allows for a more interactive experience. Users can

BUPT

navigate between standards, easily identify gaps in compliance, and visualize the compliance process in a clear and structured way. Unlike traditional methods, which often require users to toggle between multiple documents and sheets, the web-based tool integrates all necessary information in one interface, making the compliance process faster and more intuitive. The tool also enables real-time updates, allowing teams to make adjustments and track progress without delays. This real-time collaboration ensures that all stakeholders are on the same page, and any changes in compliance requirements can be quickly incorporated into the system, ensuring the tool remains relevant and up-to-date.

2.2 Key Features and Functionalities

The web-based tool developed in this thesis offers several innovative features designed to enhance the compliance process. One of the primary features is its ability to directly integrate the compliance matrix into a dynamic interface that allows users to interact with the matrix in a more intuitive and manageable way. Unlike traditional, static matrices, which can be difficult to update and share, the web-based tool provides a centralized platform for all compliance activities.

The user interface (UI) was designed with usability in mind. It features clear navigation menus that enable users to quickly locate specific compliance requirements, tasks, and gaps. The dashboard provides an at-a-glance overview of the compliance projects, allowing users to track the progress of their assessments and easily identify areas that require further attention. This dashboard feature is especially valuable for project managers and team leaders, who need to keep track of multiple compliance assessments simultaneously and ensure that deadlines are met.

Another important feature of the tool is its ability to support team collaboration. In traditional compliance systems, teams often work in isolation, with each member tracking their progress separately. The web-based tool facilitates real-time collaboration, allowing team members to update their progress, share findings, and review each other's work. This collaborative environment reduces the risk of errors and ensures that all team members are aligned on the compliance requirements. The tool also supports different levels of user access control, ensuring that sensitive data is only accessible to those who require it.

2.3 Streamlining Compliance Tasks

A major advantage of the web-based tool is its ability to streamline compliance tasks by automating repetitive processes. For instance, the tool automatically maps and cross-references the compliance requirements from both ISO/SAE 21434 and ASPICE for Cybersecurity, eliminating the need for manual effort in identifying where the two standards overlap. By automating this mapping process, the tool drastically reduces the time required to conduct a gap analysis and ensures that no overlaps are overlooked.

Additionally, the tool simplifies the tracking of compliance activities, such as documentation reviews, risk assessments, and process evaluations. As teams progress through the assessment, they can mark off completed tasks, ensuring that all

BUPT

requirements have been addressed in a systematic manner. The tool's automated gap analysis function helps professionals identify discrepancies between ASPICE for Cybersecurity and ISO/SAE 21434, allowing them to focus on the areas where compliance is not fully aligned. This minimizes the need for back-and-forth discussions and manual cross-checking of requirements, allowing teams to resolve gaps more efficiently and effectively. This is particularly beneficial for organizations looking to implement continuous improvement processes, as the tool provides valuable insights into areas where the organization may be falling short of the required standards. All these, leading to a continuous compliance approach, enabling organizations to regularly update the necessary work products and artefacts in order to maintain compliance with new standards [81].

2.4 Benefits of the Web-Based Tool

The web-based tool brings several key benefits to organizations and professionals involved in automotive cybersecurity and compliance management. First, it reduces the time and effort required to perform assessments, ultimately leading to significant cost savings. By automating many of the manual processes involved in compliance verification, the tool frees up valuable time for compliance teams to focus on more complex tasks, such as risk mitigation and process improvement. Second, the tool improves visibility and transparency across compliance activities. Managers and stakeholders can gain real-time insights into the progress of the assessment and make informed decisions based on up-to-date data. This increased transparency helps avoid delays, reduces risks, and fosters a more effective and responsive compliance process. Third, the tool's user-centric design allows professionals with varying levels of experience to use it effectively. Whether a user is an expert in ISO/SAE 21434 or new to ASPICE for Cybersecurity, the tool's intuitive interface, clear workflows, and interactive features make it accessible and valuable for all team members. By making the compliance process more user-friendly, the tool encourages wider adoption and consistent usage, ensuring that organizations can consistently meet the necessary compliance requirements.

3 Contribution to Industry Practice and Academia

Cybersecurity is a critical issue in the automotive industry, as inadequate security measures can jeopardize human lives [87]. The contributions made in this thesis extend beyond theoretical knowledge and provide substantial value to both industry practice and academic research. By developing a compliance matrix for aligning ASPICE for Cybersecurity and ISO/SAE 21434, coupled with a web-based tool designed to support its use, this work offers practical solutions to pressing challenges in the automotive sector. At the same time, the thesis presents significant insights into the integration of cybersecurity standards within automotive software development processes, making it a valuable resource for both industry professionals and academic researchers.

BUPT

3.1 Contribution to Industry Practice

In the automotive industry, compliance with cybersecurity standards is crucial for ensuring the safety and integrity of increasingly complex software systems in vehicles. ISO/SAE 21434 and ASPICE for Cybersecurity are two of the most important frameworks used to achieve this, but their implementation has often been challenging due to their complexity and overlap. Organizations have had to apply these standards separately, which led to redundant tasks, increased costs, and the potential for errors or omissions. Many efforts have been made to develop a secure system that satisfies the criteria and requirements of the automotive vehicle development life cycle. However, a significant gap remains in the secure development lifecycle [88]. The compliance matrix and the web-based tool developed in this thesis provide an innovative solution to these issues by simplifying and streamlining the compliance process.

One of the key contributions of this research to industry practice is the integration of two critical cybersecurity frameworks. The compliance matrix not only helps organizations understand how the requirements of ISO/SAE 21434 and ASPICE for Cybersecurity intersect but also offers a clear mapping of overlapping requirements. This integration is invaluable because it allows automotive manufacturers and suppliers to conduct assessments more efficiently, without duplicating efforts or missing key requirements. For organizations striving to meet both standards, this matrix offers a practical solution to navigating the complexities of multiple frameworks. By reducing redundancy and aligning compliance processes, the matrix can significantly cut costs and reduce the time needed for assessments. Moreover, it can also be applied in Agile development methodologies as there are multiple papers proving ASPICE application in Agile development [89] [90]. Another paper presents a case study on applying a new standard to a sample set of projects, exploring the challenges and lessons learned from using traditional process capability assessments in Cybersecurity process evaluations. It also introduces tool proposals to address the unique requirements of a Cybersecurity process model, offering practical solutions [91]. In contrast, this thesis provides a more structured approach by introducing a compliance matrix that bridges key frameworks, offering a clearer and more accessible way to ensure compliance across multiple standards simultaneously. The accompanying web-based tool plays a pivotal role in transforming the compliance matrix from a theoretical concept into a practical, usable resource. By offering a user-friendly, interactive platform for managing compliance, the tool streamlines workflows and enhances collaboration among team members, making compliance processes more efficient. The tool's ability to automate tasks like gap analysis, reporting, and tracking progress ensures that organizations can maintain a real-time overview of their compliance status. This level of visibility is crucial for ensuring that no requirement is overlooked and that assessments are completed in a timely manner. Moreover, the tool's ability to integrate both frameworks into a single compliance workflow is a game-changer for project managers, auditors, and compliance officers. It allows teams to perform both ISO/SAE 21434 and ASPICE for Cybersecurity assessments simultaneously, streamlining compliance management and ensuring that critical cybersecurity standards are met without unnecessary delays. The flexibility of the web tool ensures that it can be customized to suit the needs of individual projects, enhancing

BUPT

its utility across a wide range of automotive applications. Therefore, the tool can also be used to understand the parallel between ISO/SAE 2143 and ISO 26262, Strengthening Automotive Cybersecurity, as major gaps between security and safety are being identified in the industry [82]. Another case study was presented to demonstrate the impact of the new Automotive SPICE standard for Cybersecurity on the implementation of the ISO 26262 standard for Functional Safety, using a specific methodology [92]. The industry's need for such efficient, scalable solutions is ever-growing, and the tool offers tangible benefits for organizations looking to optimize their compliance processes.

This work also addresses a critical need within the automotive industry for more effective training and knowledge transfer. As automotive cybersecurity becomes vital for type approval, training in this area is essential [93]. The compliance matrix and tool can be used to train new engineers, managers, and other stakeholders in the intricacies of ASPICE for Cybersecurity and ISO/SAE 21434, providing a hands-on, practical approach to understanding the complex requirements of both frameworks. Providing organizations cheaper training alternative comparing to the official certification trainings. As an example, starting early 2022 the training of ASPICE for Cybersecurity assessors has started [94]. It is not only automotive security experts who are needed, but also the entire system development team must possess the skills to understand, address, and integrate cybersecurity into the system (Stolfa et al., 2023). This tool has the potential to accelerate the onboarding process and ensure that compliance teams are well-versed in the standards they are required to follow.

There is an increasing need to enhance cybersecurity in future autonomous vehicles. Papers focusing on autonomous vehicles highlight the importance of cybersecurity compliance. A published paper reviews significant automotive cyber-attacks from the past decade and presents state-of-the-art solutions utilizing artificial intelligence. It also proposes a roadmap for building secure autonomous vehicles and identifies key open challenges that must be addressed [96]. Therefore, this hesis may offer valuable insights by bridging cybersecurity frameworks, helping address some of these challenges in the context of automotive security.

3.2 Contribution to Academia

In addition to its practical applications in industry, this thesis also makes valuable contributions to academic research. A literature review of a total of 537 papers demonstrates that research on the automotive cybersecurity topic is organized into four clusters corresponding to four lines of research: Automotive Security, Vehicle Engineering, Smart Vehicle, and IT Security [97]. Highlighting the lack of resources dedicated to cybersecurity process management within these domains. Moreover, there is a gap in the literature regarding a systematic and comprehensive review of cyber-attacks on connected and autonomous vehicles, including mitigation strategies, preparedness, and future research directions [98]. The idea of the thesis has already been presented to the academia, receiving impressive feedback. It has been presented as a methodology seeking to streamline the compliance process, significantly reducing the resources required for conducting gap analyses and ensuring adherence to requirements [99]. The creation

BUPT

of the compliance matrix and web-based tool represents an innovative approach to cybersecurity standards integration in the context of automotive development processes. While there has been research on individual standards like ISO/SAE 21434 and ASPICE for Cybersecurity, there has been no work focused on how these standards intersect and can be effectively managed in tandem. This thesis fills a gap in the academic literature by addressing the need for integrated compliance solutions that bridge the requirements of multiple frameworks. An initial article on automotive cybersecurity was published in 2012. Since then, there has been a substantial increase in publications, with nearly two-thirds of the total articles appearing in the last three years, underscoring the growing importance of cybersecurity within the automotive industry [71].

One of the primary academic contributions of this research is the methodology developed for aligning cybersecurity standards within a single, unified compliance framework. The compliance matrix provides an example of how different regulatory and industry standards can be mapped together, offering a systematic way to integrate complex requirements. This work can serve as a model for future research in other industries where compliance with multiple standards is necessary, such as in aerospace, healthcare, or energy sectors. By developing a structured mapping system, this thesis lays the groundwork for future studies that can further explore how the alignment of standards can improve efficiency and reduce the costs of compliance in various industries. Furthermore, the development of the web-based tool itself adds a technological contribution to the field of compliance management. In the academic realm, there is growing interest in digital tools that can support regulatory compliance, and this research provides a practical, real-world example of how a web-based platform can be used to streamline complex compliance tasks. The tool's ability to automate processes like gap analysis, progress tracking, and reporting represents an advancement in how organizations can manage cybersecurity compliance more effectively. By providing a digital solution that integrates the compliance matrix and facilitates real-time collaboration, this research contributes to the digitalization of compliance management and provides a new avenue for future academic inquiry into automated compliance solutions. Moreover, it also contributes to the emerging research topic of continuous compliance, allowing organizations to continuously refresh the required documentation and resources to uphold compliance with standards [81].

Additionally, the research methodology employed in this thesis, blending theoretical development with practical application, serves as a model for applied research in cybersecurity and compliance management. By developing a tool that directly addresses a real-world problem faced by industry professionals, the research highlights the value of applied research in the field of cybersecurity standards. This approach aligns with growing calls in academia to move beyond purely theoretical studies and focus on creating solutions that have tangible impacts on industry practice. The work presented in this thesis encourages further collaboration between academia and industry to develop practical tools that address the ever-evolving challenges of regulatory compliance.

Finally, the academic value of this research extends to future studies on integrated standards, where researchers can build on the foundations laid here. As cybersecurity standards continue to evolve and new standards emerge, the need for cross-framework compliance will only grow. This thesis presents a useful starting point for future

BUPT

research that can examine the scalability and adaptability of the compliance matrix for other standards or sectors. Researchers can also explore the tool's applicability to other industries, including healthcare, energy, and even governmental regulatory environments, where similar challenges exist regarding the integration of multiple standards.

BUPT

4 Scientific Contribution Summary

This research makes several significant contributions to the field of automotive cybersecurity compliance, focusing on improving efficiency, integration, and automation of compliance processes. The key contributions of this work can be summarized as follows:

1. Development of a Compliance Matrix for ASPICE for Cybersecurity and ISO/SAE 21434

- Bridges the gap between ASPICE for Cybersecurity and ISO/SAE 21434, providing a structured mapping of overlapping requirements.
- Eliminates redundant work by identifying common compliance activities, reducing unnecessary effort.
- Improves alignment between software development processes and cybersecurity risk management.
- Enhances audit readiness by offering a clear and structured approach to compliance verification.
- Facilitates continuous compliance, allowing for regular updates and maintenance of cybersecurity documentation.

2. Development of a Web-Based Compliance Tool

- Replaces traditional Excel-based compliance tracking with a dynamic, interactive platform.
- Automates compliance verification, reducing manual effort in assessing standards alignment.
- Provides real-time tracking of cybersecurity compliance, improving project visibility.
- Supports team collaboration, allowing multiple stakeholders to work within a centralized compliance system.
- Enables easy updates and scalability, adapting to changing regulatory requirements without major rework.

3. Integration of Cybersecurity Standards into a Unified Framework

- Presents a methodology for integrating multiple cybersecurity standards within a single compliance framework.
- Reduces complexity in meeting regulatory requirements, making cybersecurity compliance more efficient.
- Ensures a systematic approach to handling cross-framework compliance, making it easier for organizations to manage multiple standards simultaneously.
- Enables organizations to transition to a continuous compliance approach, reducing last-minute certification efforts.

BUPT

4. Practical Contributions to Industry

- Simplifies compliance processes for OEMs and suppliers, reducing both cost and effort in cybersecurity assessments.
- Optimizes compliance workflows, ensuring that cybersecurity standards are met without disrupting development processes.
- Improves training and knowledge transfer, making cybersecurity compliance easier to understand and implement across engineering teams.
- Addresses the need for a structured compliance methodology, filling an industry gap in aligning ASPICE for Cybersecurity with ISO/SAE 21434.

5. Academic Contributions

- Expands research on cybersecurity standards integration, providing a model for future compliance studies in the automotive industry.
- Introduces a methodology for mapping cross-framework requirements, applicable to other domains such as functional safety (ISO 26262).
- Lays the foundation for further research on automated compliance tools, digitalization, and AI-assisted cybersecurity compliance.
- Contributes to the emerging topic of "continuous compliance", an evolving research area in cybersecurity standardization.

In conclusion, this research introduces both theoretical and practical advancements in automotive cybersecurity compliance, offering structured methodologies, practical tools, and industry-oriented solutions. By aligning ASPICE for Cybersecurity and ISO/SAE 21434, developing a digital compliance platform, and providing a framework for integrated compliance, this work significantly enhances efficiency, reduces redundancy, and sets a new standard for cybersecurity assessments in the automotive sector.

BUPT

E. Final Conclusions

1 Conclusion

The development of the Compliance Matrix stands as a cornerstone of this thesis, representing a significant advancement in harmonizing the requirements of ISO/SAE 21434 with ASPICE for Cybersecurity within the automotive industry. This endeavor was initiated with the creation of a comprehensive matrix in Excel, meticulously mapping the critical clauses of ISO/SAE 21434 to the corresponding base practices of ASPICE for Cybersecurity. This foundational work not only bridged the gap between two pivotal standards but also provided a strategic framework for organizations to achieve integrated compliance, thereby enhancing their cybersecurity posture while optimizing resource allocation and reducing costs.

The creation and utilization of the Compliance Matrix in Excel provided a structured and systematic approach to mapping and aligning the requirements of ISO/SAE 21434 with ASPICE for Cybersecurity. This matrix served as a valuable tool for organizations, enabling them to identify overlapping requirements, streamline compliance efforts, and ensure comprehensive coverage of cybersecurity aspects within their software development processes. By leveraging the matrix, organizations could effectively manage compliance with both standards simultaneously, reducing the need for duplicate assessments and minimizing resource expenditure. One of the significant contributions of the Compliance Matrix was its ability to highlight areas of synergy between ISO/SAE 21434 and ASPICE for Cybersecurity. By identifying common requirements and practices, the matrix facilitated a more integrated approach to compliance, allowing organizations to implement measures that satisfied both standards concurrently. This not only enhanced operational efficiency but also reinforced the organization's commitment to maintaining high standards of cybersecurity and process quality. Moreover, the Compliance Matrix provided a clear and actionable roadmap for addressing non-conformances identified during audits and assessments. By mapping specific clauses and practices, organizations could systematically identify gaps in their processes and develop targeted corrective actions that addressed both ISO/SAE 21434 and ASPICE requirements. This proactive approach to compliance management ensured that organizations were well-prepared for audits, minimizing the potential for non-conformances and associated corrective actions that could lead to project delays and increased costs. The development process of the Compliance Matrix also underscored the importance of cross-functional collaboration and expertise. Creating an effective mapping required a deep understanding of both standards, as well as the ability to interpret and translate requirements across different frameworks. This collaborative effort not only enriched the quality of the matrix but also fostered a culture of continuous learning and improvement within the organization. By engaging subject matter experts from various domains, the matrix was crafted with a comprehensive and nuanced understanding of the intricacies involved in cybersecurity and software process improvement.

Furthermore, the Compliance Matrix served as a foundation for the subsequent development of the web application, enhancing its functionality and user-friendliness.

BUPT

The insights gained from the Excel-based matrix informed the design and features of the web application, ensuring that it effectively operationalized the mapping process and provided users with an intuitive and efficient tool for managing compliance. The matrix's structured framework enabled the seamless integration of advanced functionalities such as interactive mapping, documentation management, and progress tracking within the web application, thereby amplifying its utility and impact. The successful implementation of the Compliance Matrix also reinforced the importance of strategic planning and proactive compliance management. By anticipating compliance challenges and addressing them systematically, organizations could enhance their readiness for audits and assessments, reducing the likelihood of non-conformances and associated disruptions. This strategic approach not only improved compliance outcomes but also contributed to a more resilient and security-conscious organizational culture.

In reflecting on the overall impact of the Compliance Matrix, it is evident that this tool offers significant value beyond mere compliance alignment. It serves as a catalyst for continuous improvement, driving organizations to refine their processes, enhance their cybersecurity measures, and adopt best practices that align with industry standards. The matrix's ability to integrate and harmonize complex requirements fosters a holistic approach to cybersecurity and process quality, ensuring that organizations are well-equipped to navigate the evolving landscape of automotive cybersecurity.

Despite its numerous benefits, the development and application of the Compliance Matrix also highlighted certain challenges and areas for future enhancement. One such challenge was ensuring the accuracy and comprehensiveness of the mappings, given the complexity and breadth of both ISO/SAE 21434 and ASPICE for Cybersecurity standards. Continuous validation and updating of the matrix are essential to maintain its relevance and accuracy, particularly as standards evolve and new requirements emerge. Future efforts could focus on automating parts of the mapping process and incorporating advanced analytics to identify and address gaps more efficiently. Additionally, the scalability of the Compliance Matrix remains an important consideration. As organizations grow and their compliance needs become more complex, the matrix must be adaptable to accommodate new requirements and standards. Developing a dynamic and scalable framework that can evolve with the changing regulatory landscape will enhance the matrix's long-term utility and relevance. Integrating the matrix with digital tools and platforms, such as the aforementioned web application, could further enhance its scalability and accessibility, providing organizations with a robust and flexible solution for managing compliance across multiple standards.

In conclusion, the Compliance Matrix developed in this thesis represents a significant contribution to the field of automotive cybersecurity and process compliance. By systematically mapping ISO/SAE 21434 clauses 7, 9, 10, 11, and 15 to ASPICE for Cybersecurity base practices, the matrix provides a clear and actionable framework for organizations to achieve integrated compliance. The successful implementation and demonstrated benefits through the case studies underscore the matrix's value in enhancing operational efficiency, reducing costs, and strengthening cybersecurity postures. As the automotive industry continues to evolve, the Compliance Matrix stands as a testament to the importance of strategic alignment, cross-functional collaboration, and

BUPT

innovative tool development in achieving and maintaining high standards of cybersecurity and process quality.

1.1 Web Application Summary

The development and implementation of the web application for the Compliance Matrix represent a significant advancement in the realm of automotive cybersecurity and process compliance. This application emerged as a pivotal component of the thesis, addressing the complex challenges associated with aligning and managing compliance with multiple industry standards, specifically ISO/SAE 21434 and ASPICE for Cybersecurity. Throughout this research, the web application has demonstrated its efficacy as an indispensable tool for organizations striving to streamline their compliance efforts, enhance operational efficiency, and reduce associated costs. At its core, the web application was designed to operationalize the Compliance Matrix, transforming it from a theoretical framework into a practical, user-friendly tool. The application encompasses several key features that facilitate the mapping and alignment of non-conformances between ISO/SAE 21434 and ASPICE standards. By providing an interactive platform, the application enables users to input their compliance data, map non-conformances accurately, and generate comprehensive reports tailored for audit preparation. This seamless integration of data management and compliance mapping underscores the application's role in bridging the gap between abstract compliance requirements and their practical implementation within organizational processes.

One of the foremost strengths of the web application lies in its ability to enhance the accessibility and usability of the Compliance Matrix. Prior to the development of this application, the process of mapping non-conformances between different standards was often manual, time-consuming, and prone to errors. The web application automates much of this process, reducing the potential for human error and significantly accelerating the mapping process. Users can now navigate the complexities of compliance standards with greater ease, leveraging the application's intuitive interface to manage and visualize their compliance status effectively. The case studies presented in this thesis vividly illustrate the practical benefits of the web application. In both scenarios involving Tier 1 suppliers collaborating with German Original Equipment Manufacturers (OEMs), the application played a crucial role in facilitating the efficient mapping of non-conformances between ASPICE assessments and ISO/SAE 21434 requirements. By utilizing the web application, the suppliers were able to systematically address overlapping compliance requirements, thereby reducing duplication of efforts and optimizing resource allocation. The quantitative cost reductions observed in the case studies—ranging from decreased personnel involvement to shortened audit durations—underscore the application's impact on enhancing operational efficiency and reducing financial expenditures. Furthermore, the web application proved instrumental in fostering better collaboration and communication among project teams, auditors, and stakeholders. The application's centralized platform allows for real-time updates and collaborative input, ensuring that all relevant parties have access to the latest compliance data and mappings. This transparency not only streamlines the audit process but also builds trust and accountability within the organization. The ability to generate detailed reports

BUPT

and visualize compliance status through the application also aids in communicating progress and readiness to external auditors and internal stakeholders alike.

The development of the web application also provided valuable insights into the intersection of technology and compliance management. By integrating advanced functionalities such as interactive mapping, documentation management, and progress tracking, the application demonstrated how digital tools can revolutionize traditional compliance processes. The incorporation of these features not only enhances the application's utility but also aligns it with contemporary trends in digital transformation and automation within the automotive industry. This alignment ensures that the application remains relevant and adaptable to evolving industry standards and technological advancements.

Despite its numerous strengths, the development and implementation of the web application were not without challenges. One challenge was designing the application to be flexible enough to accommodate varying organizational needs and compliance scenarios. Different organizations may have unique compliance requirements, processes, and workflows, necessitating a customizable and scalable solution. To address this, the web application was built with a modular architecture, allowing for customization and expansion as needed. This design philosophy not only enhances the application's adaptability but also ensures that it can serve a diverse range of users across different sectors within the automotive industry. The user experience (UX) design of the application was also a critical focus area. Ensuring that the application is intuitive and user-friendly was essential for encouraging widespread adoption and effective utilization. Extensive user testing and feedback were incorporated into the development process, leading to iterative improvements that enhanced the application's interface and functionality. By prioritizing UX design, the application was made accessible to users with varying levels of technical expertise, thereby broadening its applicability and impact.

The integration of the web application into organizational processes also highlighted the importance of training and support. To maximize the application's benefits, users required adequate training on how to effectively utilize its features and interpret the compliance mappings. Comprehensive training programs and user documentation were developed to accompany the application, ensuring that users could seamlessly integrate it into their existing workflows. Additionally, ongoing support and updates were planned to address any emerging needs and incorporate user feedback, thereby fostering a culture of continuous improvement and adaptability.

Looking forward, the web application holds immense potential for further enhancement and broader adoption within the automotive industry. Future developments could include the integration of advanced analytics and machine learning algorithms to predict and identify potential compliance gaps proactively. Such features would enable organizations to anticipate compliance issues before they arise, further enhancing their ability to manage and mitigate risks effectively. Additionally, expanding the application's capabilities to include integration with other industry standards, such as ISO 26262 for functional safety, could provide a more holistic compliance management solution, catering to the multifaceted nature of automotive system development. Moreover, the web application's architecture allows for the incorporation of collaborative features that could facilitate more dynamic interactions between different stakeholders.

BUPT

For instance, real-time collaboration tools, automated notifications, and integrated communication channels could enhance the application's utility, making it a central hub for all compliance-related activities. Such enhancements would not only improve the application's functionality but also foster a more collaborative and cohesive approach to compliance management within organizations.

In conclusion, the web application developed as part of this thesis represents a transformative tool for managing compliance with ISO/SAE 21434 and ASPICE for Cybersecurity in the automotive industry. By operationalizing the Compliance Matrix, the application addresses the intricate challenges of multi-standard compliance, offering a streamlined, efficient, and cost-effective solution for organizations. The successful implementation of the application in the case studies underscores its practical utility and strategic value, demonstrating significant cost reductions, enhanced operational efficiencies, and improved cybersecurity postures. The web application's development highlights the critical role of digital tools in modern compliance management, showcasing how technology can simplify and optimize complex processes. Its user-centric design, robust functionality, and adaptability ensure that it meets the diverse needs of organizations striving to maintain high standards of cybersecurity and process quality. As the automotive industry continues to evolve, the web application stands as a testament to the importance of innovation, strategic planning, and continuous improvement in achieving and maintaining compliance with industry standards.

1.2 Case Studies Summary

The two case studies presented in this thesis vividly demonstrate the practical effectiveness and strategic value of utilizing the Compliance Matrix in managing compliance with ISO/SAE 21434 and ASPICE for Cybersecurity within the automotive industry. Both case studies involve Tier 1 suppliers collaborating with German Original Equipment Manufacturers (OEMs), yet they approach the integration of the Compliance Matrix from different starting points—one beginning with an ISO/SAE 21434 audit and the other with an ASPICE assessment. Despite these differing entry points, both suppliers achieved significant cost reductions, streamlined audit processes, and enhanced their overall cybersecurity posture through the strategic application of the Compliance Matrix.

In the first case study, the supplier conducted an ISO/SAE 21434 audit prior to the ASPICE assessment. By proactively identifying non-conformances during the ISO audit and mapping them to the corresponding ASPICE base practices using the Compliance Matrix, the supplier was able to address overlapping requirements efficiently. This strategic mapping minimized duplicate efforts and allowed the team to enter the ASPICE assessment with many potential non-conformances already resolved. Quantitatively, the supplier achieved substantial reductions in effort across various phases of the ASPICE assessment. For instance, the Project Audit effort was reduced from five employees over four days to five employees over three days, the Preparation Phase from six employees over three days to six employees over one day, and the Gap Closure Phase from six employees over five days to six employees over two days. These

BUPT

reductions not only translated into direct cost savings but also improved resource allocation and project timelines.

The second case study, conversely, began with the supplier having completed an ASPICE assessment. Utilizing the Compliance Matrix, the supplier mapped the identified ASPICE non-conformances to ISO/SAE 21434 requirements. This reverse mapping allowed the supplier to streamline the subsequent ISO 21434 audit process significantly. The organizational audit phase remained unchanged due to the unique requirements of ISO 21434 in that domain; however, the Project Audit/Assessment phase saw a reduction from five employees over five days to five employees over three days. Similarly, the Preparation Phase was reduced from six employees over five days to six employees over two days, and the Gap Closure Phase from ten employees over five days to ten employees over three days. These reductions underscored the efficacy of the Compliance Matrix in optimizing audit preparation and execution, leading to substantial cost savings and operational efficiencies.

Comparing the two case studies reveals several common themes and insights. First, both suppliers effectively leveraged the Compliance Matrix to bridge the requirements of ISO/SAE 21434 and ASPICE, regardless of their starting point. This flexibility highlights the Compliance Matrix's utility as a tool adaptable to different organizational contexts and compliance strategies. By mapping non-conformances from one standard to the requirements of the other, both suppliers were able to address overlapping areas proactively, reducing duplication of efforts and ensuring a more comprehensive approach to compliance. Second, the significant cost reductions achieved in both cases emphasize the economic benefits of using the Compliance Matrix. By reducing the time and resources required for audit preparation, execution, and gap closure, the suppliers were able to allocate their resources more efficiently, focus on enhancing critical processes, and avoid unnecessary expenditures associated with extended audit durations and extensive post-audit corrective actions. These cost savings are particularly important in the highly competitive automotive industry, where efficient resource management can directly impact an organization's profitability and market position. Third, the improved readiness and effectiveness of the suppliers' teams were evident in both case studies. The use of the Compliance Matrix facilitated better understanding and communication among team members, auditors, and stakeholders. By providing clear traceability between the standards, the teams were better prepared to address auditor inquiries, present comprehensive documentation, and demonstrate their compliance efforts convincingly. This not only streamlined the audit processes but also fostered a culture of continuous improvement and proactive compliance management within the organizations. Fourth, both case studies highlight the strategic value of the Compliance Matrix in strengthening relationships with OEMs. Demonstrating the ability to efficiently manage compliance with complex industry standards reinforced the suppliers' reputations as reliable and forward-thinking partners. This can lead to long-term collaborations, preferred supplier status, and new business opportunities, all of which are critical for sustained success in the automotive sector.

Despite these commonalities, the case studies also underscore the importance of tailoring compliance strategies to the specific circumstances of the organization. In the first case study, initiating the compliance effort with an ISO/SAE 21434 audit allowed

BUPT

the supplier to build a strong cybersecurity foundation before addressing software process improvements through ASPICE. In the second case study, beginning with an ASPICE assessment enabled the supplier to enhance their software development processes and then extend those improvements to meet cybersecurity requirements. Both approaches were effective, demonstrating that the Compliance Matrix can be integrated into various compliance pathways to achieve optimal results.

The challenges faced by the suppliers during the mapping process also provide valuable lessons. Accurate mapping requires a deep understanding of both standards, meticulous attention to detail, and cross-functional collaboration. The suppliers needed to ensure that all relevant stakeholders were engaged in the process, including cybersecurity experts, software engineers, quality assurance personnel, and project managers. Overcoming these challenges reinforced the importance of organizational commitment to compliance and the value of investing in training and capacity building. Furthermore, the case studies illustrate that while the Compliance Matrix significantly reduces potential non-conformances, it does not eliminate the need for thorough and comprehensive audits. Certain requirements in ISO/SAE 21434 and ASPICE do not have direct mappings, necessitating focused efforts to address those unique aspects. Recognizing and preparing for these areas ensures that organizations maintain a holistic approach to compliance and do not overlook critical requirements that could pose risks if left unaddressed.

In conclusion, the two case studies affirm the effectiveness of the Compliance Matrix as a strategic tool for managing compliance with ISO/SAE 21434 and ASPICE for Cybersecurity. By enabling organizations to map and address overlapping requirements proactively, the Compliance Matrix facilitates significant cost reductions, operational efficiencies, and enhanced cybersecurity postures. The experiences of the two Tier 1 suppliers demonstrate that the Compliance Matrix can be effectively integrated into different compliance strategies, whether starting with an ISO/SAE 21434 audit or an ASPICE assessment. The successful application of the Compliance Matrix in these case studies provides a compelling argument for its broader adoption within the automotive industry. As cybersecurity threats continue to evolve and regulatory requirements become more stringent, organizations must find efficient and effective ways to manage compliance. The Compliance Matrix offers a practical solution to this challenge, enabling organizations to streamline their efforts, reduce costs, and maintain a competitive edge. Moreover, the insights gained from these case studies contribute to the body of knowledge on compliance management in the automotive sector. They highlight the importance of strategic planning, cross-functional collaboration, and the use of innovative tools in navigating complex regulatory landscapes. By sharing these experiences, this thesis aims to guide other organizations in implementing similar strategies, ultimately contributing to the advancement of industry practices and the enhancement of automotive cybersecurity. In essence, the two case studies serve as practical exemplars of how the Compliance Matrix can transform compliance challenges into opportunities for improvement and growth. By embracing this tool, organizations can not only meet their regulatory obligations but also strengthen their operational capabilities, enhance stakeholder relationships, and contribute to the overall security and integrity of the automotive industry.

BUPT

1.3 Financial Analysis Summary

The financial analysis underscores the substantial impact of the compliance tool for the ASPICE for Cybersecurity assessment, particularly in terms of cost savings, efficiency gains, and the significant return on investment (ROI) it offers. Through a comprehensive cost-benefit analysis, it is evident that the tool plays a critical role in optimizing financial resources by reducing both effort and expenses during the compliance process. The comparison of planned versus actual costs, along with the evaluation of resulting cost savings, clearly demonstrates that the tool delivers substantial financial benefits while enhancing the overall efficiency of the assessment process. The resulting positive financial metrics, such as the Net Present Value (NPV) of €30,678.03 and the exceptionally high Benefit-Cost Ratio (BCR) of 14.65, solidify its effectiveness in delivering a high return for every euro spent.

The tool's introduction significantly reduces the time and resources required at each stage of the assessment process, from preparation to findings closure. By streamlining key tasks such as documentation review, gap closure, and mapping of standards, the tool helps organizations complete the assessment process in a more efficient and cost-effective manner. When factoring in the tool’s annual subscription fee, the remaining net savings clearly highlight the tool’s cost-effectiveness, proving that it is a highly advantageous investment for organizations that regularly undertake ASPICE assessments. The substantial reduction in total assessment costs, along with the tool’s ability to accelerate key processes, ensures that its financial value will continue to increase over time as organizations gain more experience using it.

Furthermore, the calculated ROI of 1367.9% further reinforces the financial advantages offered by the tool. The significant return, coupled with the cost reductions and improved assessment timelines, makes it clear that the tool provides not only immediate financial benefits but also long-term gains. However, while the analysis presents favorable financial outcomes, it is important to recognize the challenges that come with cost estimation in complex assessments. In particular, the high labor costs associated with conducting assessments in regions such as Bavaria, Germany, add an additional layer of complexity when estimating both planned and actual costs. These regional differences in labor costs, along with the varying levels of expertise and experience among team members, influence the financial outcomes of the assessment. Highly skilled personnel may expedite tasks, thus reducing overall costs, but may also lead to the underestimation of time requirements due to over-confidence in their capabilities. Additionally, unforeseen complications, scope changes, and external factors such as market shifts or regulatory updates can affect the accuracy of cost projections. Despite these uncertainties, the value of the compliance tool remains clear. The efficiency gains, cost reductions, and improved timelines associated with its use validate its role in supporting compliance efforts, particularly in industries as regulated and technically demanding as automotive cybersecurity. The tool’s positive financial impact, demonstrated by its substantial cost reductions and high ROI, suggests that organizations using the tool will continue to reap financial rewards. As organizations become more proficient in using the tool, the financial benefits are expected to increase, making it an even more valuable asset for future assessments.

BUPT

In summary, the implementation of the compliance tool for ASPICE for Cybersecurity assessments represents a sound financial investment. It not only helps organizations reduce assessment costs and improve efficiency but also optimizes resource allocation and supports long-term sustainability in compliance efforts. By enabling organizations to meet regulatory requirements in a more cost-effective manner, the tool contributes to improving operational performance while maximizing financial outcomes. The positive ROI, significant cost savings, and enhanced efficiency ensure that organizations using the tool will continue to realize long-term financial advantages. Moreover, as organizations gain more experience with the tool and refine their processes, the financial benefits are expected to grow, further solidifying its position as a critical resource for organizations navigating the increasingly complex regulatory landscape of automotive cybersecurity. Therefore, the compliance tool not only provides immediate financial value but also offers long-term strategic benefits, making it an essential component of the modern compliance ecosystem in the automotive sector.

BUPT

References

[1] A. Torok, Z. Szalay, and B. Saghi, "New Aspects of Integrity Levels in Automotive Industry-Cybersecurity of Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 1, pp. 383–391, Jan. 2022, doi: 10.1109/TITS.2020.3011523.

[2] H. Martin *et al.*, "Combined automotive safety and security pattern engineering approach," *Reliab Eng Syst Saf*, vol. 198, 2020, doi: 10.1016/j.ress.2019.106773.

[3] D. Zelle, C. Plappert, R. Rieke, D. Scheuermann, and C. Krauß, "ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering," *Microprocess Microsyst*, vol. 90, 2022, doi: 10.1016/j.micpro.2022.104461.

[4] Upstream Security Ltd., *2024 Global Automotive Cybersecurity Report - The automotive cybersecurity inflection point: From experimental hacking to large-scale automotive attacks— the focus shifts to im-pact*. 2024.

[5] Upstream Security Ltd., *2023 Global Automotive Cybersecurity Report - The Automotive industry is rapidly expand-ing into a vast smart mobility ecosystem, introducing new levels of cyber sophistication and attack vectors*. 2023.

[6] ISO/SAE 21434, *ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering*. 2021.

[7] VDA QMC, *Automotive SPICE® Process Reference and Assessment Model for Cybersecurity Engineering*, 1st Edition. VDA QMC, 2021.

[8] Upstream Security Ltd., *2022 Global Automotive Cybersecurity Report - Automotive Cyber Threat Landscape In Light Of New Regulations*. 2022.

[9] L. Rehberg and A. Brem, "Industrial prototyping in the German automotive industry: bridging the gap between physical and virtual prototypes," *Journal of Engineering and Technology Management - JET-M*, vol. 71, 2024, doi: 10.1016/j.jengtecman.2024.101798.

[10] R. Barrios, D. Schippers, C. Heiden, and G. Pappas, "A cybersecurity strategy for Industry 4.0," in *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019*, M. C. Dudzik and J. C. Ricklin, Eds., SPIE, May 2019, p. 23. doi: 10.1117/12.2524667.

[11] F. Siddiqui *et al.*, "Cybersecurity Engineering: Bridging the Security Gaps in Advanced Automotive Systems and ISO/SAE 21434," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, IEEE, Jun. 2023, pp. 1–6. doi: 10.1109/VTC2023-Spring57618.2023.10200490.

[12] T. Kaneko, S. Yamashita, A. Takada, and M. Imai, "Triad concurrent approach among functional safety, cybersecurity and SOTIF," *Journal of Space Safety Engineering*, vol. 10, no. 4, 2023, doi: 10.1016/j.jsse.2023.09.001.

[13] G. Baldini, "Detection of cybersecurity spoofing attacks in vehicular networks with recurrence quantification analysis," *Comput Commun*, vol. 191, 2022, doi: 10.1016/j.comcom.2022.05.021.

[14] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Cybersecurity Readiness for Automated Vehicles," in *2022 International Conference on*

BUPT

Frontiers of Artificial Intelligence and Machine Learning (FAIML), IEEE, Jun. 2022, pp. 7–12. doi: 10.1109/FAIML57028.2022.00012.

[15] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," 2022. doi: 10.1016/j.compind.2022.103614.

[16] M. Hataba, A. Sherif, M. Mahmoud, M. Abdallah, and W. Alasmary, "Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey," *IEEE Open Journal of the Communications Society*, vol. 3, 2022, doi: 10.1109/OJCOMS.2022.3169500.

[17] M. Schellekens, "Car hacking: Navigating the regulatory landscape," *Computer Law and Security Review*, vol. 32, no. 2, 2016, doi: 10.1016/j.clsr.2015.12.019.

[18] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, "Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability," *Energies (Basel)*, vol. 16, no. 3, 2023, doi: 10.3390/en16031113.

[19] R. Aghapour, M. Zeraati, F. Jabari, M. Sheibani, and H. Arasteh, "Cybersecurity and Data Privacy Issues of Electric Vehicles Smart Charging in Smart Microgrids," in *Green Energy and Technology*, 2022. doi: 10.1007/978-3-031-05909-4_4.

[20] C. Miller, "Lessons learned from hacking a car," *IEEE Des Test*, vol. 36, no. 6, 2019, doi: 10.1109/MDAT.2018.2863106.

[21] Upstream Security Ltd., *2021 Global Automotive Cybersecurity Report - Research Into Cyber Attack Trends In Light Of Cybersecurity Standards And Regulations*. 2021.

[22] UNECE R155, *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*. 2021.

[23] UNECE R156, *Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system*. 2021.

[24] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Cybersecurity regulatory challenges for connected and automated vehicles – State-of-the-art and future directions," *Transp Policy (Oxf)*, vol. 143, 2023, doi: 10.1016/j.tranpol.2023.09.001.

[25] D. Morris, G. Madzudzo, and A. Garcia-Perez, "Cybersecurity threats in the auto industry: Tensions in the knowledge environment," *Technol Forecast Soc Change*, vol. 157, 2020, doi: 10.1016/j.techfore.2020.120102.

[26] N. Argyropoulos *et al.*, "Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL," in *Transportation Research Procedia*, 2021. doi: 10.1016/j.trpro.2021.01.036.

[27] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, 2023, doi: 10.1016/j.inffus.2023.101804.

[28] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," 2018. doi: 10.1016/j.compind.2018.09.004.

BUPT

[29] G. Costantino, M. De Vincenzi, and I. Matteucci, “A Comparative Analysis of UNECE WP.29 R155 and ISO/SAE 21434,” in *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022*, 2022. doi: 10.1109/EuroSPW55150.2022.00041.

[30] Vicone, “UN R155 Understanding UN Regulation No. 155 and Its Requirements,” https://vicone.com/why-vicone/un-r155.

[31] United Nations Economic Commission for Europe, “WP.29 - Introduction,” https://unece.org/wp29-introduction.

[32] Cyres Consulting, “UN Regulation No 155: What You Need to Know about UN R155.,” https://www.cyres-consulting.com/un-regulation-no-155-requirements-what-you-need-to-know/.

[33] Cyres Consulting, “UN REGULATION NO 156 (UNECE),” https://www.cyres-consulting.com/automotive-cybersecurity-online-courses/un-regulation-no-156-unece/?lang=de.

[34] United Nations Economic Commission for Europe, “UN extends its cyber security management regulation to motorcycles and scooters,” https://unece.org/media/transport/Vehicle-Regulations/press/387828.

[35] N. Huq and R. Vosseler, “Identifying Cybersecurity Focus Areas in Connected Cars Based on WP.29 UN-R155 Attack Vectors and beyond,” in *SAE Technical Papers*, 2022. doi: 10.4271/2022-01-0116.

[36] Cyres Consulting, “How to establish a CSMS in accordance with UN R155? A short, practical guide,” https://www.cyres-consulting.com/how-to-establish-a-cyber-security-management-system-csms-in-accordance-with-un-r155/.

[37] Stuttgarter Zeitung, “Porsche nimmt wichtiges Modell wegen Cybersicherheit vom Markt,” https://www.stuttgarter-zeitung.de/inhalt.neue-eu-vorschriften-porsche-stoppt-wichtiges-modell-wegen-cybersicherheit.2fcb6c6e-7dd1-44ea-9cfe-8fb8134591ad.html.

[38] Etas, “The road to secure automotive products: ISO/SAE 21434 and ASPICE for cybersecurity,” https://www.etas.com/en/support/webinars-webinar-iso-sae-21434-and-aspice-for-cybersecurity.php.

[39] S. Japs, F. Kargl, H. Anacker, and R. Dumitrescu, “Why make it hard?-Usage of aggregated statistical data for risk assessment of damage scenarios in the context of ISO/SAE 21434,” in *Procedia CIRP*, 2022. doi: 10.1016/j.procir.2022.05.252.

[40] S. Japs, “Towards the development of the cybersecurity concept according to ISO/SAE 21434 using model-based systems engineering,” in *Proceedings of the IEEE International Conference on Requirements Engineering*, 2021. doi: 10.1109/RE51729.2021.00073.

[41] C. Schmittner, B. Schrammel, and S. König, “Asset Driven ISO/SAE 21434 Compliant Automotive Cybersecurity Analysis with ThreatGet,” in *Communications in Computer and Information Science*, 2021. doi: 10.1007/978-3-030-85521-5_36.

[42] T. Faschang and G. Macher, “An Open Software-Based Framework for Automotive Cybersecurity Testing,” in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42307-9_22.

BUPT

[43] C. Schmittner, “Automotive Cybersecurity Auditing and Assessment - Presenting the ISO PAS 5112,” in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_37.

[44] T. Liedtke, R. Messnarz, D. Ekert, and A. Much, “The New Cybersecurity Challenges and Demands for Automotive Organisations and Projects - An Insight View,” in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42307-9_21.

[45] S. Halder, A. Ghosal, and M. Conti, “Secure over-the-air software updates in connected vehicles: A survey,” *Computer Networks*, vol. 178, 2020, doi: 10.1016/j.comnet.2020.107343.

[46] M. Khatun, F. Wagner, R. Jung, and M. Glaß, “An application of DEMATEL and fuzzy DEMATEL to evaluate the interaction of safety management system and cybersecurity management system in automated vehicles,” 2023. doi: 10.1016/j.engappai.2023.106566.

[47] M. Benyahya, A. Collen, and N. A. Nijdam, “Cybersecurity and Data Privacy Certification Gaps of Connected and Automated Vehicles,” in *Transportation Research Procedia*, 2023. doi: 10.1016/j.trpro.2023.11.468.

[48] S. Marksteiner, S. Bronfman, M. Wolf, and E. Lazebnik, “Using Cyber Digital Twins for Automated Automotive Cybersecurity Testing,” in *Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2021*, 2021. doi: 10.1109/EuroSPW54576.2021.00020.

[49] A. Bolovinou, U. I. Atmaca, A. T. Sheik, O. Ur-Rehman, G. Wallraf, and A. Amditis, “TARA+: Controllability-aware threat analysis and risk assessment for L3 automated driving systems,” in *IEEE Intelligent Vehicles Symposium, Proceedings*, 2019. doi: 10.1109/IVS.2019.8813999.

[50] Vector Consulting, “Automotive Cybersecurity,” https://consulting.vector.com/int/en/solutions/cybersecurity/.

[51] C. Schlager, G. Macher, R. Messnarz, D. Ekert, and E. Brenner, “Reduce Time Performing an Assessment - Considering Work Products,” in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_39.

[52] D. Barmayoun, M. Marian, and R. Bogdan, “Automotive Internal Development Process Improvement for Assuring Compliance with the ASPICE for Cybersecurity Extension,” in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_25.

[53] E. Magdy, “A-SPICE for Cybersecurity: Analysis and Enriched Practices,” in *Communications in Computer and Information Science*, 2021. doi: 10.1007/978-3-030-85521-5_37.

[54] N. Moselhy, A. Adel, and A. Seddik, “Automotive SPICE Draft PAM V4.0 in Action: BETA Assessment,” in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42310-9_7.

[55] VDA QMC, *ASPICE PAM 4.0*. 2023.

[56] R. Messnarz *et al.*, “First Experiences with the Automotive SPICE for Cybersecurity Assessment Model,” in *Communications in Computer and Information Science*, 2021. doi: 10.1007/978-3-030-85521-5_35.

BUPT

[57] C. Schlager *et al.*, "Consistency of Cybersecurity Process and Product Assessments in the Automotive Domain," in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42307-9_24.
[58] VDA QMC, *Automotive SPICE® for Cybersecurity Guidelines*. 2021.
[59] R. Messnarz, D. Ekert, G. Macher, S. Stolfa, J. Stolfa, and A. Much, "Automotive SPICE for Cybersecurity – MAN.7 Cybersecurity Risk Management and TARA," in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_23.
[60] VDA QMC, *Automotive SPICE® Guidelines*, 2nd Edition. 2023.
[61] C. Schlager and G. Macher, "The Cybersecurity Extension for ASPICE - A View from ASPICE Assessors," in *Communications in Computer and Information Science*, 2021. doi: 10.1007/978-3-030-85521-5_27.
[62] E. Zinhom, "Utilization of Automotive SPICE Assessments with Cybersecurity Extension," in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_28.
[63] S. Stolfa *et al.*, "CYBERENG - Training Cybersecurity Engineer and Manager Skills in Automotive - Experience," in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42307-9_26.
[64] R. Dreves, R. Mayer, and B. Sechser, "Challenges with Multi-PAM SPICE Assessments," in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_20.
[65] VDA QMC, *ASPICE PAM 3.1*. 2017.
[66] VDA QMC, *Automotive SPICE® Guidelines*, 1st Edition. 2017.
[67] ISO/IEC, *ISO/IEC 33020:2019*. 2019.
[68] S. Ballingall, M. Sarvi, and P. Sweatman, "Standards relevant to automated driving system safety: A systematic assessment," *Transportation Engineering*, vol. 13, 2023, doi: 10.1016/j.treng.2023.100202.
[69] J. P. C. Ardila and B. Gallina, "Towards Efficiently Checking Compliance Against Automotive Security and Safety Standards," in *2017 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, IEEE, Oct. 2017, pp. 317–324. doi: 10.1109/ISSREW.2017.33.
[70] J. P. Castellanos Ardila and B. Gallina, "Towards Increased Efficiency and Confidence in Process Compliance," 2017, pp. 162–174. doi: 10.1007/978-3-319-64218-5_13.
[71] C. V. Kifor and A. Popescu, "Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies," *Sensors*, vol. 24, no. 18, p. 6139, Sep. 2024, doi: 10.3390/s24186139.
[72] F. Luo, Y. Jiang, J. Wang, Z. Li, and X. Zhang, "A Framework for Cybersecurity Requirements Management in the Automotive Domain," *Sensors*, vol. 23, no. 10, p. 4979, May 2023, doi: 10.3390/s23104979.
[73] G. Costantino, M. De Vincenzi, and I. Matteucci, "A Comparative Analysis of UNECE WP.29 R155 and ISO/SAE 21434," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, Jun. 2022, pp. 340–347. doi: 10.1109/EuroSPW55150.2022.00041.

BUPT

[74] F. Oberti, F. Abrate, A. Savino, F. Parisi, and S. Di Carlo, “Navigating the road to automotive cybersecurity compliance,” in *2024 IEEE 30th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, IEEE, Jul. 2024, pp. 1–4. doi: 10.1109/IOLTS60994.2024.10616052.

[75] A. A. Mohamed, H. Aslan, and T. Arafa, “Automotive Cybersecurity Engineering Standardization and Regulation: An Integrated Model,” 2024, pp. 429–445. doi: 10.1007/978-3-031-71139-8_29.

[76] Corporate Finance Institute, “Benefit-Cost Ratio (BCR).”

[77] Department of Transport and Main Roads Australia, “Technical Guide,” 2011.

[78] R. Roy, P. Souchoroukov, and E. Shehab, “Detailed cost estimating in the automotive industry: Data and information requirements,” *Int J Prod Econ*, vol. 133, no. 2, 2011, doi: 10.1016/j.ijpe.2011.05.018.

[79] S. S. Makkar, A. M. Abdelfatah, and A. H. Yousef, “Automotive Standards Compliance Cost Reduction by Mutual Integration between Automotive SPICE and IATF 16949:2016,” *IEEE INTERNATIONAL CONFERENCE OF VEHICULAR ELECTRONICS AND SAFETY (ICVES 19)*, 2019.

[80] C. Schmittner and G. Macher, “Automotive Cybersecurity Standards - Relation and Overview,” 2019, pp. 153–165. doi: 10.1007/978-3-030-26250-1_12.

[81] T. Santilli, P. Pelliccione, R. Wohlrab, and A. Shahrokni, “Continuous Compliance in the Automotive Industry,” *IEEE Softw*, vol. 41, no. 4, pp. 134–142, Jul. 2024, doi: 10.1109/MS.2023.3342974.

[82] B. Boi *et al.*, “Strengthening Automotive Cybersecurity: A Comparative Analysis of ISO/SAE 21434-Compliant Automatic Collision Notification (ACN) Systems,” *Vehicles*, vol. 5, no. 4, pp. 1760–1802, Dec. 2023, doi: 10.3390/vehicles5040096.

[83] P. Grümer and P. Brandão, “An Automotive Cybersecurity Maturity Level Assessment Programme,” in *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, IEEE, Jun. 2023, pp. 84–91. doi: 10.1109/DSN-W58399.2023.00035.

[84] M. Kamal *et al.*, “A Comprehensive Solution for Securing Connected and Autonomous Vehicles,” in *2022 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, IEEE, Mar. 2022, pp. 790–795. doi: 10.23919/DATE54114.2022.9774594.

[85] V. Paleta, “The Impact of Digitalization and Connectivity on Automotive OEM: Sustainability Dashboard,” *FINANCIAL MANAGEMENT OF FIRMS AND FINANCIAL INSTITUTIONS: 11TH INTERNATIONAL SCIENTIFIC CONFERENCE*, 2017.

[86] C. Llopis-Albert, F. Rubio, and F. Valero, “Impact of digital transformation on the automotive industry,” *Technol Forecast Soc Change*, vol. 162, p. 120343, Jan. 2021, doi: 10.1016/j.techfore.2020.120343.

[87] P. Bajpai and R. Enbody, “Towards Effective Identification and Rating of Automotive Vulnerabilities,” in *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*, New York, NY, USA: ACM, Mar. 2020, pp. 37–44. doi: 10.1145/3375706.3380556.

BUPT

[88] I. Fernandez de Arroyabe, T. Watson, and I. Phillips, "Cybersecurity Maintenance in the Automotive Industry Challenges and Solutions: A Technology Adoption Approach," *Future Internet*, vol. 16, no. 11, p. 395, Oct. 2024, doi: 10.3390/fi16110395.

[89] M. Noureldin, A. Ghalwash, L. Abd-Ellatif, and M. ElGazzar, "Blending agile methodologies to support automotive SPICE compliance," *Journal of Software: Evolution and Process*, vol. 34, no. 1, Jan. 2022, doi: 10.1002/smr.2391.

[90] P. Diebold, T. Zehler, and D. Richter, "How do agile practices support automotive SPICE compliance?," in *Proceedings of the 2017 International Conference on Software and System Process*, New York, NY, USA: ACM, Jul. 2017, pp. 80–84. doi: 10.1145/3084100.3084108.

[91] N. Moselhy and A. A. Mahmoud, "Standardization of Cybersecurity Concepts in Automotive Process Models: An Assessment Tool Proposal," 2023, pp. 635–655. doi: 10.1007/978-3-031-28073-3_44.

[92] N. Moselhy and Y. Ali, "Impact of the New A-SPICE Appendix for Cybersecurity on the Implementation of ISO26262 for Functional Safety," 2021, pp. 122–136. doi: 10.1007/978-3-030-85521-5_9.

[93] C. Schmittner *et al.*, "Automotive Cybersecurity - Training the Future," 2021, pp. 211–219. doi: 10.1007/978-3-030-85521-5_14.

[94] R. Messnarz, D. Ekert, G. Macher, A. Much, T. Zehetner, and L. Aschbacher, "Experiences with the automotive SPICE for cybersecurity assessment model and tools," *Journal of Software: Evolution and Process*, vol. 35, no. 9, Sep. 2023, doi: 10.1002/smr.2519.

[95] S. Stolfa *et al.*, "CYBERENG - Training Cybersecurity Engineer and Manager Skills in Automotive - Experience," 2023, pp. 366–383. doi: 10.1007/978-3-031-42307-9_26.

[96] V. K. Kukkala, S. V. Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 13–23, Nov. 2022, doi: 10.1109/MCE.2022.3154346.

[97] I. Fernandez de Arroyabe, T. Watson, and O. Angelopoulou, "Cybersecurity in the Automotive Industry: A Systematic Literature Review (SLR)," *Journal of Computer Information Systems*, vol. 63, no. 3, pp. 716–734, May 2023, doi: 10.1080/08874417.2022.2103853.

[98] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accid Anal Prev*, vol. 148, p. 105837, Dec. 2020, doi: 10.1016/j.aap.2020.105837.

[99] D. Barmayoun and M. Kemeter, "Paving the Road Towards Cybersecurity Compliance: Navigating ISO 21434 and ASPICE from Organizational- to Project-Level Compliance," 2024, pp. 353–362. doi: 10.1007/978-3-031-71139-8_23.

BUPT