

# Creation of an overall cybersecurity management policy in automotive industry to reduce the potential project risks

A Master's Thesis submitted for the degree of  
“Master of Business Administration”

supervised by  
DI Dr. Walter Mayrhofer, ME DWT MBA

Emrah Eminoglu, MSc

11742559

## Affidavit

I, **EMRAH EMINOGLU, MSC**, hereby declare

1. that I am the sole author of the present Master's Thesis, "CREATION OF AN OVERALL CYBERSECURITY MANAGEMENT POLICY IN AUTOMOTIVE INDUSTRY TO REDUCE THE POTENTIAL PROJECT RISKS", 118 pages, bound, and that I have not used any source or tool other than those referenced or any other illicit aid or tool, and
2. that I have not prior to this date submitted the topic of this Master's Thesis or parts of it in any form for assessment as an examination paper, either in Austria or abroad.

Vienna, 12.02.2020

---

Signature

## Acknowledgement

This Master's Thesis is the last part of my Professional MBA Automotive Industry studies, which is a joint program of the Vienna University of Technology and the Slovak University of Technology in Bratislava. With this occasion, I would like to show my gratitude to the academic directors Mr. Univ. Prof. Dr. -Ing. Dr. h. c. Wilfried Sihm and Mr. Ing. Ján Lešínský as well as the program managers Mr. Dipl. –Ing. Dr. Man-Wook Han, MSc. and Mr. Miroslav Babinský.

It is a pleasure to thank those who made this thesis possible, particularly my supervisor DI Dr. Walter Mayrhofer for his comments, feedbacks, remarks and proposals throughout the thesis.

In addition, I would like to thank to my valuable colleagues for sharing their expertise and reviewing the created outcome. Moreover, I am thankful to the contributions of all the participants of the breakout-session, which I moderated. My most special thanks and dedication go to my beloved wife Dilan. Without your support, patience and understanding during the whole two years of my studies, this academic work would not be possible.

As I promised to you dad, wherever I am, whatever I do, I will give my best. You will always be my best tutor.

# Table of Contents

<b>Acknowledgement .....</b>	<b>i</b>
<b>List of abbreviations.....</b>	<b>v</b>
<b>Abstract .....</b>	<b>vii</b>
<b>Executive Summary .....</b>	<b>1</b>
<b>1. Introduction, Motivation and Research Questions.....</b>	<b>2</b>
1.1 The importance of cybersecurity in automotive industry.....	2
1.2 Current challenges regarding cybersecurity .....	5
1.3 Research focus and problem definition.....	5
1.4 Research questions and aim .....	7
1.5 Research approach and methodology .....	8
1.6 Structure of the thesis.....	9
<b>2. Project risk management in automotive industry .....</b>	<b>11</b>
2.1 Risk and Risk Management .....	11
2.2 Factors that increase risks of a project .....	12
2.2.1 Risks posed to projects through cybersecurity threats .....	12
2.2.2 Cybersecurity risk in supply chains.....	12
2.2.3 The necessity of an overall cybersecurity management policy to reduce the potential project risks .....	13
2.2.4 Drivers for cybersecurity investment.....	17
<b>3. Theoretical framework and background information.....</b>	<b>18</b>
3.1 Definitions and Key concepts.....	18
3.2 The interface between Cybersecurity, Information Security and Functional Safety.....	23
3.3 Cybersecurity norms and standards applicable in automotive industry.....	25
3.3.1 Product Liability .....	26
3.3.2 Legally binding vs. Suggestion Requirements with respect to Product Liability.....	26
3.4 State of the art information (including risk assessment methods according to ISO/SAE 21434-Road vehicles-cybersecurity engineering).....	27
<b>4. Research .....</b>	<b>29</b>
4.1 Results of the quantitative and qualitative data from survey and moderation of a break-out session at a conference.....	29
4.1.1 Quantitative Data from Survey.....	29
4.1.2 Qualitative Data from the Moderation of a Break-Out Session at a Conference.....	32

<b>5.</b>	<b>The proposed overall cybersecurity management policy.....</b>	<b>40</b>
<b>5.1</b>	<b>Objectives .....</b>	<b>41</b>
<b>5.2</b>	<b>Scope.....</b>	<b>41</b>
<b>5.3</b>	<b>Executive Summary.....</b>	<b>42</b>
<b>5.4</b>	<b>Threat Landscape .....</b>	<b>42</b>
<b>5.5</b>	<b>Mission .....</b>	<b>42</b>
<b>5.6</b>	<b>Vision.....</b>	<b>42</b>
<b>5.7</b>	<b>Principles .....</b>	<b>43</b>
<b>5.8</b>	<b>Organization.....</b>	<b>43</b>
<b>5.9</b>	<b>RASIC within Organization Regarding Cybersecurity Activities.....</b>	<b>43</b>
<b>5.10</b>	<b>Intent of Cybersecurity.....</b>	<b>44</b>
<b>5.10.1</b>	<b>Split between process management and product development .....</b>	<b>44</b>
<b>5.10.2</b>	<b>Role responsibility structure .....</b>	<b>46</b>
<b>5.11</b>	<b>Cybersecurity related processes at MPT .....</b>	<b>52</b>
<b>5.11.1</b>	<b>Mapping between ISO/SAE 21434 and Company (MPT) Work Products. ....</b>	<b>52</b>
<b>5.11.2</b>	<b>Engineering Process Landscapes.....</b>	<b>52</b>
<b>5.12</b>	<b>Cybersecurity Governance Proposal .....</b>	<b>52</b>
<b>5.12.1</b>	<b>ISO/SAE 21434 Compliance Strategy .....</b>	<b>53</b>
<b>5.12.2</b>	<b>Location Specific Guidelines.....</b>	<b>54</b>
<b>5.12.3</b>	<b>Cybersecurity Handover from Product Development to Production .....</b>	<b>55</b>
<b>5.13</b>	<b>Project Team Role Descriptions .....</b>	<b>61</b>
<b>5.14</b>	<b>Information Classification, Handling and Sharing .....</b>	<b>62</b>
<b>5.14.1</b>	<b>Marking of Information.....</b>	<b>62</b>
<b>5.14.2</b>	<b>Handling of Information .....</b>	<b>62</b>
<b>5.15</b>	<b>Competence Management .....</b>	<b>62</b>
<b>5.16</b>	<b>Quality Management.....</b>	<b>64</b>
<b>5.17</b>	<b>Tool Management .....</b>	<b>64</b>
<b>5.18</b>	<b>Cybersecurity Monitoring, Event Assessment, Vulnerability Management and Incident Response.....</b>	<b>65</b>
<b>5.18.1</b>	<b>Incident Response Procedure .....</b>	<b>66</b>
<b>5.19</b>	<b>Product Cybersecurity .....</b>	<b>68</b>
<b>5.19.1</b>	<b>Requirements for Product Cybersecurity .....</b>	<b>68</b>
<b>5.19.2</b>	<b>Requirements for Maintenance, Repair and Decommissioning .....</b>	<b>68</b>
<b>5.19.3</b>	<b>Requirements for Key Management.....</b>	<b>69</b>
<b>5.19.4</b>	<b>Requirements for Accessible Data.....</b>	<b>69</b>

<b>5.20</b>	<b>Incident and Escalation Management for Product Cybersecurity.....</b>	<b>69</b>
<b>5.21</b>	<b>Lessons Learned .....</b>	<b>71</b>
<b>6.</b>	<b>Validation .....</b>	<b>72</b>
<b>7.</b>	<b>Conclusion.....</b>	<b>73</b>
	<b>Bibliography.....</b>	<b>76</b>
	<b>References .....</b>	<b>78</b>
	<b>List of figures .....</b>	<b>80</b>
	<b>List of tables.....</b>	<b>82</b>
	<b>Appendices .....</b>	<b>83</b>

## List of abbreviations

AD	Autonomous Driving
ADAS	Advanced Driver Assistance Systems
ASPICE	Automotive Software Performance Improvement and Capability dEtermination
AUTOSAR	AUTomotive Open System ARchitecture
CCTV	Closed Circuit Television
CERT	Computer Emergency Response Team
CVSS	Common Vulnerability Scoring System
DIN	German Institute for Standardization
DIS	Draft International Standard
DMC	Data Matrix Code
DoD	Department of Defense
DoS	Denial of Service
DS	Driveline System
DVP	Design Verification Plan
ECE	Economic Commission for Europe
ECU	Electronic Control Unit
EN	European Standards
ETA	Event Tree Analysis
EVITA	E-safety Vehicle Intrusion Protected Applications
FIPS	Federal Information Processing Standards
FMEA	Failure Mode and Effects Analysis
FMEDA	Failure Modes, Effects and Diagnostic Analysis
FMVSS	Federal Motor Vehicle Safety Standards
FTA	Fault Tree Analysis
GDPD	Global Data Privacy Director
GPMS	Global Project Management System
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operational Study
HEAVENS	Healing Vulnerabilities to Enhance Software Security and Safety
HW	Hardware
IATF	International Automotive Task Force
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
MISRA	Motor Industry Software Reliability Association
MPT	Magna Powertrain
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OEM	Original Equipment Manufacturer
OSS	Operational Safe Systems
OTA	Over the Air Update
PII	Personally Identifiable Information
PAS	Publicly Available Specification
PMI	Project Management Institute
SAE	Society of Automotive Engineers
SOC	Security Operation Center
SQD	Supplier Quality Development

STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
SW	Software
TARA	Threat Analysis and Risk Assessment
TCU	Transmission Control Unit
TISAX	Trusted Information Security Assessment Exchange
TS	Transmission Systems
TVRA	Threat, Vulnerability and Risk Assessment
VDA	German Association of the Automotive Industry
WP	Work Product



## Abstract

The importance of cybersecurity is an unknown phenomenon for many people who are working in the automotive industry. Furthermore, future trends like connected cars, driving assistance systems, autonomous driving, e-mobility, etc. will require more cybersecurity. If companies do not define how to deal with the cybersecurity risks in a project with a systematic approach, they can go even into bankruptcy. Although a company-specific, project and location independent overall cybersecurity policy is the initial step to start with, there is no guideline or standard available as state of the art, which explains how to create such an overall cybersecurity policy to reduce potential cybersecurity risks. Despite the fact that the state of the art norm ISO/SAE 21434 is expected to be released at the end of 2020, it is neither a handbook, nor a checklist which explains the steps to be followed. Hence, the objective of this thesis is to create an overall cybersecurity policy, which can be used as a guidance by other (automotive) companies to reduce potential project cybersecurity risks.

The thesis will not only help more people, specifically the executive management to understand the importance of cybersecurity, but also it will solve a significant problem in automotive industry, namely how to deal with cybersecurity risks in a systematic approach specifically in projects/products. Such an approach is required for ISO/SAE 21434 compliance, hence product liability.

Throughout the thesis, after explaining the importance of and challenges about cybersecurity, the research focus, problem definition, research questions, aim of the thesis and the research approach and methodology are elaborated. Afterwards, the project related cybersecurity risks, the theoretical framework and background information are provided. Subsequently, necessity of an overall cybersecurity policy is proven by means of a quantitative survey and a qualitative break-out session at a conference. In total, the opinions of hundreds of people from the automotive industry were taken into account. Furthermore, the experience of a well-known consulting company, which conducted a self-assessment regarding cybersecurity, reveals the criticality of an overall cybersecurity policy. The assessment indicates the low level of time required for completion of such implementations and the high benefits the overall cybersecurity policy can provide in project risk reduction. Therefore, by applying this overall cybersecurity policy (or its adapted version), companies can reduce cybersecurity risks and it could be implemented very quickly (i.e. mostly less than 3 months). Finally, the overall cybersecurity management policy was validated by means of Magna Powertrain expert reviews.

**Key Words:** Cybersecurity, Overall Cybersecurity Policy, Cybersecurity Strategy

## Executive Summary

The global threat landscape is ever-evolving. Cyber-attackers across the world are more brazen than ever before. An increasing number of corporations are experiencing large and impactful cybersecurity breaches, seriously damaging their brand and marketplace confidence. People and products everywhere are increasingly connected through technology and the trend in the automotive industry continues to shift towards a reliance on mobile and data-enhanced technologies and systems.

As the cyber threat landscape has continued to evolve, cyber-attacks have become more and more advanced and have shifted their focus to target to corporations. The companies must protect their reputations as they become target of malicious threat actors that seek to acquire intellectual property, including new engineering designs, product features, and knowledge-based engineering systems and processes.

This overall cybersecurity management policy gathers inputs from the literature, especially the SAE/ISO 21434 standard, by reviewing the surveys in the field, conducting moderation sessions with the experts at a conference, doing peer reviews and analyzing the industry trends. The purpose is to define an overall strategy with its respective requirements that aligns to business objectives taking into consideration product cybersecurity risks.

# 1. Introduction, Motivation and Research Questions

## 1.1 The importance of cybersecurity in automotive industry

Nowadays, the automotive industry is wrestling with the trends such as tighter emission controls, the rise of electric vehicles, car ownership versus mobility, connectivity, advanced driver assistance systems (ADAS), autonomous driving (AD), digitalization, new players in the market, safety and cybersecurity.

Cybersecurity deals with protection of the IT-system (hardware, software, data) against theft, attacks and/or damage from the environment. Cybersecurity of the vehicle systems is becoming more and more important as the means of interfaces with the outside environment are increasing and the number of requirements for electrical and electronical (E/E) systems are growing steadily. Moreover, the new trends such as e-mobility, autonomous driving, enhanced telematic services, driver support systems stimulates the need for cybersecurity. To define proper guidelines, automotive (vehicle) cybersecurity requires a well-defined risk analysis strategy.

The type and amount of cyber-risk depends on, for example, the:

- Cyber attacker's motivation
- Internal, local, and remote attacks (i.e. distance to the system)
- Magnitude of hazards when security is compromised
- Vulnerability (weaknesses which allow a cyber attacker to reduce a system's information) of system security

With regard to vehicle cybersecurity, vulnerabilities include:

- Hazards to the lives of drivers and passengers
- Hazards to real-time operation
- Limited computational performance
- Limited vehicle external connectivity
- Unpredictable attack scenarios and threats
- Large number of components/parts from many different suppliers

One of the most problematic aspects of cybersecurity is the fast and constantly evolving nature of security risks owing to the fact that cyberattacks are becoming more sophisticated and possess the ability to spread in a matter of seconds.<sup>1</sup>

Past computer systems processed information and did not interact with the physical world. Today, it is not surprising to see vehicles driving autonomously in cities from Munich to San Francisco. Nonetheless, the failure of the security controls of these vehicles could cause a danger to public safety and shake public confidence in the autonomous driving technology. The ability to assess the security of autonomous vehicle systems and provide assurances for risk reduction that the technology is safe to operate is critical for their success and acceptance.<sup>2</sup> Of the people who stated they never plan to buy an autonomous car, 30% listed the risk of hacking as the most important reason for not purchasing an autonomous automobile.<sup>3</sup>

In order to protect the assets and systems, it is required to know who, why and how the attack takes place and how the "good" and "bad" data could be distinguished from each other. However, in the general content of cybersecurity, the identification of an attacker's motivation is extremely difficult, as it may root from several sources. The motivations provided below were determined via a brainstorming session among the experts at Magna Powertrain:

#### Financially motivated crime

- all criminal offences that yield a direct financial benefit for the attacker
- theft of credit card number
- theft of identity
- manipulation of data, e.g. stocks and shares
- blackmail
  - use of ransomware
- sale of security software (e.g. McAfee USA, Kaspersky Russia)
- sale of security know-how

#### Industrially motivated crime

- industrial espionage
- gaining a competitive advantage

---

<sup>1</sup> cf. Möller, et al., 2019

<sup>2</sup> cf. Bailey, 2018: 9

<sup>3</sup> cf. Ponemon, 2017

- sabotage
  - destroying or manipulating
    - data, information
    - IT (Information Technology) architecture, infrastructures
    - systems

#### Politically motivated crime

- state-sponsored crime
  - to influence political decision making
  - to manipulate voting results
- gaining a state-level economic advantage
- act of terrorism
  - destabilisation of security
  - vandalism

#### Psychological motivation

- lust for destruction
- frustration coping
- inferiority complex
- revenge for anything
- boredom
- sports
- intellectual curiosity

Cybersecurity threats to conventional vehicles with automated features already exist. In their survey (i.e. by means of a internet survey) of 5000 respondents across 109 countries to gauge public opinion of fully-automated vehicles, Kyriakidis, Happee, and de Winter<sup>4</sup> found that people were most concerned about software hacking and misuse of vehicles with all levels of automation. Moreover, as the cars connect with the environment through wireless networks such as Bluetooth, keyless entry systems, cellular or other connections, hackers could take control of the vehicle.

---

<sup>4</sup> Kyriakidis, Happee, and de Winter, 2015

In 2013, by hacking a Chrysler Jeep through its internet connection and took control of its engines and brakes, Miller and Valasek demonstrated that malicious attacks on autonomous vehicles are a near-term possibility.<sup>5</sup>

## 1.2 Current challenges regarding cybersecurity

Although it is not possible to establish a complete list of challenges for cybersecurity, the most important challenges for cybersecurity are:

- no universal agreement on how the cybersecurity risks shall be measured,
- selection of right scale for the cybersecurity risk,
- how the uncertainty shall be dealt with,
- increasing number of vulnerabilities due to high number of features/functions offered,
- variety of suppliers,
- cost pressure (i.e. project and process related),
- growth of the cybersecurity industry,
- accountability (e.g. OEM, the driver, equipment supplier, hacker, pedestrian, other vehicles on the road, etc.) in the event of a software glitch, unpredicted circumstance or hack of the autonomous driving and connected vehicles,
- no prevailing set of rules, regulations and roles of insurance companies

## 1.3 Research focus and problem definition

According to the “Cost of Cybercrime Study” conducted by the consultancy firm Accenture across 11 countries in 16 industries, where 2,647 senior leaders from 355 companies were interviewed, the average number of security breaches increased 11% from 2017 to 2018 (67% increase in the last 5 years) and the average cost of cybercrime became \$13.0m in 2018.

---

<sup>5</sup> cf. Schellekens, 2016

As shown in Figure 1, the average cost of cybercrime in automotive industry has risen from \$10.7m to \$15.78m (increase of 47.48%) from 2017 to 2018.<sup>6</sup>

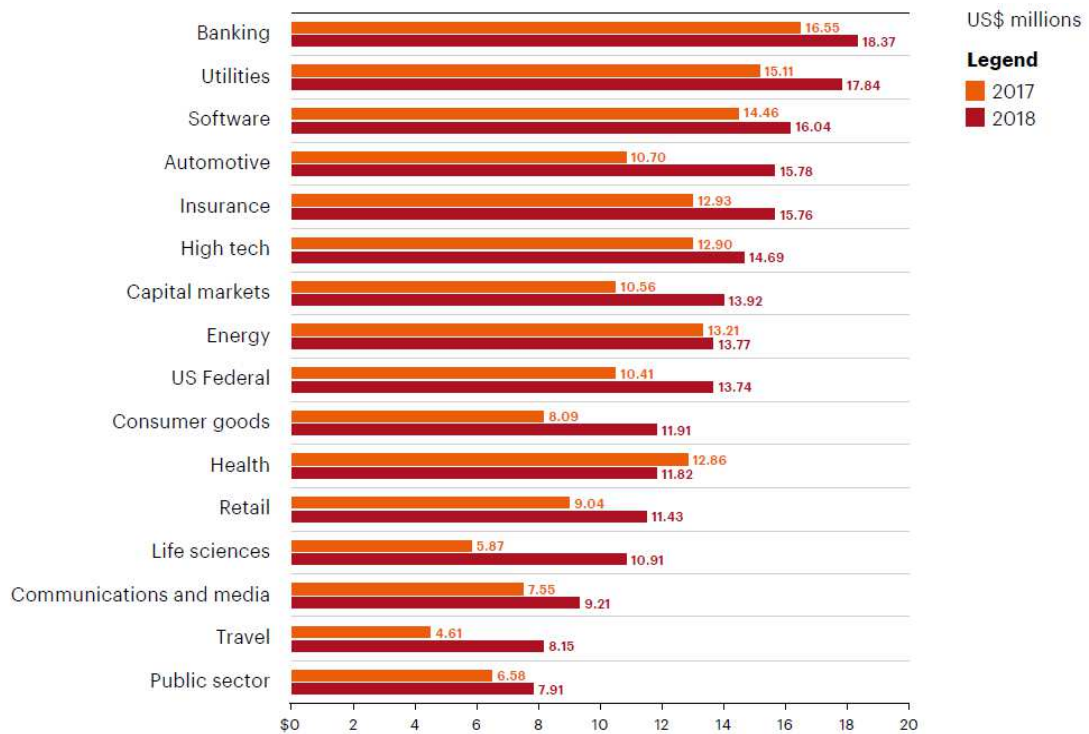


Figure 1: The average annual cost of cybercrime by industry<sup>6</sup>

Especially after the Jeep Chrysler hacking case, the interest of the media and general public towards cybersecurity in automotive industry increased dramatically. Although cybersecurity became a hot topic for the entire industry, yet still most companies are not aware how to anticipate possible risks or more concretely where to even start. Although the development of a global cybersecurity standard (ISO/SAE 21434) is ongoing, it only mentions *what to do*. The standard neither explains *why to do*, nor *how to do*. The focus of this thesis is to guide the automotive companies to be able to define an overall cybersecurity management policy in order to reduce the potential cybersecurity risks in a project. Furthermore, the thesis will help supporting the automotive companies regarding interpretation of the existing cybersecurity standards (i.e. ISO/SAE 21434) as well as explaining how to build a touchstone for cybersecurity development.

<sup>6</sup> cf. Kelly Bissell, et. al, 2019, 10

## 1.4 Research questions and aim

“Within the project management context, the important thing is not to keep risk out of the projects, but to ensure that the inevitable risk associated with every project is at a level which is acceptable and is effectively managed. According to the Project Management Institute<sup>7</sup>, project risk management includes the processes concerned with identifying, analysing and responding to project risk. It includes maximizing the results of positive events and minimizing the consequences of adverse events.”<sup>8</sup>

The master thesis aims at answering the following questions:

- What are the project and company independent qualitative risks that can arise from cybersecurity threats and how can they be reduced by an overall cybersecurity management policy?
- How does an overall cyber security management policy have to look like in order to reduce the potential project risks?
- How can the ISO/SAE 21434 (Road vehicles-Cybersecurity Engineering) be used to create an overall cybersecurity management policy to reduce the potential project risks?

Although the cost of cybercrime is constantly increasing and every single company and their projects are vulnerable for cyber-threats, most companies either do not perceive the importance of cybersecurity or they don't know how to deal with it. The goal of this academic work is to provide a project, company-scale, location independent recipe, which does not require a high investment, nevertheless will reduce the potential project risks stemming from cybersecurity issues.

The expected result of the research is the creation of an overall cybersecurity management policy to reduce potential project risks, which is SAE/ISO 21434 compliant, that fulfills the business needs, reflects the state of the art and is in alignment with the project management practices. The results will reflect the required content of the overall cybersecurity management policy.

---

<sup>7</sup> PMI, 2013

<sup>8</sup> Lamas, et al. 2012, 1



## 1.5 Research approach and methodology

The author of this thesis is working as global functional safety manager at a global automotive industry company. In addition, since 2018, he is member of ISO TC22-SC32-WG11, which is the working group of ISO that is responsible from creation of the ISO/SAE 21434 standard.

The overview of the research approach and methodology is shown in Figure 2.

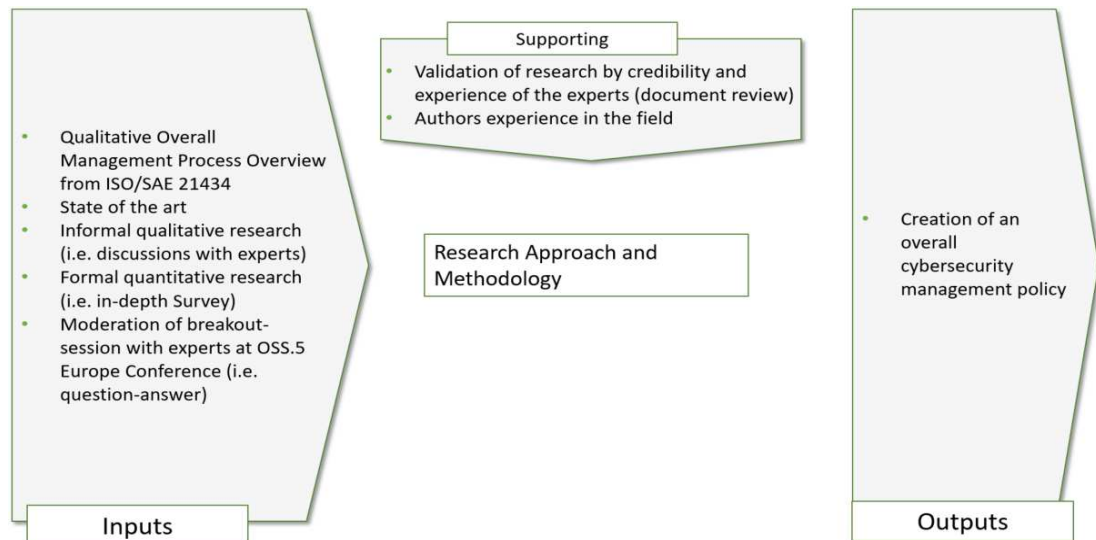


Figure 2: Overview of the research approach and methodology

This thesis utilized the following research approach and methodologies in order to answer the research questions stated in chapter 1.4:

- Qualitative overall management process overview including potential benefits and challenges of creating an overall cybersecurity management policy from ISO/SAE 21434.
- Researching the existing literature resources conducted in the field to comprehend the state of the art (especially the existing norms/standards such as SAE/ISO 21434, J3061, etc.).
- Informal qualitative approaches, such as discussions with employees and experts
- Formal quantitative research through in-depth survey about automotive industry cybersecurity practices, which was conducted by SAE and Synopsys (obtaining expert ideas and opinions)<sup>9</sup>. The survey enables the collection and sharing of opinions and interesting ideas from the participants who have expertise in the field.

<sup>9</sup> SAE and Synopsys (2018): Securing the modern vehicle: A study of cybersecurity automotive practises

- Obtaining expert opinions via moderation of a break-out session discussion at the OSS.5 Europe 2019 conference, which was conducted on September 26-27<sup>th</sup>, 2019 in Berlin. The opinions of the experts were asked about the questions related to the research questions and the answers were utilized.
- Validation of the research by credibility and experience of the experts (i.e. comments of the experts were considered as part of the review of the created overall cybersecurity management policy)
- Author's years of professional experience in functional safety and the knowledge gained through the ISO Meetings, where the author participated as ISO TC22-SC32-WG8 (Working Group Functional Safety) and WG11 (Working Group Cybersecurity) Austrian Member.

## 1.6 Structure of the thesis

Figure 3 illustrates the overview of the master thesis structure.

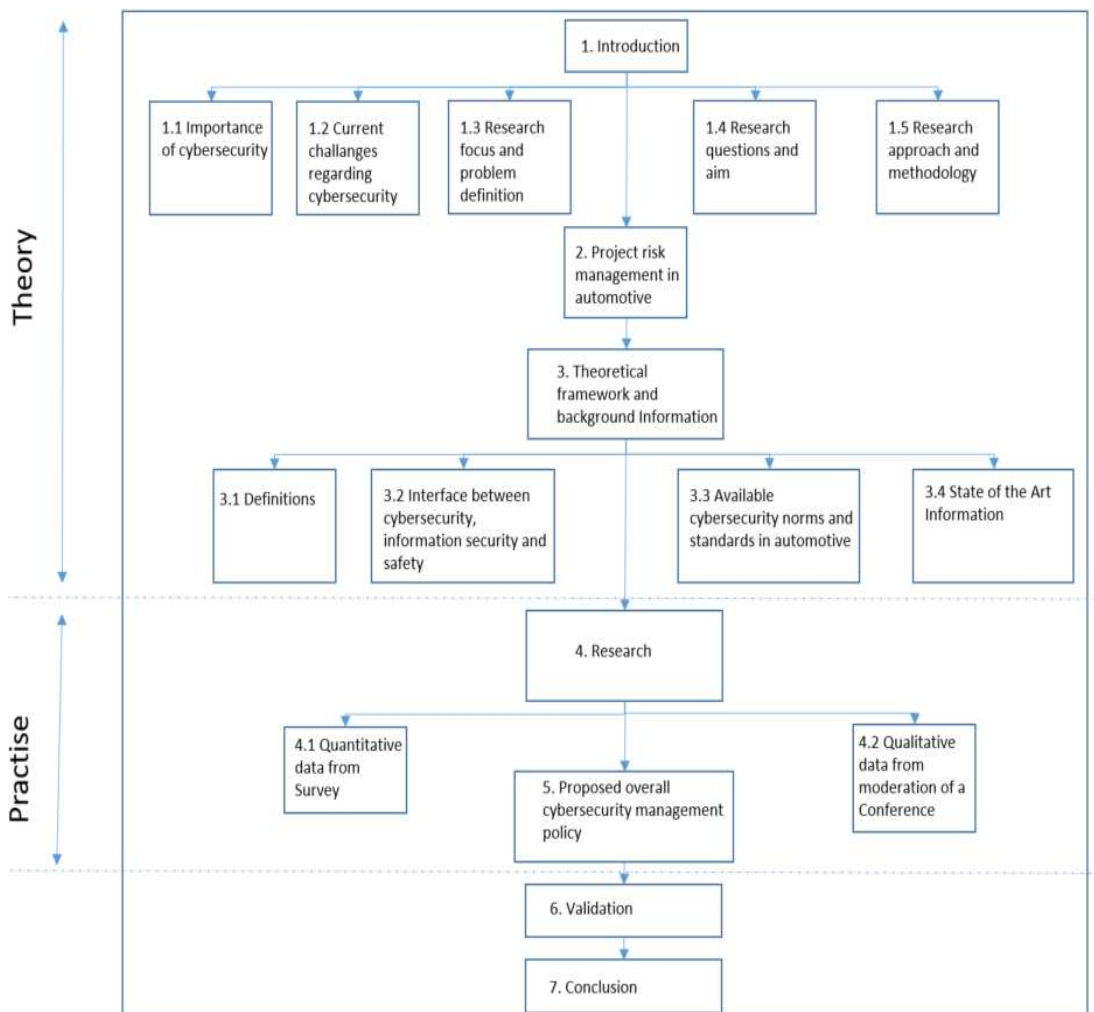


Figure 3: Overview of the master thesis structure

Chapter 1 gives an introduction about importance of cybersecurity, the challenges regarding cybersecurity in the automotive industry, the research focus and the definition of the problem, the research questions, aim, approach and methodology, which will be carried out. Subsequently, in chapter 2, the project risks in automotive industry, factors that increase project risks and the cybersecurity threats and risks that are posed to projects are explained. In chapter 3, the theoretical framework and background information is provided. This contains the definitions related to cybersecurity to give a better understanding to the reader, then explaining the interface to other areas such as information security and safety and finally introducing the available norms, standards and state of the art in automotive regarding cybersecurity. In chapter 4, the conducted research based on a quantitative data from a survey and qualitative data from moderation of a conference are presented. In chapter 5, the overall cybersecurity management policy, the content of the document and how to create such a document are explained (for details please see chapter 5). Subsequently, how the overall management policy was validated is explained in Chapter 6. Finally, in conclusion part, key points, final outcomes based on collected data and research and thoughts of the author about the study are expressed.

## 2. Project risk management in automotive industry

### 2.1 Risk and Risk Management

Federal Information Processing Standard 200 defines risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence"<sup>10</sup>. Similarly, ISO 31000 defines risk as "effect of uncertainty on objectives," which implies that risk is neither positive or negative<sup>11</sup>. Risk is defined in Equation 1. Risk = Impact × Likelihood (Equation 1)

Although it is not possible to eliminate the cybersecurity risk, i.e. no system or product would be 100% secure, and there will always be a residual risk, the purpose of risk reduction is to reduce the not acceptable risk to an acceptable level as shown in Figure 4.

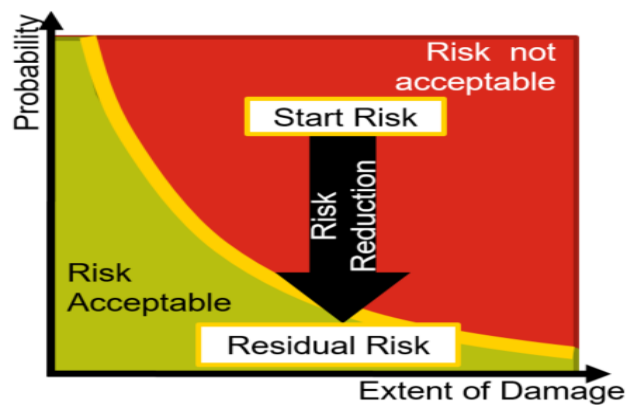


Figure 4: Reduction of the start risk to an acceptable level in cybersecurity<sup>12</sup>

Risk management, which is not rocket science but is much more complicated<sup>13</sup>, is an organizational process to measure and manage risk. Risk management is common in many industries as a way to protect an organization from uncertainty. Risks could be financial, operational, legal, or other ways such as strategic and political. This thesis chooses to focus on cybersecurity risks. Organizations have four options for handling risks once identified:<sup>14</sup>

- Avoidance: Eliminate the cause of the risk
- Control: Implement controls to reduce the risk

<sup>10</sup> National Institute of Standards and Technology, 2006

<sup>11</sup> International Organization for Standardization, 2018b

<sup>12</sup> own depiction

<sup>13</sup> cf. John Adams 2005

<sup>14</sup> cf. Bailey, 2018: 21

- Transference: Contract with a third party to buy insurance against the risk, hedge against the risk, or outsource the risk
- Acceptance: Accept the risk

## 2.2 Factors that increase risks of a project

### 2.2.1 Risks posed to projects through cybersecurity threats

“There is evidence that cybersecurity threats pose risks to projects in terms of both project execution as well the project deliverables.<sup>15</sup> Any cybersecurity risk that would affect an organization can also affect projects within that organization. For example, most projects depend on the same enabling technology resources to carry out project tasks (e.g. - mobile devices, infrastructure, networks, and workstations) that are also used for other business activities. If these devices are disabled or compromised, impacts to the project will be unavoidable and may be disastrous.”<sup>15</sup> Project deliverables may also be vulnerable to cybersecurity risks, which becomes a concern for project management. An example could be a decision to source components for a new product from a supplier.<sup>16</sup>

Due to the unique nature of cybersecurity risks, specialized knowledge is required to assess and the security control mechanisms required to avoid or mitigate them; cybersecurity threats present unique challenges to project management.<sup>16</sup> These threats are very broad in nature, both in terms of the wide variety of potential attack vectors, the types and mechanisms of threats, and the fact that all phases of the project are potentially affected.<sup>17</sup> In addition, the posed cybersecurity risks change rapidly as new threats and vulnerabilities are discovered constantly. Therefore, controlling the risks that are associated with cybersecurity threats often require highly specialized and technical solutions (such as firewalls, intrusion detection software, network segregation, etc.) as well as specialists to implement and monitor.

### 2.2.2 Cybersecurity risk in supply chains

Among the risks that are posed to projects, supply chain risks remain the weakest link in cybersecurity, because organisations can not always control the security measures taken by the supply chain partners, which creates opportunities for cybercriminals to attack an

<sup>15</sup> Hendershot, 2014; US DoD, Sept. 2015

<sup>16</sup> cf. Presley et al., 2016, 1

<sup>17</sup> US DoD, Jan. 2015 and Sept. 2015

organisation by infiltrating first a supply chain partner. Hence, it is important for the organisations and their partners to be aware of this risk and act to protect each other. The reason why different organisations along supply chain are targeted is because often they are not aware of potential threats and may not have adequate resources to manage cybersecurity.<sup>18</sup>

Moreover, since projects involve the integration of components from various suppliers, this becomes a source of risk for the projects and its deliverables. The selection of suppliers is a part of project management concern, as it is related to procurement and the quality of the project output.<sup>19</sup>

Two main gaps regarding the cybersecurity risks at supply chain that are affecting the project management are:<sup>20</sup>

- 1) Insufficient understanding of the particular characteristics of cyber-risks and how these compare to other supply chain risks for effective risk management, and
- 2) Insufficient addressing by current methods to aspects of compartmentalization, static focus and history-dependence in the management of supply chain cyber-risk and cyber-resilience

### **2.2.3 The necessity of an overall cybersecurity management policy to reduce the potential project risks**

“As the automotive world becomes increasingly more interconnected through digital transformation, users must pay more attention to the security of their digital connections, since the past decade has witnessed a remarkable increase in the use of digital technologies. However, the newest wave of digital technologies is different. This has been accompanied by the fast, constantly evolving spread of security risks. It seems as though every week there are new headlines about cyberattacks bringing an organization’s computers or network to its knees, with the resulting bad publicity and embarrassing revelations appearing as front-page news. This raises the question of how to protect organizations and systems from these issues. The best protection is the development and implementation of plans and procedures to improve intrusion detection and prevent/eliminate vulnerabilities.”<sup>21</sup>

---

<sup>18</sup> Sean Duca (2019): Supply chain remains the weakest link in cybersecurity

<sup>19</sup> PMI, 2013

<sup>20</sup> cf. Estay et al., 2017, 9

<sup>21</sup> Möller et al., 2019

As mentioned earlier, the incurred cybersecurity threats increase the project risks. Therefore, all the measures that reduce the cybersecurity threats will also reduce the corresponding potential project risks. When it comes to dealing with cybersecurity risks, just installing a firewall or an anti-virus software is not sufficient to protect the organisation, business or project from cyber threats. In order for a company to protect their organisation properly, a cybersecurity risk management framework, i.e. overall cybersecurity management policy is required. The technology based solutions could then be part of the framework. The overall cybersecurity management shall include the policies, rules, roles and strategies to protect the organisation from cyber threats as managing cybersecurity risk is critical for the success of an organization's mission in order to achieve business as well as the project goals. As the companies become more aware of the cybersecurity risks and create policies and company-specific cybersecurity infrastructure within their organisation, they can set up repeatable processes and actions, which can be taken across all projects and for all incidents (i.e. an attack on the system that may have or may not have been successful (SAE J3061)).<sup>22</sup>

By creating an overall cybersecurity management policy, a company could not only reduce the potential project risks, but also will have a more effective resource allocation, operational efficiency, ability to mitigate and respond to cybersecurity risks.

The cybersecurity self-assessment study conducted by a well-known consultant company indicates the importance of an overall cybersecurity management policy for the reduction of potential project risks. The descriptions for priority, risk reduction and overall level of effort needed for implementation are shown in Figure 5.

Item	Description	● HIGH	● MEDIUM	● LOW
<b>Priority</b>	An estimate of the priority based on risk and opportunity	Foundational and necessary to successfully execute subsequent security initiatives	Important part of an effective security program	Enable more timely and efficient responses to emerging risks
<b>Risk reduction</b>	Describes the level of potential risk reduction and business benefit	Recommendation provides high benefit in risk reduction	Recommendation will help to reduce risk in certain moderate risk areas	Recommendation will help to reduce risk in low risk areas
<b>Overall level of implementation time</b>	Approximate time to complete initiative	> 6 months	3-6 months	0-3 months

Figure 5: Descriptions for priority, risk reduction and overall level of effort needed for implementation

<sup>22</sup> Brad Egeland (2015): How much will cybercrime affect project management.in 2016?



Recommendations on different focus areas with respect to priority, risk reduction and overall effort from the same study are illustrated in Figure 6 and 7.

Focus area	#	Recommendation	Priority	Risk reduction	Overall implementation time
<u>Strategy and alignment</u>	1	Establish a product cybersecurity strategy	● HIGH	● HIGH	● LOW
	2	Establish a formal governance structure for product cybersecurity	● HIGH	● HIGH	● LOW
	3	Adequately staff product security roles	● HIGH	● HIGH	● MEDIUM
<u>Governance and organization</u>	4	Formally publish and communicate policies and standards	● HIGH	● MEDIUM	● MEDIUM
	5	Enhance customer communications and response capabilities	● MEDIUM	● MEDIUM	● LOW
	6	Establish a formal product cybersecurity training and awareness program	● MEDIUM	● HIGH	● MEDIUM
	7	Establish a formal product cybersecurity risk management program	● HIGH	● HIGH	● MEDIUM
<u>Architecture</u>	8	Formalize product cybersecurity architecture roles and responsibilities	● MEDIUM	● MEDIUM	● MEDIUM
	9	Document and communicate product cybersecurity standards	● LOW	● MEDIUM	● MEDIUM
	10	Establish and communicate minimum product cybersecurity requirements	● MEDIUM	● LOW	● MEDIUM
<u>Requirements</u>	11	Perform threat modeling	● HIGH	● HIGH	● HIGH
	12	Expand current capabilities to consider applicable security domains	● MEDIUM	● MEDIUM	● LOW

Figure 6: Recommendations on different focus areas with respect to priority, risk reduction and overall effort from Self-Assessment Study (Points 1-12)



Focus area	#	Recommendation	Priority	Risk reduction	Overall implementation time
Design	13	Enhance cybersecurity process and engagement requirements	● HIGH	● HIGH	● MEDIUM
	14	Require secure software update be a default feature	● LOW	● MEDIUM	● MEDIUM
	15	Create and implement secure data communication protocols	● LOW	● HIGH	● MEDIUM
Build	15	Develop secure coding standards	● LOW	● MEDIUM	● MEDIUM
	16	Develop a secure product testing methodology	● MEDIUM	● HIGH	● MEDIUM
Deployment and support	17	Develop product cybersecurity operational processes	● MEDIUM	● MEDIUM	● MEDIUM
	18	Enhance incident response process	● MEDIUM	● HIGH	● MEDIUM
	19	Develop operational guidance documentation	● LOW	● LOW	● LOW
Metrics and Reporting	20	Establish a product cybersecurity metrics and reporting program	● LOW	● MEDIUM	● MEDIUM

Figure 7: Recommendations on different focus areas with respect to priority, risk reduction and overall effort from the Self-Assessment Study (Points 13-20)

The points 1-6 and 17-19 in Figure 6 and 7 are related to overall cybersecurity management and most of the recommendations require low effort to implement and their risk reduction effects are mainly high.

“An incident response plan documents processes used to help respond to cybersecurity incidents. A comprehensive response plan that develops increased awareness and capabilities and that establishes communications protocols between automotive manufacturers, suppliers, cybersecurity researchers, and government agencies could assist industry stakeholders in coordinated efforts to address discovered vulnerabilities and enhance product cybersecurity. The forthcoming best practices such as ISO/SAE 21434 aim to address incident response plans that may include processes to activate response teams, notify an internal chain-of-command, and trigger response activities to assess and counter cyber-attacks. A comprehensive incident response plan provides strategic flexibility for managing many types of cyber incidents and takes into account internal resources and, where appropriate, external resources likely needed to support incident response measures. The development of protocols for recovering from cybersecurity incidents is also important for ensuring consistent approaches for making available updates to vehicles in a reliable and expeditious manner based on specific circumstances”.<sup>23</sup>

<sup>23</sup> Members of Auto Alliance and Global Automakers (2016): Framework for Automotive Cybersecurity Best Practices

An overall cybersecurity policy shall also include the strategy of a company, about how an incident will be responded including creation of the necessary awareness, resources, accomplishing the required updates and definition of roles and responsibilities. An incident response plan proposal is explained in chapter 5.18.

#### 2.2.4 Drivers for cybersecurity investment

According to a report on identifying how firms manage cybersecurity investment<sup>24</sup>, the most important drivers for investment are perceived risk reduction, compliance and industry best practises, respectively. The report was based on 40 interviews with information security executives (chief security officer level) and managers from variety of firms and government agencies. The purpose of the report was to learn more about how organizations decide about their cybersecurity investment decisions. According to the same report<sup>24</sup>, when the participants were asked to name the approaches they use to identify which threats are most important and prioritize accordingly, the top two answers were *industry based practises* and *frameworks*. Therefore, one can conclude that an overall cybersecurity management policy is one of the most preferred and proposed way to identify the threats, hence the risks as it includes the cybersecurity risk management according to the ISO/SAE 21434<sup>25</sup>, which can be considered as one of the few industry based practises.

Irrespective of the industry a company is operating (because business and organizational results are achieved mainly due to successful implementation of projects), project management is the driving force of the organization and strives to make most of the invested resources. In automotive industry, as the number of projects is high this becomes even more important. A better approach to project management starts at the portfolio level, that is a materialized strategic vision of the organization through a whole range of investments. More and more companies and organizations are aware of the fact that investing time and money to build professional project methodologies and processes pay off ultimately to reduce costs and risks, improve efficiency and customer satisfaction as well as the relationship between business parties involved.<sup>26</sup> Therefore, an upfront investment in overall cybersecurity management policy will help companies to reduce potential project risks.

---

<sup>24</sup> cf. Moore et al. 2015: 8-9

<sup>25</sup> ISO/SAE 21434 – Road vehicles – Cybersecurity engineering, draft for intended DIS

<sup>26</sup> Sabo, 2016, 7

### 3. Theoretical framework and background information

#### 3.1 Definitions and Key concepts

In this chapter, the definitions that are related to cybersecurity are explained.

##### **Cyberspace**

“A metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop.”<sup>27</sup>

##### **Cyber-system**

“A cyber-system is a system that makes use of a cyberspace.”<sup>28</sup>

##### **Cyber Threats**

“A cyber-threat is a threat that exploits a cyberspace. Cyber-threats may be malicious (e.g. denial of service (DoS) attacks and injection attacks that are caused by intention) or non-malicious (e.g. systems that crash due to programming errors or loss of Internet connection due to wear and tear of communication cables or other hardware).”<sup>28</sup>

##### **Cybersecurity**

“Cybersecurity the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.”<sup>29</sup>

##### **Asset**

“An asset is anything of value to a party. The party is the entity or unit, such as a company or other organization, for which the assets in question have value. In the same way as there is no risk without an asset, there is no asset without a party. What is held as assets and how valuable they are depend on the party; therefore, it is always needed to be specific about who the party is when the risk is managed or assessed.”<sup>28</sup>

---

<sup>27</sup> Vangie Beal: What is cyberspace?, Webopedia

<sup>28</sup> Refsdal, et al. 2015

<sup>29</sup> National Initiative for Cybersecurity Careers and Studies, 2008

In order to understand the term asset in the scope of cybersecurity it is important to comprehend the three pillars of information security, which are *confidentiality* (i.e. avoiding unauthorized access to protected resources), *integrity* (i.e. avoiding and detecting unauthorized modifications of information or components), and *availability* (i.e. proper and timely access to data and services by the authorized entities) of information. The pillars can be extended for authenticity, which is verification of origin of information and governance (i.e. security policies). Therefore, the goal of cybersecurity in a broader sense is to ensure confidentiality, integrity, availability, authenticity and governance of the assets in cyberspace. As the attacks are performed against assets and they cause threats, it is vital to understand the meaning of asset for cybersecurity. The relation between asset, threat and attacks are shown in Figure 8.

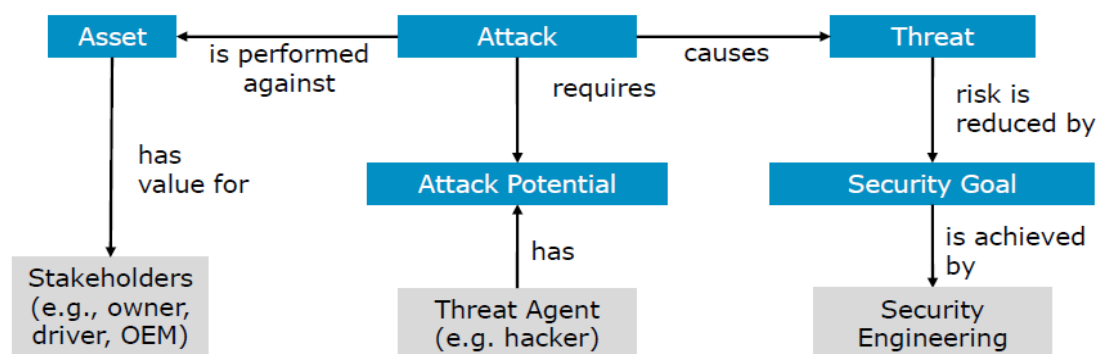


Figure 8: The relation between asset, attack, attack potential, threat and security goal<sup>30</sup>

“Vulnerabilities are the weaknesses, flaws, or deficiencies that can be exploited by a threat to cause harm to an asset, whose criticality depends on the threats that may exploit them. A threat is an action or event that is caused by a threat source, which is the potential cause that may lead to an incident. Hence, without assets there is nothing to harm, without vulnerabilities there is no way to cause harm, and without threats there are no causes of harm.”<sup>31</sup>

The relation between threat source, threat, vulnerability and risk is shown in Figure 9.

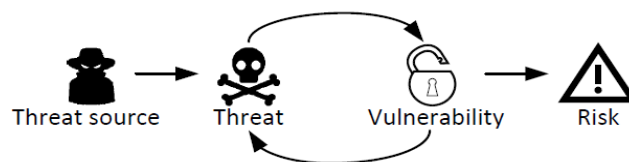


Figure 9: The relation between threat source, threat, vulnerability and risk<sup>32</sup>

<sup>30</sup> Vector (2019): Automotive Cybersecurity Webinar

<sup>31</sup> Solhaug, 2015

<sup>32</sup> Refsdal, et al. 2015

In order to identify the assets in a company, the following checklist questions can be asked:<sup>33</sup>

- 1) Which information, algorithm or intellectual property shall remain confidential?
- 2) Which data (e.g. configuration parameters) shall remain unchanged?
- 3) Which functions or procedures shall only be applied by e.g. OEM?
- 4) Which functions or data shall be always available?
- 5) Which company guidelines or legal requirements on data or procedures shall be fulfilled?

By answering the above listed questions, an automotive company (in general any company) can determine their assets. The specific asset categories in automotive industry are illustrated in Figure 10.

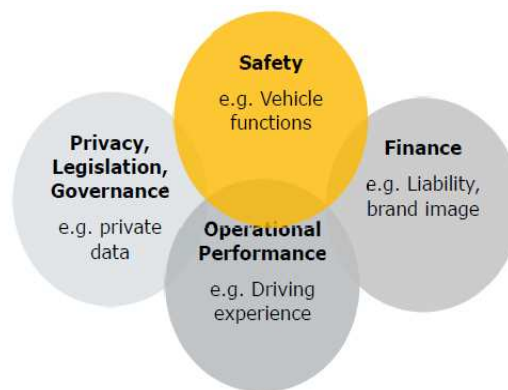


Figure 10: Specific automotive asset categories<sup>33</sup>

In relation to the reasons given in chapter 2.1, an overall cybersecurity management policy will reduce and/or avoid a lot of threats against the assets of the companies by reducing the attack potentials. This topic will be elaborated in chapter 5.

## Party

“A party is an organization, company, person, group, or other body on whose behalf a risk assessment is conducted. A party is not same as a stakeholder. A party may be thought of as a stakeholder, but in a risk assessment situation there are normally many stakeholders that are not parties. In most risk assessments there is only one party. If, however, there are several parties then the assets of the different parties must be kept apart. The same object, for example a human life, may be an asset of different values or different parties.”<sup>34</sup>

<sup>33</sup> Vector (2019): Automotive Cybersecurity Webinar

<sup>34</sup> Refsdal, et al. 2015

## Stakeholder

“A stakeholder in this context is basically any person or organization that may affect or be affected by the subject of the assessment. If a risk assessment is conducted on behalf of a company then the company is the party. Within and related to the company there may be many stakeholders (for instance, employees and suppliers) with all kinds of conflicting interests and they are not parties in this risk assessment. When assets are identified on behalf of a party, solely the interests of the party in question are focused.”<sup>35</sup>

## Incident

“Breach of a system's security policy in order to affect its integrity or availability and/or the unauthorized access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).”<sup>36</sup>

## Likelihood

“Likelihood is that something will happen.”<sup>37</sup> It can be described qualitatively as well as quantitatively.

## Risk

“A risk is the likelihood of an incident and its consequence for an asset. Basically, risk is the potential that something goes wrong and thereby causes harm or loss. The gravity of a risk depends on its likelihood to occur and its consequence. The consequence is the impact on an asset, which is wanted to be protected.”<sup>35</sup>

The relation between risk, incident, asset, likelihood and party is shown in Figure 11.

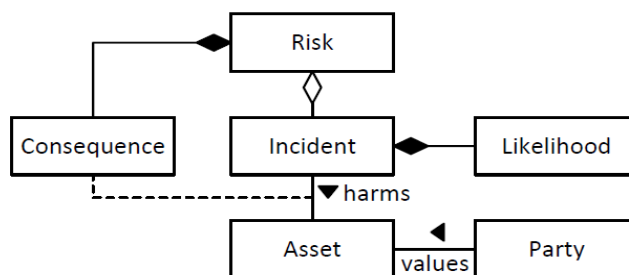


Figure 11: The relation between risk, incident, asset, likelihood and party<sup>35</sup>

<sup>35</sup> Refsdal, et al. 2015

<sup>36</sup> National Cybersecurity Centre (2018), What is a cyber incident?

<sup>37</sup> Cambridge Dictionary, Likelihood?

“The relation represented by a line with a black diamond connecting risk and consequence captures that consequence is an ingredient that belongs to risk. The consequence represents the impact of an incident on an asset. Consequence is therefore also connected to the relation between incident and asset, since it is a measure of harm. The same incident may give rise to several risks. Risk is therefore connected to incident with a white diamond to express that although incident is an ingredient of risk, it does not necessarily belong uniquely to one risk.”<sup>38</sup>

### **Risk Identification**

“Risk identification involves determining what could happen to cause potential harm to assets (the valuables aimed to be protected) which includes gaining insight into how, where, and why such incidents may occur, irrespective of whether the source of the cyber-risk is under the control of the party on whose behalf the cyber-risk assessment is carried out.”<sup>38</sup>

### **Risk Analysis**

“Risk analysis involves determining the level of cyber-risk, typically in terms of the likelihood of incidents to happen and the consequence for assets. This can be done qualitatively or quantitatively.”<sup>38</sup>

### **Risk Evaluation**

“Risk evaluation is the task of comparing the results of the risk analysis with the risk evaluation criteria (defined during context establishment) to determine whether the cyber-risks need treatment. It also involves aggregation and grouping of risk that should be considered together.”<sup>38</sup>

### **Risk Treatment**

“Risk treatment involves deciding on strategies and controls to deal with cyber-risks. It also involves deciding to accept the (residual) cyber-risk, and formally recording the decisions and responsibilities.”<sup>38</sup>

---

<sup>38</sup> Refsdal, et al. 2015



### 3.2 The interface between Cybersecurity, Information Security and Functional Safety

“Information security is the preservation of confidentiality, integrity and availability of information.”<sup>39</sup> Information can be in any form such as electronic, material, or knowledge of personnel. In order to ensure and maintain information security, information in all formats needs to be protected from threats and threat sources of any kind, including physical, human, and technology-related threats. Since threats may also target information assets in the cyberspace, information security is an important part of cybersecurity.

However, cybersecurity is not limited to the protection of information assets only, it also concerns the protection of infrastructure. One maybe concerned about the wider impact of threats to information or infrastructure security in order to protect assets such as life, health, reputation, finance, availability, etc.. Cybersecurity goes beyond information security as it is not limited to the protection and the preservation of confidentiality, integrity and availability of information assets. Information security, in contrast, goes beyond cybersecurity as it is not limited only to threats that arise via cyberspace. The relation between information security, cybersecurity and ICT (information and communication technology) security is illustrated graphically in Figure 12.

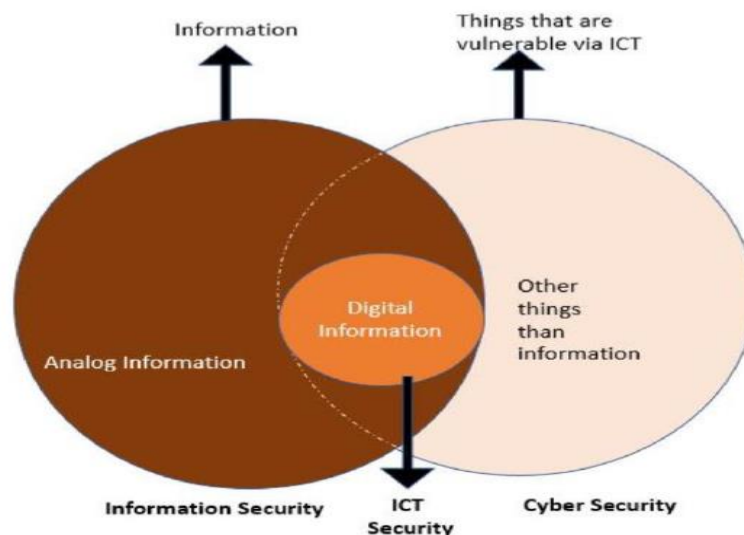


Figure 12: The relation between information security, information and communication technology security and cybersecurity<sup>40</sup>

<sup>39</sup> British Standards Institution, 2016

<sup>40</sup> Hack2Secure (2017): Cybersecurity vs. Information Security



“Safety can be defined as the protection of life and health by the prevention of physical injury caused by damage to property or to the environment. One of the main differences between safety and cybersecurity is that while safety focuses on system incidents that can harm the surroundings, cybersecurity focuses on threats that cause harm via a cyberspace. A further difference is that the assets that are considered with respect to safety are usually limited to human life and health, as well as environmental assets, while the assets of concern with respect to cybersecurity can be anything that needs to be protected.”<sup>41</sup>

According to SAE J3061<sup>42</sup>, system safety is the state of a system that does not cause harm to life, property or to the environment, whereas cybersecurity is the state of a system that does not allow exploitation of vulnerabilities to lead to losses, such as financial, operational, privacy, or safety losses. All safety critical systems are cybersecurity-critical because a cyber-attack either directly or indirectly on a safety critical system could lead to potential safety losses. On the contrary, not all cybersecurity-critical systems are safety critical since cyber-attacks on cybersecurity-critical systems can result in losses other than safety losses; namely, privacy, operational or financial.

As an example, entertainment system is just cybersecurity critical and may lead to privacy and financial losses; however, steering system is both cybersecurity and safety critical. The relation between safety critical and cybersecurity critical systems is highlighted in Figure 13.

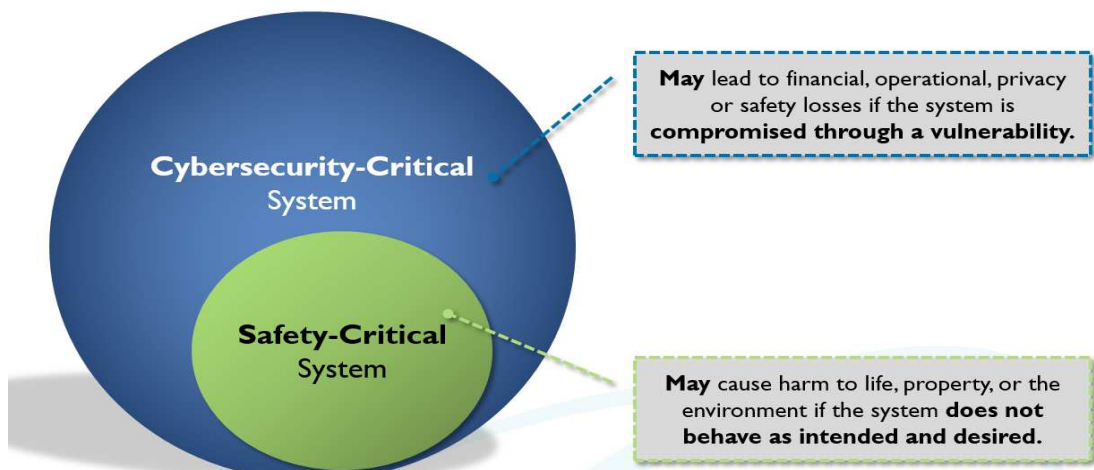


Figure 13: The relation between safety critical and cybersecurity critical systems (SAE J3061)<sup>42</sup>

<sup>41</sup> Refsdal, et al. 2015

<sup>42</sup> SAE J3061- Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

### 3.3 Cybersecurity norms and standards applicable in automotive industry

A literature review is a first step towards understanding the state of the knowledge in a specific field, which for this thesis is the knowledge regarding creation of an overall cybersecurity management policy in order to reduce project risks. A literature review process avoids “reinventing the wheel”<sup>43</sup>, integrates existing knowledge through the accumulation of scattered and potentially unconnected research, and revitalizes the development of knowledge.<sup>44</sup>

An overview of the standards, assessments, software coding standards, organisations and methods that are related with cybersecurity are shown in Figure 14. In this thesis, ISO/SAE 21434 will be investigated and utilized in detail.

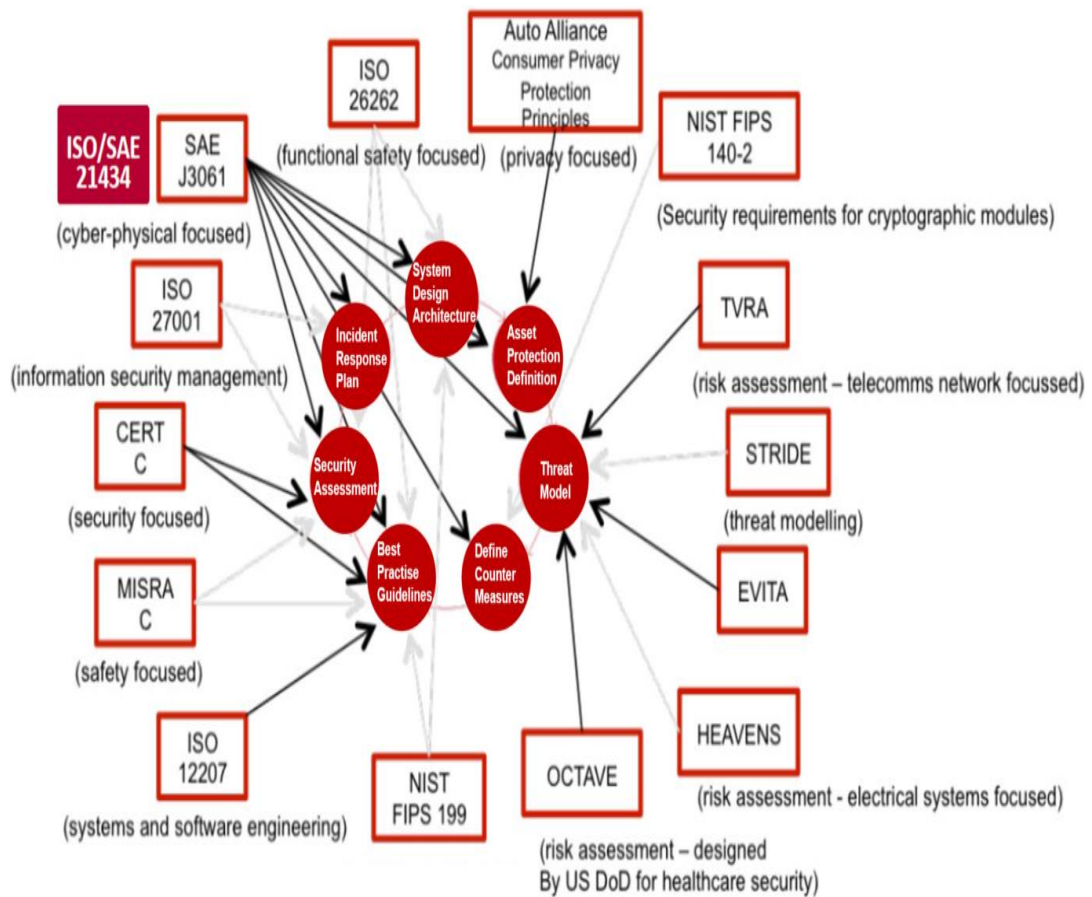


Figure 14: Overview of standards, assessments, software coding standards, organisations and methods related to cybersecurity<sup>45</sup>

<sup>43</sup> Zorn et al., 2006

<sup>44</sup> Webster et al., 2002

<sup>45</sup> Vector (2018): Automotive Cybersecurity Training

### 3.3.1 Product Liability

Every producer is liable for its product. “Product liability puts the burden of proof for acting with due care on the manufacturer.”<sup>46</sup> A product, which is put in service, must provide the level of safety, which can be expected by the general public. According to law, the companies shall require protecting themselves against foreseeable harms. “Manufacturer’s liability is excluded, if a failure can not be detected using current state of science and technology at the time the manufacturer put the product into market.”<sup>47</sup> Hence, in case of trials, only well-defined and followed processes and good documentation can help companies.

As seen in chapter 3.2, safety and cybersecurity are related, i.e. if a product is not secure it can not be safe, cybersecurity also becomes part of product liability. Although it is still a debatable question if a product can be hacked, whether it is defective or not and who should be accountable for that in front of the law, it has no doubt that companies should prove their implemented processes and cybersecurity measures in order to claim that they followed the state of the art. “Today, for the most part, liability for cybersecurity failures – meaning those responsible for writing code that can be manipulated to perform in a way contrary to that anticipated by its writers - is almost non-existent.”<sup>48</sup> Nevertheless, there is no doubt it will change in the near future, especially when ISO/SAE 21434 is officially released.

### 3.3.2 Legally binding vs. Suggestion Requirements with respect to Product Liability

Although ISO standards are considered to be the state of the art, they are only suggestions for the companies and are not legally binding. Nevertheless, although standards are not laws, they are legally meaningful. If a company sells a product that could impact safety and does not conform to the well-recognized standard (e.g. ISO 26262), they are exposing their customers to a risk. Therefore, although the ISO standard are considered as suggestion, for the companies to argument that they followed the state of the art, it is important for them to apply the existing ISO standard on the topic they are working on. The overview of the legal requirements, which are homologation such as ECE (Economic Commission for Europe) for automotive products that are sold within European Union and FMVSS (Federal Motor Vehicle Safety Standards) for automotive products that are sold within United States, and technical recommendations that are suggestions are shown in Figure 15.

---

<sup>46</sup> kVA (2016): An Overview of Functional Safety for Automotive

<sup>47</sup> Vector (2016): Functional Safety with ISO 26262 Webinar

<sup>48</sup> Paul Rosenzweig (2017): The Evolving Landscape of Cybersecurity Liability

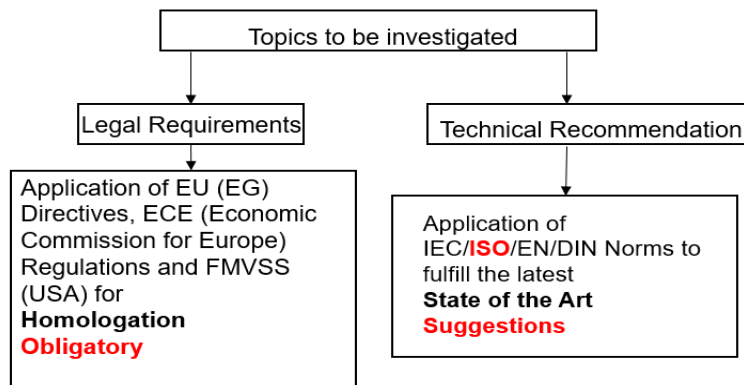


Figure 15: Difference between legally binding requirements and ISO Standards<sup>49</sup>

### 3.4 State of the art information (including risk assessment methods according to ISO/SAE 21434-Road vehicles-cybersecurity engineering)

ISO/SAE 21434 standard was initiated due to the fact that when it was initiated at the beginning of 2016, there existed no cybersecurity standard apart from SAE J3061 “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems” which was a guidebook. In September 2016, SAE & ISO defined cooperation agreement in order to work together to develop a cybersecurity standard for road vehicles and intelligent transportation systems. ISO/SAE 21434 is planned to be jointly released by both SAE and ISO in November 2020.

The benefits of such a standard are:<sup>50</sup>

- Defining common terminology for use throughout the supply chain
- Driving industry consensus on key cybersecurity issues
- Setting minimum criteria for vehicle cybersecurity engineering
- Being reference for the regulators
- Providing evidence for importance of cybersecurity in the automotive industry

82 companies from OEMs (e.g. BMW, Volvo, Daimler, VW, GM, Ford, Nissan, Toyota, JLR, Renault, Mitsubishi, Honda, Opel, FCA, etc.), Tier 1-n (e.g. Magna, Bosch, Continental, Valeo, Denso, Delphi, Wabco, Infineon, Intel, etc.), cybersecurity companies (Vector, Synopsys, etc.), government and standard organisations (e.g. SAE, ISO, VDA, NIST, etc.) participated in the development of the ISO/SAE 21434 standard.

<sup>49</sup> Own depiction

<sup>50</sup> Angela Barber (2018): Status of Work in Process on ISO/SAE 21434 Automotive Cybersecurity Standard

The key principles of the standard are:<sup>51</sup>

- 1) The goal is reasonably secure vehicles and systems
- 2) Automakers and suppliers to benefit from the standard to show “due diligence”
- 3) Focus on automotive cybersecurity engineering (although it includes more than engineering)
- 4) Based on current state-of-the-art
- 5) Risk oriented approach
- 6) Management activities for cybersecurity (especially overall cybersecurity management)
- 7) Cybersecurity activities/processes for all phases of vehicle lifecycle
  - a. Design and Engineering
  - b. Production
  - c. Operation by customer
  - d. Maintenance, Service and Decommissioning

The standard is applicable to road vehicles, its systems, components, software and connection from vehicle to any external device/network. The purpose of ISO/SAE 21434 is to define a structured process to ensure cybersecurity is designed in upfront by following a structured process in order to reduce the potential for a successful attack by means of reducing the likelihood of losses.<sup>51</sup> The structured process will also react to the continually changing threat landscape and maintain consistency globally.

As can be seen in Appendix A.1, the ISO/SAE 21434 chapter 5 is about overall cybersecurity management. The overall cybersecurity management policy that will be created as part of this thesis will be ISO/SAE 21434 compliant, i.e. it will fulfill the existing requirements of the standard regarding overall cybersecurity management.

---

<sup>51</sup> Angela Barber (2018): Status of Work in Process on ISO/SAE 21434 Automotive Cybersecurity Standard

## 4. Research

### 4.1 Results of the quantitative and qualitative data from survey and moderation of a break-out session at a conference

In order to answer the research question(s), data is required, which can be qualitative or quantitative. Quantitative data is numerical, whereas qualitative data is not. Although many process improvement methods are quantitative in nature, this research will be mainly qualitative apart from the quantitative survey, which will be used to support the research goal and solution proposal. The sources of data, which is planned are primary (acquisition of data through inputs from the experts in the field and survey, which was conducted by SAE and Synopsys<sup>52</sup> with 593 participants, 47% of which is from OEMs, 36% from Tier1s and 12% from Tier2s) and secondary data, which is the data that contains all information that is written and made available through articles, internet, databases etc. Another source of data is the inputs of the experts in the field from the conference (i.e. OSS.5 Europe 2019) participated (for details see chapter 2.5).

#### 4.1.1 Quantitative Data from Survey

For the thesis, apart from the ISO/SAE 21434 standard, which is qualitative, mainly one quantitative source was utilized. As per quantitative data, a survey which was an independent study commissioned by SAE International and Synopsys was used. The number of participants, their current positions within their organizations, primary leaders the participants report to, spending of the companies in component security each year and details of the survey can be found in Appendix A.2. The most important outcomes of the quantitative survey are shown in Figures 16-18.<sup>52</sup>

---

<sup>52</sup> SAE, Synopsys, Ponemon Institute (2018): Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practises





Figure 16: Status of cybersecurity according to survey<sup>53</sup>

As can be seen in Figure 16, 84% of the participants of the survey have the belief that the practises in cybersecurity are not keeping pace with the evolving technology. 30% of the companies involved in the survey, does not even has an established cybersecurity program and team. In addition, 63% of the participants highlighted the fact that they do not test half of their hardware, software and other technologies for vulnerabilities.

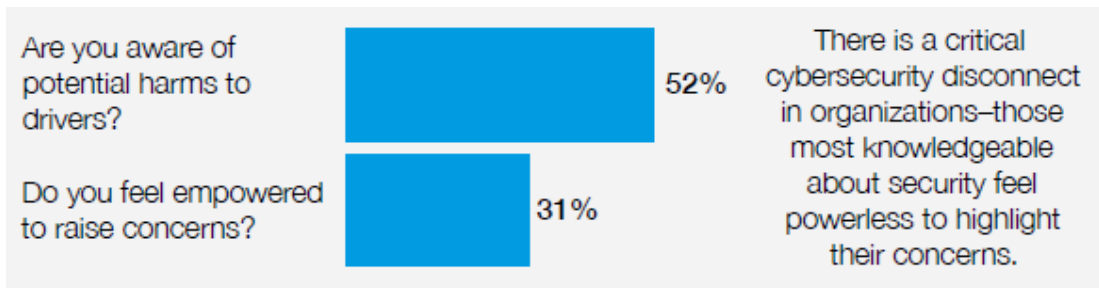


Figure 17: Awareness of potential cybersecurity harms and concerns voiced<sup>53</sup>

Figure 17 illustrates that, even though the participants are aware of the danger attached to cybersecurity, due to lack of communication channels, 69% do not feel empowered to raise their concerns. The questions that are addresses to the participants are listed below:

In your opinion, how likely is a malicious or proof-of-concept (i.e. security research) attack to occur against automotive software/technology/components developed or in use by your organization over the next 12 months?	• Very likely	27%
	• Likely	35%
	• Somewhat likely	23%
	• Not likely	15%

<sup>53</sup> SAE, Synopsys, Ponemon Institute (2018): Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practises

Which of the following best describes your organization's approach to product cybersecurity? Please select one choice only.	• Product cybersecurity is part of the traditional IT cybersecurity team (typically under a global CISO)	20%
	• Product cybersecurity is part of the functional safety team	17%
	• We have a centralized product cybersecurity team (i.e. center of excellence) that guides and supports multiple product development teams	10%
	• We have a decentralized product cybersecurity team, with cybersecurity experts attached to specific product development teams	23%
	• <b>We do not have an established product cybersecurity program or team</b>	<b>30%</b>
<hr/>		
Does your organization allocate enough resources (i.e. budget and human resources) to cybersecurity?	• Yes	49%
	• <b>No</b>	<b>51%</b>
<hr/>		
Does your organization have the necessary cybersecurity skills in product development?	• Yes	38%
	• <b>No</b>	<b>62%</b>
<hr/>		
Which technologies pose the greatest cybersecurity risk? Select all that apply.	• Infotainment systems	31%
	• Powertrain control units	46%
	• SOC system on chip-based components	44%
	• <b>Self-driving (autonomous) vehicles</b>	<b>58%</b>
	• Software-focused service provider (e.g. cloud, insurance provider, streaming service, etc.)	51%
	• <b>Telematics</b>	<b>60%</b>
	• Steering systems	46%
	• Electrification components	17%
	• Cameras	29%
• <b>RF technologies (e.g. Wi-Fi, Bluetooth, Hot spots)</b>	<b>63%</b>	
<hr/>		
What are the primary factors leading to vulnerabilities in the automotive technologies used by your organization?	• Accidental coding errors	56%
	• The use of insecure/outdated open source software components	40%
	• Malicious code injection	23%
	• Lack of internal policies or rules that clarify security requirements	26%
	• Lack of understanding/training on secure coding practices	60%
	• <b>Pressure to meet product deadlines</b>	<b>71%</b>
	• Lack of quality assurance and testing procedures	60%
	• Product development tools have inherent bugs	39%
	• Incorrect permissions	19%
• Back end systems	15%	

Figure 18: Overview of the answers provided to the survey questions<sup>54</sup>

<sup>54</sup> SAE, Synopsys, Ponemon Institute (2018): Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practises



Figure 18 demonstrates the fact that, 62% of the participants are convinced about the likelihood of a malicious attack (i.e. very likely + likely) to occur against their organization, although 30% did not establish a team yet to deal with it. 51% of the organizations do not allocate enough resources to cybersecurity; moreover, 62% believes that they do not have the necessary cybersecurity skills in product development. Furthermore, over 60% see the technology trends such as self-driving (autonomous driving), telematics and RF (radio frequency) technologies (e.g. Wi-Fi, Bluetooth, Hot spots) for posing greatest cybersecurity risks. Last but not least, among the primary factors leading to vulnerabilities in the automotive technologies, the factors that the participants have pointed out the most are pressure to meet product deadlines, lack of secure coding practises and lack of quality assurance and testing procedures.

The survey has shown that the automotive industry is relatively unaware of the potential harms of cybersecurity, organizations mostly do not have established procedures to voice concerns, some of the organizations have even not established cybersecurity teams and programs and a few companies did not allocate enough resources and raised cybersecurity skills within their teams, which is necessary for product development. Moreover, the future trends in the automotive industry will require more cybersecurity as they pose higher risk and finally most of the factors that lead to the vulnerabilities are project independent (e.g. pressure to meet deadlines, secure coding guidelines etc.). The survey showed that the creation of an overall cybersecurity management policy will address all the points that are reflected in the survey. It will deal with the most important contributors of the potential cybersecurity risks and by applying the overall cybersecurity management policy, such risks could be mitigated.

#### **4.1.2 Qualitative Data from the Moderation of a Break-Out Session at a Conference**

The author participated between 25-27 September 2019 at the OSS.5 Europe (Operational Safe Systems) Conference, which was conducted in Berlin. On 27th September, between 11:40-15:10pm, the author moderated a break-out session (so called the Cybersecurity World Café) title of which was “The Golden Triangle between Cybersecurity, ISO 26262, and ISO/PAS 21448 for Highly Automated Vehicles”.

World Café sessions are designed to help the participants, who are experts from the automotive industry working for OEMs and Tier1-n, as well as academic and other stakeholders, to discuss with colleagues and peers about similar issues and challenges that everyone is facing in the industry. The conversation is moderated by an expert speaker. The aim of the session is to find real solutions to real world problems with the 5 rounds of this session. Throughout the sessions, the experts are sharing and deepening their knowledge. “Based on the theory of the power of

collective knowledge, participants are brought together to share challenges and jointly gain new perspectives and develop solutions. 12-15 participants are allocated to the offered World Café session tables. The host (moderator) of each round table welcomes the guests and briefly introduces controversies, challenging or domain related questions. After 30 to 35 minutes, participants move to the next table based on the assigned order on their name badge to enter into a new discussion. At the beginning of each new World Café round, the moderator gives a short conclusion of previously discussed aspects and questions emerged.<sup>55</sup> This allows continuous discussions. Hence, world café session enables fruitful discussions and a collection of expertise of the participants about the questions addressed.

In the Cybersecurity World Café, which was moderated by the author of this thesis, answers to the following questions were sought:

- What are the similarities between functional safety and cybersecurity development and how to best achieve synergies when it comes to highly automated vehicles?
- What are the main differences between functional safety and cybersecurity development?
- What are the main challenges and how can we address them?
- How do you interpret the readiness of suppliers for the new era in relation to supplier vulnerabilities?
- What is the effect of overall cybersecurity management process on project risks and costs? Can it reduce the risks and costs, if so how?

The answers were categorized under 3 categories, issues/facts, ideas/solutions and 3 key takeaways. The details of the cybersecurity world café session, the full version of the questions and answers provided can be found in Appendix A.3. Figure 19 illustrates the answers of the experts to the first question.

---

<sup>55</sup> OSS.5 Europe (2019)

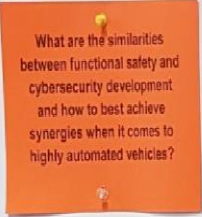
WORLD CAFÉ SESSION WC 4	ISSUES / FACTS	IDEAS & SOLUTIONS	3 KEY TAKE AWAYS
	<ul style="list-style-type: none"> <li>- safety criticality is input</li> <li>- risk oriented</li> <li>- process structure</li> <li>- testing</li> </ul>	<ul style="list-style-type: none"> <li><del>increase communication</del></li> <li>- knowledge/sharing vulnerabilities (could be regulated)</li> <li>- analyzing bidirectional impact</li> <li>- reusability of common analysis/methods/solutions</li> </ul>	<ul style="list-style-type: none"> <li>- risk oriented driven dev. process</li> <li>- dev. process (especially ISO/SAE 21434)</li> <li>- both no add on (start from design)</li> </ul>

Figure 19: Answers to the first question by the experts during the moderation of the break-out session at the OSS.5 Conference

When it comes to similarities between safety and cybersecurity development, according to the experts in the automotive industry, both functional safety and cybersecurity are risk oriented. Moreover, although the test methods and the processes itself are different, the V-model based development (see Appendix A.1) and testing process structure (i.e. comprehensive testing is essential for confidence in the final product) are same. Safety criticality is also part of cybersecurity, in other words, cybersecurity considers safety as well. In order to improve similarities between safety and cybersecurity, in the world café session, it was suggested to share the vulnerabilities and knowledge between the areas, analysing the bi-directional impact and reusability of common analysis, methods and solutions. Due to the fact that a system which is safety critical can not be safe without being secure, there is a mutual impact. The 3 takeaways from the first question were, both cybersecurity and functional safety are risk driven development processes, the cybersecurity development process ISO/SAE 21434 is also based on the safety development process structure of ISO 26262 (see Appendix A.1) and both safety and cybersecurity are not add-on features. One can not make a product safe or secure, the product shall be built safe and secure from the beginning (concept and design). In other words, a safe and secure product can be achieved by using a systematic development approach rather than reactive patching.

Figure 20 illustrates the answers of the experts to the second question.

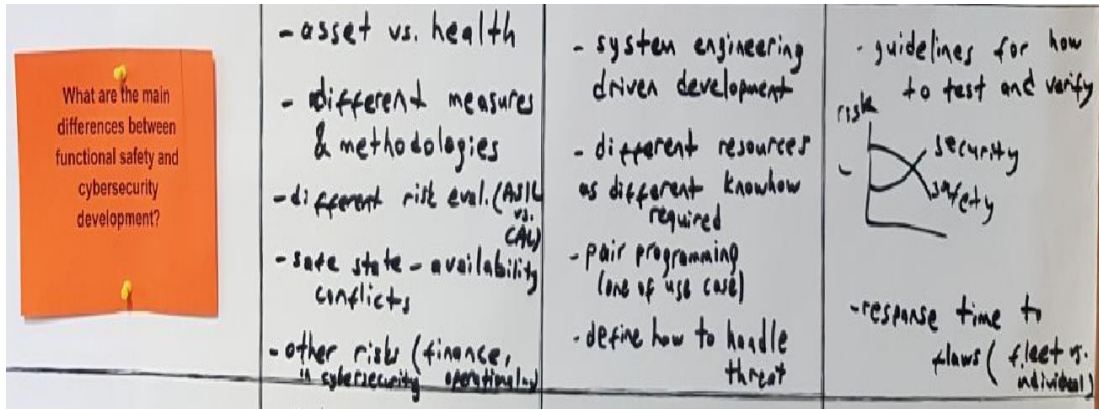


Figure 20: Answers to the second question by the experts during the moderation of the break-out session at the OSS.5 Conference

Regarding the differences between functional safety and cybersecurity development, although in functional safety the only asset to be protected is the health of the people involved, in cybersecurity there are assets, hence other risks, about finance, operation, privacy, safety, etc. As mentioned in the first question, the process and testing structure are same in both areas, yet still the methodologies and measures itself are different. For example, safety uses testing methods such as back to back testing, boundary testing, whereas in cybersecurity testing methods such as penetration testing and fuzz testing are used. In functional safety the risk integrity level is weighted with Automotive Safety Integrity Level (ASIL), on the other hand, in cybersecurity the risk integrity level is weighted with Cybersecurity Assurance Level (CAL). The risk in functional safety is rather unidimensional, whereas it is multidimensional in cybersecurity. The difference between the risk dimensions are shown in Figure 21.

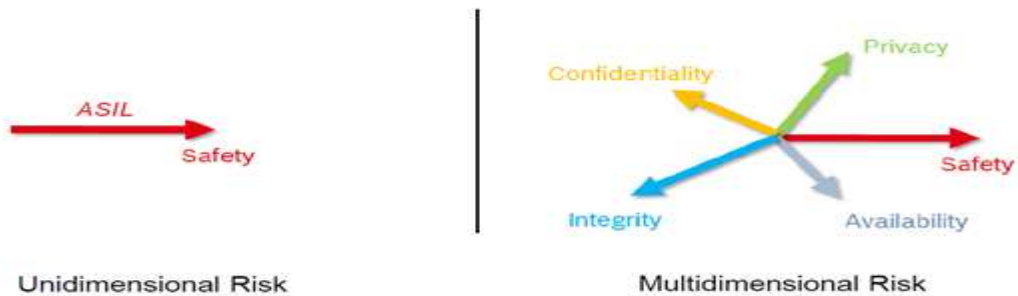


Figure 21: Difference between the functional safety and cybersecurity risk dimensions

Furthermore, there can be conflicts between safety and availability, i.e. when the vehicle goes into safe state, it could not be available anymore. For instance, in one case locking the door could be the safe state, where cybersecurity would require unlocking to provide availability. It is proposed to apply more system engineering driven development, that is start integrating functional safety and cybersecurity development at system level to improve cooperation between the fields. Since both areas require different know-how, i.e. one is very unlikely to be

a functional safety and cybersecurity expert, different resources are needed. Next point is, by means of pair programming safety and cybersecurity programmers can review and observe each other and give feedback to or learn from each other. Pair programming is an agile software development technique in which two programmers work together at one workstation. When one person writes the code, the other, the observer, reviews each line of the code as it is typed in. Both programmers switch roles frequently. Last but not least, if the incident response and risk/threat handling process is defined in advance, it can improve the collaboration between cybersecurity and safety; moreover, it can help the companies to be prepared beforehand. The 3 takeaways from the second question were: firstly, for both fields guidelines regarding testing and verification shall be created to deal with the different nature of development for functional safety and cybersecurity. Secondly, although the risk is decreasing in functional safety as the company develops more products, benefits from lessons learned and increase their know-how on the product manufactured; the risk tends to increase in cybersecurity as the number of hackers, their know-how, their equipment capabilities and number of incidents increase. Finally, although in safety one deals mainly with an individual vehicle unless there is a systematic failure, in cybersecurity the scope is the entire fleet, where the response time to flaws is different.

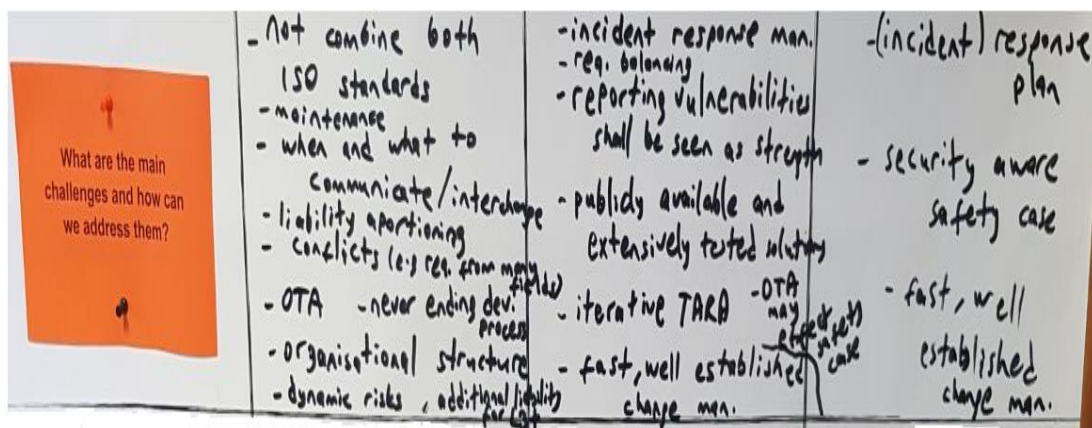


Figure 22: Answers to the third question by the experts during the moderation of the break-out session at the OSS.5 Conference

When it comes to main challenges and how they shall be addressed regarding functional safety and cybersecurity, it was highlighted that it is not possible to combine the existing functional safety (ISO 26262) and cybersecurity standards (ISO/SAE 21434). Especially for autonomous driving (level 3 and higher) maintenance and over the air update (OTA) are two big challenges. The reason is, with the increased use of connected and autonomous vehicles, the need for continuous updates to fix glitches becomes inevitable. However, there is a risk of overlooking the updates or that malicious actors infect the routine updates. Although, it is proposed to increase and improve communication between two areas as well as among companies, when and what to communicate and interchange still remains as a challenge. Another issue is the



liability apportioning as there are many stakeholders such as fleet operator/service providers, vehicle manufacturers (OEMs), technology companies, software manufacturers, governments/regulators, insurance companies, vehicle owner/operator, etc. and there will be additional liabilities as the level of autonomy increases. Yet another challenge is the never-ending development process. Due to the dynamic nature of the cybersecurity risks, it needs always iteration and regular updates, even after the product was brought into the market; therefore, it becomes a never-ending development. Furthermore, a decision cybersecurity organisations structure remains as an issue. Some solutions to deal with the challenges are:

- Creation of an incident response management process
- Balancing the requirements between functional safety and cybersecurity
- Reporting the vulnerabilities (it shall be seen as a strength)
- Increasing number of publicly available and extensively tested solutions
- Improving TARA (Threat Analysis and Risk Assessment) with iterations
- Creating a fast and well-established change management process
- Iterative improvement of the safety case via OTA (over the air update)

The 3 takeaways from the question are creation of an incident response plan in order to cope with the incidents in a more prepared way, creation of a security aware safety case, i.e. making cybersecurity part of the safety case and establishment of a sound change management process, which was also one of the solution proposals.

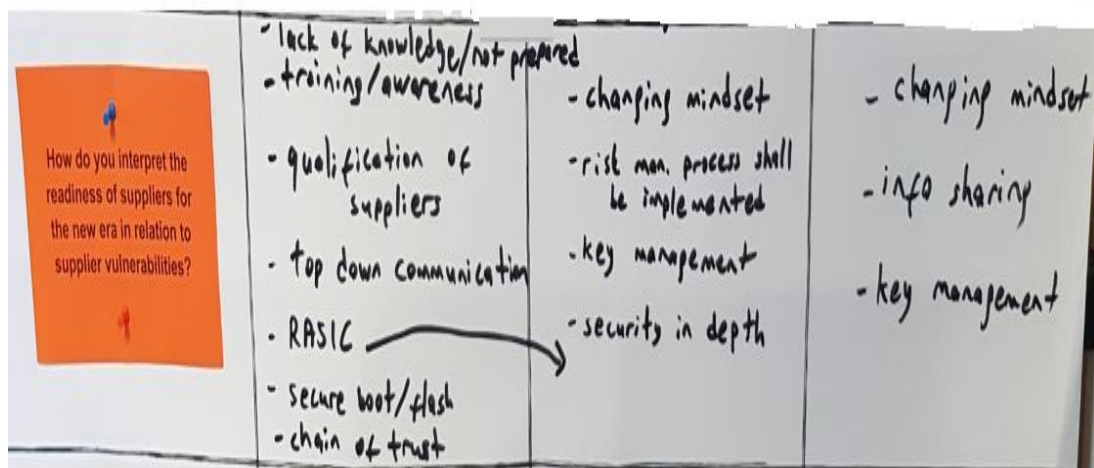


Figure 23: Answers to the fourth question by the experts during the moderation of the break-out session at the OSS.5 Conference

As also confirmed by the participants of the conference, the suppliers are lacking knowledge about cybersecurity and they are not prepared. The know-how shall be increased by trainings and enhancing awareness. Moreover, the OEMs or the supplier on the higher end of the supply

chain shall qualify their suppliers before doing business with them. The communication among the supply chain shall be top-down and a chain of trust shall be established. In addition, it is important to create a RASIC (Responsible, Accountable, Supporting, Informed and Consulted) between the parties to reduce vulnerabilities. A mindset change is needed in the industry, where a risk management process shall be implemented. Technological solutions such as key management, security in depth and secure booting and flashing can support when dealing with the vulnerabilities. For the question four, most of the solutions are also proposed as the key take away.

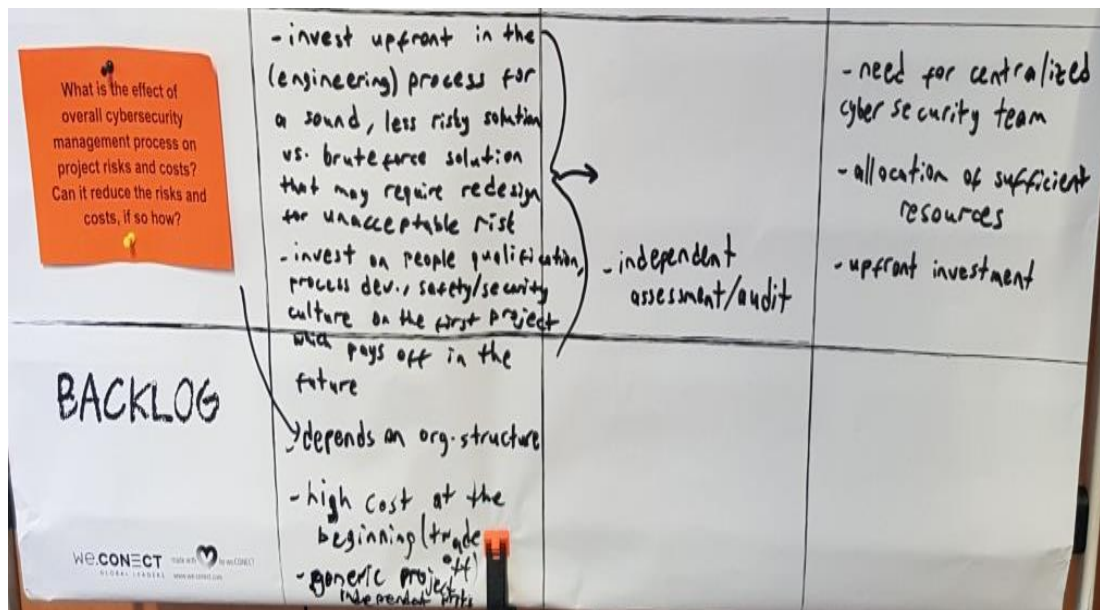


Figure 24: Answers to the fifth question by the experts during the moderation of the break-out session at the OSS.5 Conference

Regarding the question “What is the effect of overall cybersecurity management process on project risks and costs? Can it reduce the risks and costs, if so how?” the experts and academicians who participated the moderation of the author, which are roughly 50 people, highlighted the fact that cybersecurity development shall be an upfront investment. The participants agreed on the fact that, a sound overall cybersecurity management process is required. Such an overall cybersecurity management process will reduce the risks and is a lot more efficient when compared to a brute-force solution, which may require redesign for unacceptable risk. How to create such an overall cybersecurity management process is of course depending on the company and their organisational structure, but according to the participants there is no doubt about the necessity and importance of such a process. The fact that such an investment has high cost at the beginning, i.e. for the initial projects that is cybersecurity relevant was emphasized. Nevertheless, since the solution will be generic and project independent it will be a trade-off and will pay off in the long-run. It is also stressed that



independent audit/assessment shall be part of such an overall cybersecurity management process to minimize and mitigate the cybersecurity related project risks, hence costs. The 3 takeaways for the fifth question were: a centralized cybersecurity team is needed, which establishes an overall cybersecurity management process that is project and location independent, sufficient resources shall be allocated by the management in order to realize and implement the processes in the projects and finally this shall be an upfront investment that will pay off as the number of projects increases as well as it will mitigate the potential risks some of which would be impossible to quantify until a breach/incident happens.

In a nutshell, the moderation of the world café session at OSS.5 revealed the fact that for the experts and academicians in the automotive industry, there are synergies and differences between cybersecurity and functional safety which shall be taken into account; moreover, there are a lot of challenges regarding cybersecurity especially at the supplier level, and last but not least although it is an upfront investment, creation of an overall cybersecurity management policy/process will reduce the cybersecurity related potential project risks. Hence, the investment will pay off in long term.

In Chapter 5, the overall cybersecurity management policy will be defined whose framework is based on the ISO/SAE 21434 (see chapter 3.4). By applying this policy (or the adapted version for a specific firm), companies can reduce the cybersecurity related potential project risks as pointed out in the world café session at OSS.5.

## 5. The proposed overall cybersecurity management policy

In this thesis, the overall cybersecurity management policy was created by the author. For the validation of the research by credibility, the document was reviewed by cybersecurity experts of MPT (Magna Powertrain).

Each company, who would like to use this overall cybersecurity management policy shall adapt the content of this thesis for their company. It is important to highlight the fact that the process steps regarding how to fulfill the policies and the related inputs, outputs and responsibilities to fulfill the processes are excluded from the master thesis. Figure 25 represents the synopsis of the overall cybersecurity policy each part of which will be explained throughout chapter 5.

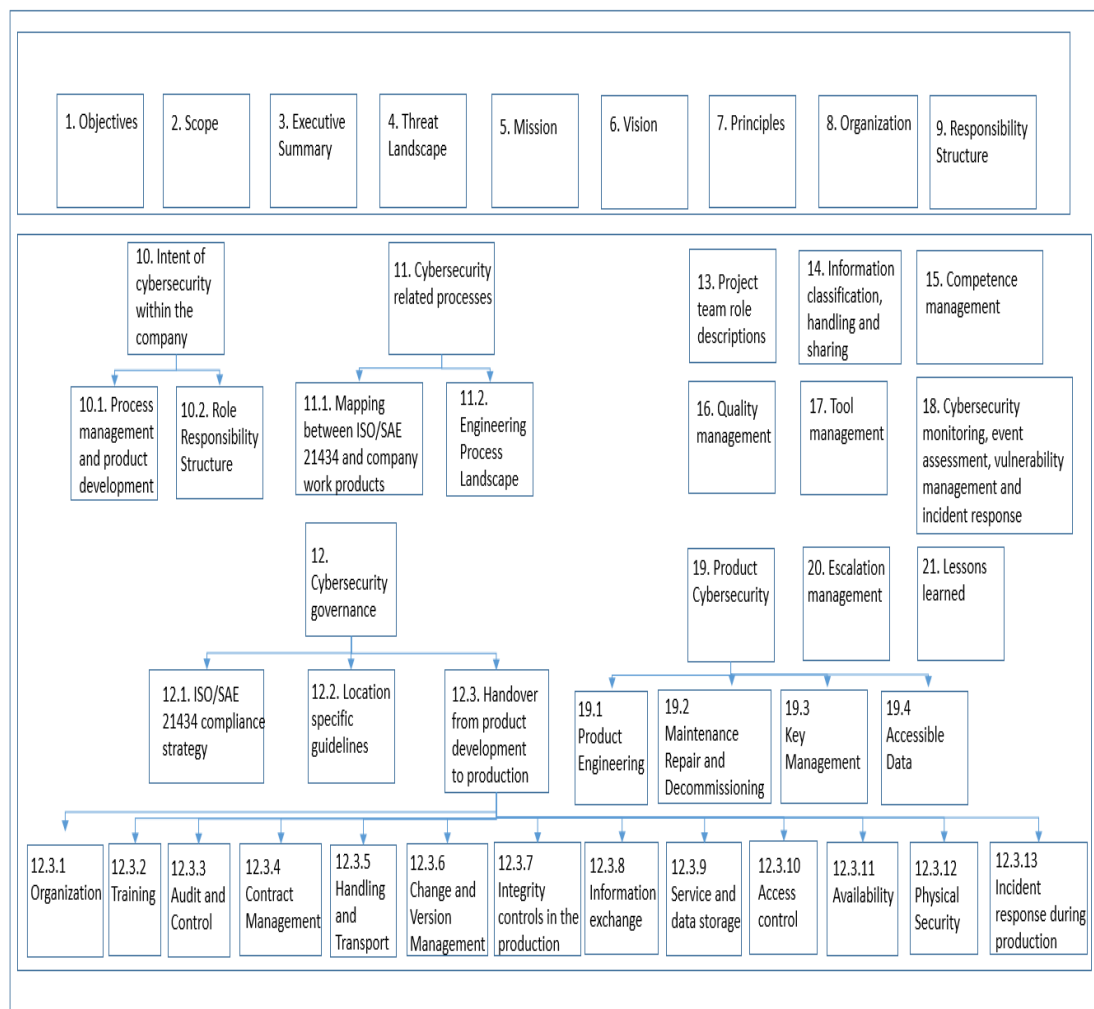


Figure 25: Synopsis of the overall cybersecurity policy

The automotive companies who are willing to create an overall cybersecurity policy are highly recommended to use the framework given in Figure 25, which is also in compliance with ISO/SAE 21434.

## 5.1 Objectives

This document explains the overall cybersecurity management policy and defines the company wide strategies necessary to achieve cybersecurity.

The objectives of this document are to ensure that the companies:<sup>56</sup>

- a) define the cybersecurity policy; the organizational strategy to achieve this policy; and the organization-specific rules and processes to implement the organizational cybersecurity strategy;
- b) assign the responsibilities and corresponding authorities that are required to perform the cybersecurity activities defined in this document;
- c) support the implementation of cybersecurity, including the provision of the resources needed for cybersecurity and the management of the interactions between cybersecurity processes and related processes;
- d) institute and maintains a cybersecurity culture, including competence management, awareness management and continuous improvement;
- e) perform an organisational cybersecurity audit;
- f) manage the sharing of cybersecurity information;
- g) institute and maintains management systems that support the cybersecurity activities;
- h) provide evidence that the tools used do not adversely affect cybersecurity

## 5.2 Scope

This standard is applicable development, production and/or all further activities related to cybersecurity. All specified requirements apply to sample, prototype, pre-series and series parts.

Implementation of an Information Security Management System (ISMS) as requested by TISAX (Trusted Information Security Assessment Exchange) is prerequisite for cybersecurity. The pre-requisite requirements of TISAX are not included within the scope of this document.

---

<sup>56</sup> ISO/SAE 21434 – Road vehicles – Cybersecurity engineering, draft for intended DIS

## 5.3 Executive Summary

As the cyber threat landscape has continued to evolve, cyber-attacks have become more and more advanced and have shifted their focus to target to corporations. Magna International is known as a leader in the automotive supplier space in the development of product solutions that improve the safety of transportation industry. This reputation must be protected as Magna is a target of malicious threat actors that seek to acquire our intellectual property, including our new engineering designs, product features, and knowledge-based engineering systems and processes.

In developing this overall cybersecurity strategy, the author gathered input from executive management across the organization, reviewed assessments results, and analysed industry trends to define a strategy that aligns to business objectives taking into consideration cybersecurity risks. MPT is dedicated continuing to be a leader in the automotive supplier space and differentiate its products based on their safety and cybersecurity.

## 5.4 Threat Landscape

The global threat landscape is ever-evolving. Cyber-attackers across the world are more brazen than ever before. More corporations are experiencing large and impactful cybersecurity breaches, seriously damaging their brand and marketplace confidence. People and products everywhere are increasingly connected through technology and the trend in the automotive industry continues to shift towards a reliance on mobile and data-enhanced technologies and systems.

## 5.5 Mission

Our cybersecurity mission at MPT is to manage cybersecurity risks to help increase the value of our products for our partners. In order to fulfill the cybersecurity mission, information security shall be ensured as prerequisite.

## 5.6 Vision

Our cybersecurity vision at MPT is to provide security leadership in order to embed security into our products allowing us to deliver more secure products and processes and support world class manufacturing.

## 5.7 Principles

To achieve our mission and vision we have outlined the following core principles for product security:

- Build and maintain an organization that holistically supports product security
- Embed security in the design and development of products
- Manage security risks throughout the product supply chain
- Strive for continuous improvement in product security
- Employ defense-in-depth mechanisms to preserve the availability, integrity and confidentiality in our products

## 5.8 Organization

To achieve our vision and mission we have develop an organization that embeds cybersecurity professionals at the right levels and creates a community for information sharing and governance across the enterprise.

## 5.9 RASIC within Organization Regarding Cybersecurity Activities

Activity	ISRC*	Corp Product Risk owner	Group/ Division Product Engineering	Group/ Division IT	MGIT
1 Strategy and Alignment	A	R	I	I	I
2 Governance and Organization / Policy	C	A	I	I	I
3 Architecture / Standards / Risk Mgmt	C	A	R	I	I
4 Threat Assessment / Requirements definition	S	A	R	C/S	C
5 Process Design and operational integration	C	A	R	C/S	C
6 Build & Test (Coding std's and test methods)	C	A	R	C/S	C
7 Deployment and Support (incl. training)	C	A	R	C/S	C
8 Incident Response	C	A	R	R	R
9 Metrics and Reporting	I	A	R	R	R

Figure 26. Cybersecurity RASIC Overview

Figure 26, illustrates a RASIC (Responsible, Accountable, Supporting, Informed and Consulted) suggestion for the cybersecurity activities where ISRC stands for Information Security Risk & Compliance, corp stands for corporate, MGIT stands for corporate IT, Mgmt stands for management and std stands for standards. As can be noticed, the definition of

strategy, governance and policy are within the responsibility of the corporate group, whereas defining the strategies such as the overall cybersecurity management relies within the responsibility of the group/division product engineering.

## 5.10 Intent of Cybersecurity

### 5.10.1 Split between process management and product development

A layered approach, which leverage between people, policy and technology shall be established. Cybersecurity yields the most effective defense, if it has an integrated framework, an overlapping strategy based on security technology, people, and processes.<sup>57</sup>

#### 5.10.1.1 People

Employees could be one of the main sources of threat for cybersecurity. Therefore, they shall be informed and trained as first line of defense. Mostly, cybercriminals specifically target employees as an attack vector (e.g. phishing emails) based on their lack of knowledge for security best practices. With this in mind, it's imperative for a company to conduct regular training sessions (for details see the training chapter) throughout the year to keep employees aware of potential scams and the ways they can make their organization vulnerable.<sup>57</sup>

Training programs will create a strong culture of cybersecurity in order to minimize threats. "Training employees to think and act with security in mind is the most underfunded activity in cybersecurity"<sup>58</sup>, although it is one of the most important ways of reducing the risks. Furthermore, the employees shall be informed about the following points:<sup>57</sup>

- Creating strong passwords that are unique to each account and not reused
- Ensuring personal and work passwords are separate
- Not opening or clicking links in suspicious emails or those from unfamiliar senders
- Ensuring applications and operating systems are regularly updated as soon as patches/updates are released
- Not installing any unknown, outside software, as they can open security vulnerabilities in the network.

---

<sup>57</sup> Renee Tarun (2018): A Layered Approach to Cybersecurity: People, Processes, and Technology

<sup>58</sup> Taryn Oesch (2019): Building a "Human Firewall": Cybersecurity Awareness Training That Works

- Immediately reporting any unusual behaviour or something strange happening on their computers.

Another way to improve cybersecurity at the employee level is with access management policies (for details see the access control chapter) such as the principle of least privilege, which provides a person with access to data only if it is necessary to do their job – thereby reducing the exposure and consequences of a breach.<sup>59</sup>

### **5.10.1.2 Policy**

The policy layer of cybersecurity ensures that a company has strategies in place to proactively prevent and respond quickly and effectively in case of a cybersecurity incident.<sup>60</sup> This is ensured by means of a cyber incident response plan (for details see the incident response management chapter).

Moreover, a threat analysis and risk assessment (TARA) process shall be defined in order to identify threat scenarios that can potentially compromise the cybersecurity properties of the identified assets.

In addition, for effective cybersecurity, assets shall be prioritized based on which are most business critical and would have the greatest impact on the business if breached.<sup>59</sup> The IT and cybersecurity teams shall know all the (prioritized) assets to develop policies and deploy strategies (e.g. network segmentation) and minimize consequences. This thesis is focusing on the people and policy layers.

### **5.10.1.3 Technology**

Once the necessary people and policy layers are established as prerequisite, the technology layer shall use the existing protection measures in cybersecurity such as network segmentation, cryptography, intelligence (e.g. plausibility), defense in depth and design with security in mind to achieve cybersecurity. Possible cybersecurity measures that can be applied at the different sections of vehicle and the associated security concepts are illustrated in Figure 27 and 28, respectively.

---

<sup>59</sup> Renee Tarun (2018): A Layered Approach to Cybersecurity: People, Processes, and Technology

<sup>60</sup> Akshay Bhargava: Cyber Risk: A Boardroom Priority



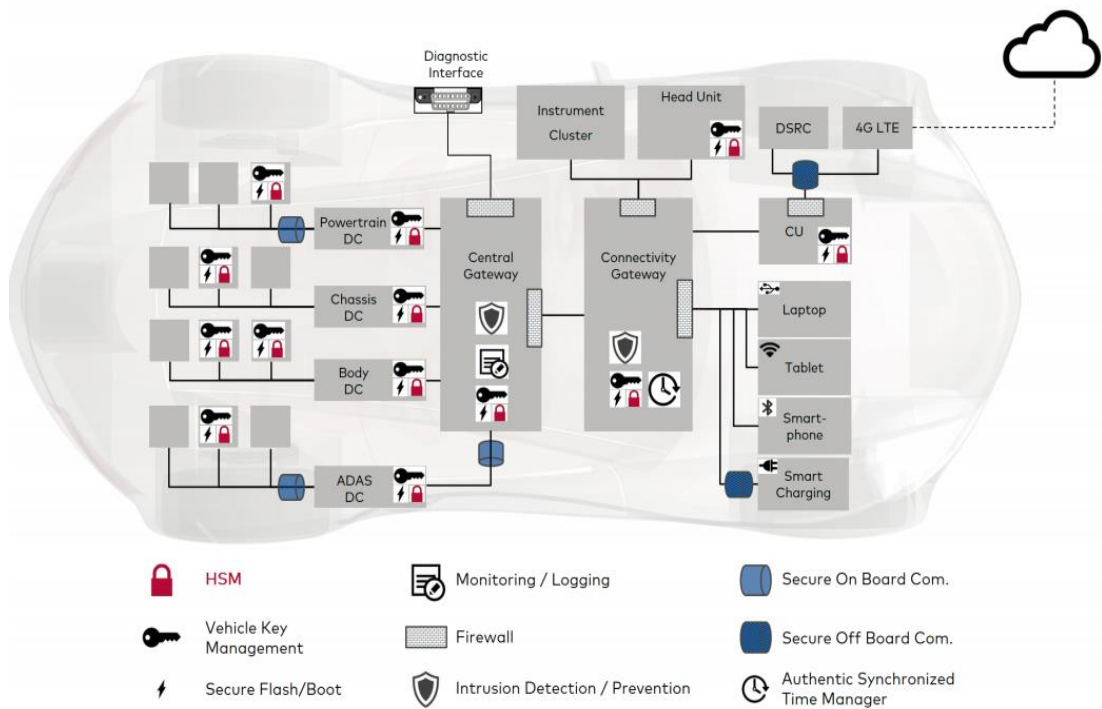


Figure 27. Cybersecurity measures that can be applied at different sections of the vehicle<sup>61</sup>

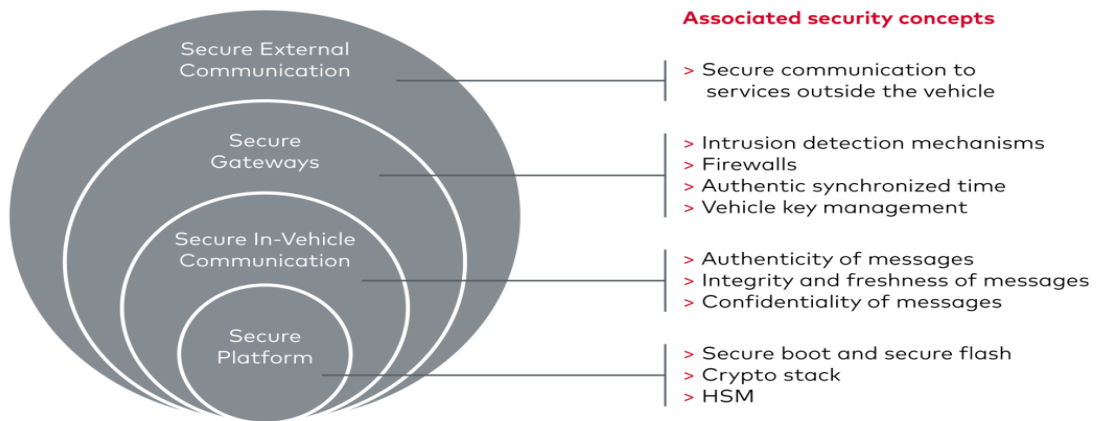


Figure 28. Layered security concept with the associated security concepts<sup>61</sup>

### 5.10.2 Role responsibility structure

In order to fulfill the objectives (see chapter 5.1) of the overall cybersecurity management policy, it is required to define the resources and roles to assign the responsibilities and corresponding authorities that are required to perform the cybersecurity activities. This chapter aims at defining and explaining the cybersecurity related roles which were defined together with the experts at MPT based on state of the art, lessons learned and gathered experiences.

<sup>61</sup> Infineon (2018): Cybersecurity Mechanism for Connected Vehicles

### **5.10.2.1 Product Cybersecurity Manager**

#### **Responsibilities:**

- Lead the product cybersecurity development according to ISO/SAE 21434
- Ensure the development team has a plan to achieve cybersecurity and provides arguments why the product achieves cybersecurity according to state of the art (e.g. ISO/SAE 21434).
- Provide and deny cybersecurity approval for system releases based on fulfillment of cybersecurity activities
- Report product security concerns to Embedded Product Security Manager

#### **Main activities:**

#### **Scope in Projects:**

- Plan and track all cybersecurity activities and provide guidance to the project team to achieve the cyber security plan during the whole cybersecurity lifecycle
- Strengthen the cybersecurity culture of the organization and improve project efficiency
- Define the distributed development of a cybersecurity system to ensure agreement among parties
- Determine the cybersecurity relevance of a project based on available information
- Align cybersecurity activities and be the point of contact with the customer, the supplier(s), the project manager, customer quality (regarding incidents) and the Functional Safety Manager
- Align cybersecurity goals and requirements with OEM and suppliers
- Support the serial production process engineering, purchasing and quality during the production, operation and maintenance focusing on the cybersecurity of the product.
- Ensure handover of cybersecurity responsibility during production, operation and maintenance
- Document the process and product arguments for achievement of cybersecurity (e.g. assessment/audits, verification of cybersecurity concept, cybersecurity case, etc.)
- Assess and support field and plant claims regarding cybersecurity issues
- Support the resolution of the incidents
- Initiate cybersecurity escalation based on the identified cybersecurity risks

### **Overall cybersecurity management activities:**

- Supporting alignment of cybersecurity over different engineering sites and plants, and over different projects
- Managing incident response process and information exchange
- Planning and organizing cybersecurity trainings

### **Skills:**

- Basic knowledge of mechatronic systems
- Understanding of cryptographic principles
- Knowledge of security standards (e.g. ISO 27001, ISO 21434, IEC 62443 ...)
- Knowledge of commonly used security architectures
- Knowledge of safety standards (e.g. ISO 26262)
- Knowledge of the analysis techniques (e.g. FMEA, FTA, FMEDA, ETA, HAZOP)
- Requirement engineering skills

### **5.10.2.2 Product Cybersecurity Engineer**

#### **Responsibilities:**

- Representation of the cybersecurity engineering within the project team, i.e. working with the development team to create a product which achieves cybersecurity according to state of the art (e.g. ISO/SAE 21434)
- Perform the project related cybersecurity activities
- Escalate issues to cybersecurity manager or project manager if necessary

#### **Main activities:**

- Analyze and evaluate specific customer product security requirements
- Lead/support the cybersecurity concept development from the product security perspective
- Lead and moderate cybersecurity analyses on system, subsystem, HW and software (SW) level
- Lead and moderate threat and risk analysis
- Define cybersecurity goals/concept
- Provide product cybersecurity methodical approach, standards

- Support the development on the System, SW, hardware (HW) level (including specifications, test reports, DVP (design verification plan), drawings, FMEAs/FMEDAs, FTAs) from the product cybersecurity perspective
- Support production and maintenance from the product cybersecurity perspective
- Support questions regarding normative issues (ISO/SAE 21434)
- Execute or initiate and check additional product cybersecurity processes like qualification of tools, qualification of hardware components, interfacing within distributed developments
- Support SQD (Supplier Quality Development) when monitoring suppliers product cybersecurity work
- Analysis of cybersecurity events
- Support the resolution of incidents
- Support assessment/audits
- Lead cybersecurity reviews with customer and suppliers

#### **Skills:**

- Knowledge of mechatronic systems
- Thorough knowledge of the programming language C
- Knowledge of programming in (e.g. in programming languages such as C#, Java, Python)
- Knowledge of cryptographic principles
- Thorough knowledge of most important attack vectors
- Knowledge of security standards (e.g. IEC 27001, ISO 21434, IEC 62443 ...)
- Knowledge Common Vulnerability Scoring System (CVSS) and different methods for Threat Assessment and Risk Analysis
- Basic knowledge of safety standards (e.g. IEC 61508, ISO 26262, ...)
- Knowledge of commonly used security architectures
- Knowledge of the analysis techniques (e.g. FMEA, FTA, FMEDA, ETA, HAZOP)
- Requirement engineering skills

### **5.10.2.3 Subject Matter Expert for Cybersecurity**

The subject matter expert (SME) is the person who provides the knowledge and expertise for cybersecurity in a project/program. Furthermore, the role responsibilities, main activities and skills definitions for SME Cybersecurity are also based on job descriptions that are available in career websites such as LinkedIn, Indeed, etc.

#### **Responsibilities:<sup>62</sup>**

- Ensure the facts and details are correct so that the project's/program's deliverable(s) meet the needs of the stakeholders, legislation, policies, standards, and best practices for cybersecurity
- Advise based on broad based technical background in IT operations and cybersecurity
- Be the organizational ambassador for cybersecurity to apply his/her expertise to support an organization's vision and strategic direction
- Provide SME Support for Strategic Engagements
- Provide thought leadership by engaging in papers, articles, podcasts, and participating in key industry events, seminars and conferences

#### **Main Activities:**

- Work closely with the engineering team to keep them abreast of industry trends and customer requirements.
- Leverage industry knowledge and experience to define and guide the customer requirements and configuration of solutions.
- Support definition of procedures or standards
- Provide expert guidance and directions and recommendations for procedural improvements
- Understand the language/terms/jargon in his/her area of expertise
- Act as the "go to" person within a department or function for questions and problems within cybersecurity
- Explain cybersecurity clearly to others

---

<sup>62</sup> Magic: Subject Matter Expert (SME) Roles and Responsibilities

## **Skills:**

- Years of hands on experience with cybersecurity
- Knowledge of mechatronic systems
- Thorough knowledge of the programming language C
- Knowledge of programming in (e.g. in programming languages such as C#, Java, Python)
- Thorough knowledge of cryptographic principles
- Thorough knowledge of most important attack vectors
- Knowledge of security standards (e.g. IEC 27001, ISO 21434, IEC 62443 ...)
- Knowledge CVSS and different methods for Threat Assessment and Risk Analysis
- Basic knowledge of safety standards (e.g. IEC 61508, ISO 26262, ...)
- Thorough knowledge of commonly used security architectures
- Knowledge of the analysis techniques (e.g. FMEA, FTA, FMEDA, ETA, HAZOP)
- Requirement engineering skills

### ***5.10.2.4 Product Cybersecurity Responsible***

## **Responsibilities:**

- Ensure that the procedures & related processes are implemented, executed and checked regularly and frequently for compliance.
- Ensure that evidence of employees being trained and its training requirements per role exists.
- Ensure that the associated requirements of this standard are communicated, abode by and reported on.
- Create, maintain, and communicate audit schedule for the related plant/location/product.
- Ensure compliance in the daily handling of cybersecurity related products (including the interface to the customer with regard to all program/product relevant questions, issues).
- Ensure the necessary security zones are created for all cybersecurity relevant areas.
- Coordinate with human resources and the facility management to ensure the necessary surveillance, secured doors and security resources are in place.
- Define and document the associated processes regarding approval, checks and deletion of the access rights.

Moreover, all the remaining roles that are necessary for cybersecurity development (i.e. roles related to System, HW, SW development, etc.), objective, main activities, skills, responsibilities of the roles, the process steps each role is responsible/accountable/supporting and the corresponding work products are shown directly in the engineering process of MPT Driveline System.

## 5.11 Cybersecurity related processes at MPT

### 5.11.1 Mapping between ISO/SAE 21434 and Company (MPT) Work Products

In this part the ISO/SAE 21434 work products shall be mapped with the corresponding company work products. In the current version of the ISO/SAE 21434 standard, there are 44 work products. An example of work product mapping (a list for 9 work products, the full version will be part of the cybersecurity plan) is shown in Figure 29 to explain the idea behind, where PE stands for the engineering process of MPT.

ID	Work Products	Planned MPT Workproduct	Responsible Role
	Overall Cybersecurity Management		
1	Cybersecurity policy, strategy, rules and processes	Overall Cybersecurity Management Document	Overall Cybersecurity Manager Global Process Owners
2	Evidence of competence management, awareness management, continuous improvement	Overall Cybersecurity Management Document	Overall Cybersecurity Manager
3	Organizational cybersecurity audit report	PE.49_07 Cyber Security Audit/Assessment Report	Cybersecurity Manager
4	Evidence of the organization's management systems	Overall Cybersecurity Management Document	Overall Cybersecurity Manager
5	Evidence of tool management	Guidelines	PE23 Owner
	Project Dependent Cybersecurity Management		
6	Cybersecurity Plan	PE.49_04 Cyber Security Plan	Cybersecurity Manager
7	Cybersecurity Case	PE.49_05 Cyber Security Case	Cybersecurity Engineer
8	Cybersecurity Assessment Report	PE.49_07 Cyber Security Audit/Assessment Report	Cybersecurity Manager
9	Release for post development	PE.44_01 Technical System Release	Cybersecurity Manager

Figure 29. Mapping between ISO/SAE 21434 and MPT Work products

### 5.11.2 Engineering Process Landscapes

In this chapter, the engineering process of the company shall be illustrated.

## 5.12 Cybersecurity Governance Proposal

According to ISO/SAE 21434, organizations shall define a cybersecurity policy (including acknowledgement of road vehicle cybersecurity risks and commitment of the executive management to manage the corresponding risk) and shall establish and maintain organizational specific-rules and processes (i.e. process definition, technical rules, guidelines, methods and templates) to fulfill the requirements of ISO/SAE 21434 and the execution of the



corresponding activities. These rules and processes cover concept, development, production, operation, maintenance, and decommissioning, including cybersecurity risk management, information sharing, vulnerability disclosure, cybersecurity monitoring, incident response and triggers. This master thesis is aiming at creation of an overall cybersecurity policy.

The cybersecurity governance (for explanations see chapter 5.1 – 5.10) proposal is illustrated in Figure 30.



Figure 30. Overview of the cybersecurity governance proposal

Moreover, the organizations shall identify disciplines related to, or interacting with, cybersecurity and establish and maintain communication channels between those disciplines (e.g. IT security, functional safety, data protection and privacy). By means of the communication channels, exchange of relevant information shall also be coordinated. Relevant information includes threat scenarios and hazard information, cybersecurity goals and safety goals, or where cybersecurity requirement might compete or conflict with a safety requirement.

The interaction and communication channels between functional safety and cybersecurity are illustrated in Appendix A.4.

### 5.12.1 ISO/SAE 21434 Compliance Strategy

It is important for each automotive company to define their strategy about how they are planning to be ISO/SAE 21434 compliant. Especially, for bigger scale companies, location and project

specific solutions are needed. Figure 31, presents the high level strategy of MPT about how to be ISO/SAE 21434 compliance and how to enable flexibility for the development at different locations and products.

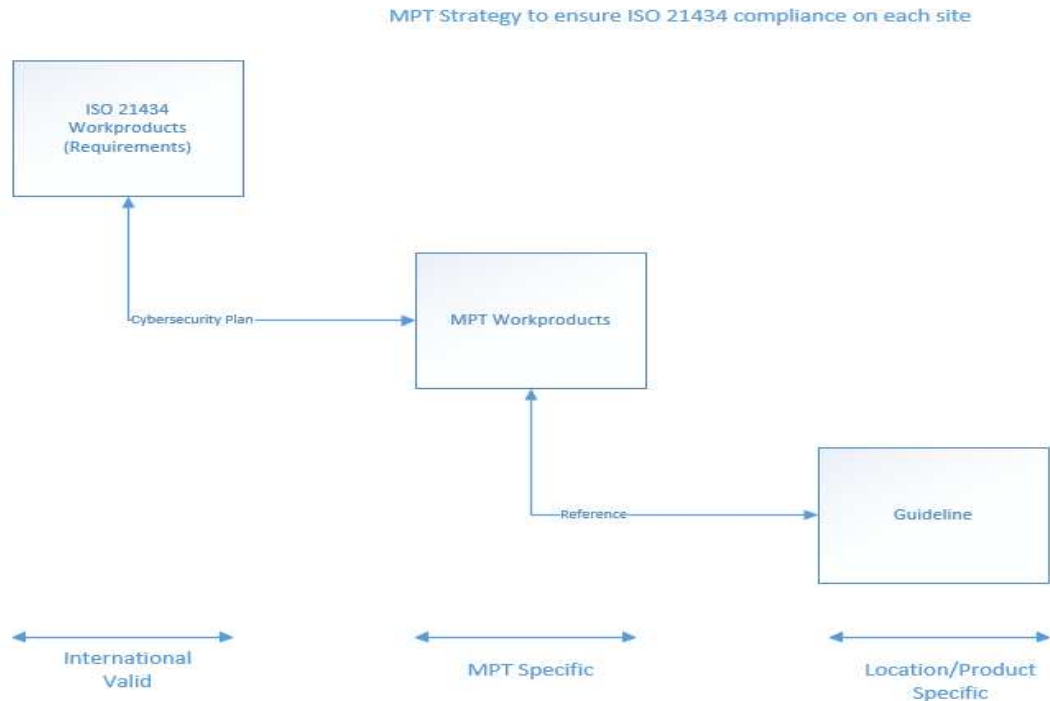


Figure 31. MPT High Level ISO/SAE 21434 Compliance Strategy

Cybersecurity Plan:

- A generic template shall be created, which illustrates the Cybersecurity Lifecycle Process within the project, where the individual phases of the Cybersecurity Lifecycle Process are shown
- Generic template shall be re-used by each cybersecurity critical project

There shall be two kind of guidelines:

- A guideline for explaining the work product (WP), which is part of the WP itself (the template itself) and
- A guideline for explaining the relation between different WPs and processes

### 5.12.2 Location Specific Guidelines

Due to the fact that companies like MPT are composed of several business units and locations, there shall be location specific guidelines in order to explain how each process and its

corresponding steps are interpreted at a specific location. The guidelines shall be stored in the corresponding process folder of the business unit.

### **5.12.3 Cybersecurity Handover from Product Development to Production**

#### **Objective:**

Ensure protection of assets by product cybersecurity handover requirements from product development to production.

#### **Target group:**

Production personnel involved in cybersecurity relevant activities.

#### **Target product:**

Scope is cybersecurity relevant products.

#### **5.12.3.1 Organization**

- A product cybersecurity responsible shall be nominated for every production plant.
- An incident response product cybersecurity responsible and a deputy shall be nominated for every production plant.
- Assigned responsibilities shall be documented.
- The protection of the assets shall be specified, ensured and monitored along the entire value chain.
- Each person involved in cybersecurity relevant activities shall only be provided with and access the information necessary for their jobs, and to complete their tasks and activities (“need to know” principle).

#### **5.12.3.2 Training**

- All personnel involved in product development, production and IT shall be trained appropriately and regularly (at least every two years).
- Evidence of the trainings shall be documented.
- All core team member involved in product cybersecurity relevant activities shall complete a dedicated awareness training in relation to the protection of product cybersecurity assets.
  - NOTE: Training includes but not limited to:

- Processes
- Best practices
- Work products
- Information sharing policy
- Assets, threats, risks, attacks
- Vulnerability & incident handling

### **5.12.3.3 Audit and Control**

- Each affected entity (i.e. locations where cybersecurity relevant activities take place) shall perform yearly audits to ensure compliance with the related requirements.
- Each affected entity shall verify the specified requirements.
  - NOTE: Methods of verification include for example:
    - Penetration test
    - Manual inspection
    - Configuration check
    - Unannounced audits
- All confidentiality agreements and processes relevant to product cybersecurity shall be checked and documented at least yearly.
- The descriptions in the order of installation and the physical security shall be reviewed in relation to product cybersecurity vulnerabilities and process weaknesses at least yearly.
- Cybersecurity related third party suppliers (sub-contractors including transportation companies) shall be audited regularly as defined by suitably qualified personnel to ensure compliance to the customer (OEM) and the company cybersecurity requirements. The audit results need to be verified and appropriate measures shall be implemented by the third-party supplier.

### **5.12.3.4 Contract Management**

- All personnel involved in product cybersecurity relevant activities shall sign a non-disclosure agreement (NDA).
- All suppliers and business partners involved in product cybersecurity relevant activities shall sign a non-disclosure agreement (NDA).
- All suppliers and business partners involved in product cybersecurity shall provide complete documentation of product access interfaces including its authentication information.

- All suppliers and business partners involved shall comply with the guidelines of the process which are described. The sub-supplier needs to fulfill the defined security measures.
- All suppliers and business partners involved in product cybersecurity shall sign a contract acknowledging the non-existence of backdoors in finalized products which is not stated.

#### **5.12.3.5 Handling and Transport**

- The material flow of all components relevant to product cybersecurity relevant systems shall be described in a detailed graphical overview of the physical implemented security zones.
  - NOTE: Material flow includes but not limited to:
    - Microcontroller
    - Transmission control units (TCUs), Electronic control units (ECUs)
    - Powertrain components
    - Finalized products
- The exchange and storage of product cybersecurity relevant information from the product development to the finalized system shall be described.
- The generation, exchange and storage of product cybersecurity relevant cryptographic material shall be described.
- Prompt detection of the discrepancies and the corresponding countermeasure/improvement implementation shall be ensured, which applies to all construction conditions (e.g. parts to be scrapped)
- All product cybersecurity relevant components shall be traceable.
  - NOTE: Product cybersecurity relevant components include for example:
    - TCU
    - Inverter
    - Wiring harness
    - Finalized product
    - Mobile electronic storage devices (e.g. USB-sticks, hard drives)
- All internal and external hand-over points shall be defined, documented, recorded (barcode/DMC (Data matrix code) scanners and software can be used to automate the processes) and agreed contractually with the customer and/or the designated transport carrier.
- All product cybersecurity relevant components shall be tracked up to the customer.

- Loss of product cybersecurity relevant components shall be communicated to the product cybersecurity responsible.
- Cybersecurity relevant components/products shall be packaged and transported securely within the location storage facilities. In case of automated internal transportation, additional security means such as physically covered conveyor belts, lockable units, lockable pallets etc. can be applied.
- Anti-theft protected transport shall be ensured (secure packaging) for the transmission unit/ID sender with transponder (model-dependent component of the locking set).

#### **5.12.3.6 Change and Version Management**

- All product cybersecurity relevant components and software revisions in production shall be documented.
- A management and tracking system shall be implemented in production to prevent malicious alteration and systematically update product cybersecurity relevant components.
- The compliance and impact to the requirements shall be reviewed in case of changes in product cybersecurity relevant production processes.

#### **5.12.3.7 Integrity Controls in the Production**

- The integrity of product firmware shall be verified in production.
  - NOTE: Possible solution: Digital signature check of the finalized system - product development has to provide a corresponding mechanism and documentation (according to product cybersecurity best practice).
- The integrity of cryptographic material and cybersecurity functionality shall be ensured and verified in production.
  - NOTE: Methods of verification include for example:
    - Check of public keys by secure diagnostic unlock test via backend.

#### **5.12.3.8 Information Exchange**

- All product cybersecurity relevant exchange of information between the company (also internal), customer, suppliers and business partners shall be encrypted.

#### **5.12.3.9 Server and Data Storage**

- Product cybersecurity relevant information shall be classified.

- Product cybersecurity relevant information required for production shall be stored and handled in an information management system.
  - NOTE: Product cybersecurity relevant information required for production include for example:
    - Cryptographic material
    - Bootloader software
    - Firmware
    - Calibration files
    - Access lists
    - Versioning information
    - Update information
- The information management system shall be hardened according to IT state of the art technology (e.g. availability, confidentiality and integrity).
- All IT systems that handle product cybersecurity relevant cryptographic material shall be hardened in compliance to IT state of the art technology.
  - NOTE: IT systems include for example:
    - Servers
    - Flash station
    - Exchange portals
    - Information management system
    - Production workstations
    - Mobile electronic storage devices (e.g. USB-sticks, hard drives etc.)
- IT systems that handle product cybersecurity relevant information shall be classified.
- In case a virtual server is used, those virtual environments that are hosted on the same physical server shall be comparable in terms of security requirements and their technical implementation.

#### **5.12.3.10 Access Control**

- Access control according to the principle of least privilege shall be applied to all IT systems that handle product cybersecurity relevant information.
  - NOTE: Principle of least privilege includes for example:
    - Access only with a need to know
    - Withdrawal of access rights upon expire of need to know
    - Technical abstraction of access privileges (e.g. administration rights restriction)



- All required and implemented access control rights (approval, checks and deletion) shall be maintained and checked regularly by a nominated department/person.
- Access rights of the persons who no longer requires access in order to complete their tasks (e.g. because they left the company) shall be immediately withdrawn.
- Additional security requirements and measures regarding employees who are directly involved and have access to cybersecurity related components and/or information shall be defined and agreed with Human Resources. Such measures include additional background check (as much as legally permitted), minimum employment times, dedicated confidentiality agreements etc.
- The usage of physical access control systems shall be documented in a traceable manner and the traceability of the access needs to be guaranteed.
- Access to product cybersecurity relevant cryptographic material (including computer workstations) shall be protected by two-factor authentication.
  - NOTE: For example two factor authentication can be:
    - Password & hardware token (e.g. smartcard)
- Access to hardware tokens shall be managed and tracked.
- Admittance and access to the secure storage area shall be documented comprehensibly.

#### **5.12.3.11 Availability**

- Retention and usability of product cybersecurity relevant information and in particular cryptographic material shall be ensured over product lifetime.
- The availability of production relevant and cybersecurity related infrastructure shall be ensured.
  - NOTE: Availability can be ensured by for example:
    - Redundant infrastructure

#### **5.12.3.12 Physical Security**

- Access to all areas involved in handling product cybersecurity relevant components, information and activities shall only be permitted to persons who need access to that specific area.
- Access to product cybersecurity relevant IT systems in the plant shall be secured by an additional physical security perimeter.

- A production site plan illustrating the security perimeters for all product cybersecurity relevant areas including infrastructure, activities and access interfaces shall be created and regularly audited.
  - NOTE: Infrastructure and activities include for example:
    - Servers
    - Network segmentation
    - Flash process
    - Closing cabinet
- The penetration of product cybersecurity relevant areas by devices, which are not part of the production process, shall be prevented.
  - NOTE: Not part of the production process devices include for example:
    - Sniffing devices (e.g. key loggers)
    - Mobile electronic storage devices (e.g. USB-sticks, hard drives etc.)
    - Network devices (e.g. wireless access points, routers, modems, switches)
- The introduction of devices and personnel for intended changes within product cybersecurity relevant areas and activities shall be approved.

#### **5.12.3.13 Incident Response during Production**

- The incident response product cybersecurity responsible for each plant shall collect and forward relevant product cybersecurity information from internal sources in the plant organization to the product cybersecurity manager regularly.
  - NOTE: Risk evaluation and event assessment is performed by the product cybersecurity manager.
- If the organization decides to apply an incident response, the plant responsible shall participate in the response team and coordinate necessary actions in the plant.
  - NOTE: Required actions in the plant include for example:
    - Update rollout
    - Plant internal communication

#### **5.13 Project Team Role Descriptions**

- 1) Describe method for naming roles and responsibilities
- 2) Describe method for naming people associated with each role
- 3) Describe how each person can find the deliverables for which they are responsible
- 4) Describe how each person can find their deliverables within the project plan

## 5.14 Information Classification, Handling and Sharing

According to ISO/SAE 21434, organizations shall define the circumstances under which sharing is required, permitted and prohibited, within and outside of the organisation. In order to fulfill this purpose, Magna has established rules and procedures for handling and classifying information.

Magna's and its customer's information must be secured based on 3 key objectives as defined in Magna's Information Security Policy: confidentiality, integrity and availability. For each objective, three levels of potential impact on the business (unauthorized disclosure, modification, and disruption) must be assessed as either low, moderate, or high. For the objective "confidentiality", an additional naming scheme should be used where an "Internal" classification means there is low potential impact, "Confidential" means moderate impact and "Strictly Confidential" means high impact.

### 5.14.1 Marking of Information

All Information (Confidential and Strictly Confidential) must be labelled or marked with the appropriate information classification designation, in accordance with the Magna Information Security Policy. All manifestations of the information must include such markings. No Confidential or Strictly Confidential Information should ever be shared outside of Magna unless there is a fully signed NDA in place.

### 5.14.2 Handling of Information

Magna Information Security Policy defines the rules for information handling in everyday business use, which must be obeyed at MPT. Each company shall define the corresponding rules for storing, copying, circulation, transmission and destruction of information.

## 5.15 Competence Management

In order to fulfill the required skill level, the persons dedicated to the cybersecurity roles shall be selected according to company procedures. In case of differences within the skill levels the persons shall be trained according to procedures.

The following roles (as illustrated in the role responsibility structure)

- Product Cybersecurity Engineer
- Product Cybersecurity Manager
- Subject Matter Expert for Cybersecurity

shall possess the skills specified in table 1.

<b>General Skills</b>	<b>Product Cybersecurity Engineer</b>	<b>Product Cybersecurity Manager</b>	<b>Subject Matter Expert for Cybersecurity</b>
Product lifecycle management (PLM)	Basic	Basic	Basic
Testing (Component-, Subsystem-, System-, Vehicle Testing, SW Test methods)	Basic	Basic	Basic
Change Management	Basic	Basic	Basic
PLM Tools	Basic	Basic	Basic
FMEA Tools	Competent	Competent	Competent
FMEA	Competent	Competent	Competent
Hardware Components Engineering (e.g. Bearings, Dry-/ wet clutch, housing, gears & shafts, etc.)	Basic	Basic	Basic
Project Management	Professional	Professional	Basic
Project Management tools	Professional	Professional	Basic
Project Management Methods (Moderation & Presentation)	Professional	Professional	Basic
Communication (i.e. intercultural competence, conflict solving, cooperation)	Professional	Professional	Professional
Quality Awareness	Professional	Professional	Professional
Convincing & Negotiating Skills	Competent	Competent	Competent
Customer Orientation	Professional	Professional	Professional
GPMS Knowledge	Professional	Professional	Professional
Manufacturing Knowledge	Competent	Competent	Competent
Analyses and Problem Solving (8D, Six Sigma, Methods)	Professional	Professional	Professional
Process Knowledge	Competent	Competent	Professional
Business economics/ financial basics	Basic	Basic	Basic
Market knowledge (e.g. Transmission market global & suppliers)	Competent	Competent	Professional
Functional Safety	Competent	Competent	Competent

General Skills	Product Cybersecurity Engineer	Product Cybersecurity Manager	Subject Matter Expert for Cybersecurity
Product Cybersecurity	Professional	Professional	Professional
SW Versioning	Basic	Basic	Basic
SW Lifecycle Mgmt.	Competent	Competent	Competent
Programming languages (e.g. ANSI C, Java, PERL, Python, etc.)	Competent	Competent	Competent
Software Architecture	Competent	Competent	Competent
Calibration	Competent	Competent	Competent
SW Development	Competent	Competent	Competent
SW Engineering	Competent	Competent	Competent
Requirements Engineering	Professional	Competent	Professional
AUTOSAR Standard Concept and Methods	Competent	Competent	Competent
Embedded Automotive SW	Competent	Competent	Competent

*Table 1: Skill matrix for product cybersecurity related roles*

## 5.16 Quality Management

ISO/SAE 21434 requires a quality management system (such as International Automotive Task Force (IATF) 16949 in conjunction with ISO 9001, Automotive SPICE, etc.) as prerequisite to support cybersecurity engineering including change management, documentation management, configuration management and requirement management.

## 5.17 Tool Management

Tools that are used for concept or product development (such as model based development, verification tools), during production (such as flash writer, end of line tester), for maintenance (such as on-board diagnostic and reprogramming) that could impact cybersecurity of an item, system or component shall be managed. The management of the tools can be established by:

- Correct usage of the tools based on a user manual
- Protection against unintended usage or action
- Access control for the tool user
- Authentication of the tool

## 5.18 Cybersecurity Monitoring, Event Assessment, Vulnerability Management and Incident Response

Cybersecurity monitoring collects cybersecurity information on potential threats, vulnerabilities and possible mitigations for items and components to avoid known issues and to address new threats, and can serve as the input cybersecurity incident response activities. Cybersecurity event assessment determines the criticality of a cybersecurity event and launches corresponding activities, whereas the vulnerability analysis examines weaknesses and assesses if a particular weakness can be exploited to launch an attack. Cybersecurity incident response occurs when an organization responds to a cybersecurity event. If a cybersecurity event does not rise to the level of a cybersecurity incident, it is managed according to the vulnerability management that tracks and oversees the treatment of vulnerabilities.<sup>63</sup>

The following established cybersecurity incident response policy and the corresponding procedures set out the rules and procedures to be followed when responding to reported or suspected cybersecurity incidents. For the product related cybersecurity it is provided until the end of support for the product.

To maintain the trust of its employees, customers, and partners, and meet regulatory requirements, it is essential for a company to do everything possible to protect confidential information and systems in the face of a cyber-attack. The more a company is prepared to respond to a potential cyber-attack, the faster any threat can be eradicated and the impact of the threat on the business can be reduced more effectively. The “Cybersecurity Incident Response Procedure” is intended to help quickly and effectively contain a cyber threat while allowing normal business operations to continue. The actions outlined pay special attention to protecting privileged accounts that provide access to critical systems such as databases, applications, and networks. These include service, application and root accounts, network and administrator accounts, and local domain accounts.

The cybersecurity incident response policy requires that any individual,

- who suspects that a cyber security incident has or is likely to have occurred, or;
- who receives a report of a cybersecurity incident from a contracted 3rd party (e.g.: vendor, supplier, etc....)

---

<sup>63</sup> ISO/SAE 21434 – Road vehicles – Cybersecurity engineering, draft for intended DIS

shall immediately report the incident to the (Global) IT Service Desk. Personnel involved in information security incidents shall cooperate fully with all teams assigned with responsibility to investigate the incident.

## **5.18.1 Incident Response Procedure**

### ***5.18.1.1 Reporting and Assignment of a Security Incident***

Any individual who suspects or learns of a cybersecurity incident (an “Incident”) shall report such to the (Global) IT Service Desk. The (Global) IT Service Desk will assign any suspected or reported Incident that might be classified as a Cyber Security Incident (see Examples of Cybersecurity Incidents chapter) to e.g. Security Operations Center (SOC) for further processing.

The SOC will assess the extent to which the Incident involves electronic information. If the Incident does not involve electronic information, the SOC will assign the Incident to Corporate Security for further processing.

### ***5.18.1.2 Risk Assessment***

The SOC or Corporate Security as required, will assess the potential impact of the Incident through consultation with the reporter of the incident and/or related operations managers using information classification as defined by Information Security Policy. The Incident Response will be prioritized by impact severity.

### ***5.18.1.3 Incident Investigation***

SOC/Corporate Security will investigate the Incident with the responsible operations managers. The SOC and Corporate Security may involve each other as required. Investigations may include but are not limited to:

- In cases of electronic information incidents, forensic analysis of the affected device(s);
- Follow-up interviews with the employee(s) who reported the suspected cybersecurity incident or other employees with knowledge of the incident;
- Follow-up interviews with IT staff responsible for the affected IT system; and
- Follow-up interviews with Physical Security staff responsible for the facility.



Operations managers as advised by SOC/Corporate Security are responsible to secure evidence as needed (e.g.: Logs, Videos from CCTV (Closed Circuit Television) systems or even whole IT systems). Results of the investigation shall be documented within the Incident Management System.

#### ***5.18.1.4 Low Impact Incident Recovery***

SOC/Corporate Security will work with the responsible operational managers to recover from the Incident and suggest measures to prevent such incidents in the future.

#### ***5.18.1.5 Moderate and High Impact Incident Handling***

In the event an investigation into the Incident discovers proof that information has been accidentally or intentionally destroyed, lost, altered, disclosed without appropriate authorization, or accessed by a non-authorized third party, the strategy as outlined in Compliance and Legal Obligations (5.18.1.7) is followed for further actions to be taken as required.

#### ***5.18.1.6 Examples of Cybersecurity Incidents***

A cyber security incident is defined as any incident that potentially exposes internal, confidential or strictly confidential information to anyone who has not been authorized to access the data or anyone who abuses the access they have been granted.<sup>64</sup> An incident may occur from an external or internal source. The following are examples of security incidents but is not a complete list: <sup>64</sup>

- A system is breached by an external hacker
- A virus, worm, rootkit, keylogger etc. compromises a system
- A laptop is lost or stolen
- A user gains access to unauthorized data through technical or social engineering
- A backup tape has been lost or stolen
- A thumb drive, CD, etc. is lost or stolen
- A user uses his/her access in a non-authorized manner
- Data is sent by e-mail to non-authorized users
- A potential malicious E-Mail has been received (Phishing)

---

<sup>64</sup> Chancellor Herzog (2006): Major Information Security Incident Response Policy

- A hard copy report is lost or stolen that contains company data

As these examples illustrate, security incidents may occur accidentally or from intentional malicious activity.

#### **5.18.1.7 Compliance and Legal Obligations**

If at any point during an investigation it is determined that Personally Identifiable Information (PII) has been compromised, it shall be without delay escalated to relevant parties including the data privacy department which shall complete a personal data incident report.

#### **5.18.1.8 Updates**

Updates are changes made to the hardware or software of an item or component during post-development (i.e. operations and maintenance). The cybersecurity shall be preserved after the updates. Updates can be issued for several reasons, e.g. cybersecurity vulnerabilities, functional improvement, safety issues, etc.. Modifications of items or components which are in the concept, development or production phases can be covered by change management.

How (e.g. over the air update, roll back of the update) and how long (i.e. duration of cybersecurity support shall be agreed with the customer as part of the contract) the cybersecurity related updates will be carried out shall be specified. In case of updates, verification activities (including regression tests and re-testing for patching) shall be performed.

### **5.19 Product Cybersecurity**

#### **5.19.1 Requirements for Product Cybersecurity**

The product cybersecurity during product engineering shall be compliant with ISO/SAE 21434. For the application of ISO/SAE 21434, business unit/location specific procedures shall be derived. It shall be ensured by business unit/location specific procedure that all work products and requirements of the ISO/SAE 21434 are covered.

#### **5.19.2 Requirements for Maintenance, Repair and Decommissioning**

The product cybersecurity requirements for maintenance, repair and decommissioning shall be compliant with ISO/SAE 21434. For the application of ISO/SAE 21434, business unit/location

specific procedures shall be derived. It shall be ensured by business unit/location specific procedure that all work products and requirements of the ISO/SAE 21434 are covered.

### 5.19.3 Requirements for Key Management

If keys are used as security mechanism, the following requirements shall be fulfilled:

- As access to private keys is critical because it has the potential to disable security mechanism, it shall be ensured that all private keys and the access to private keys are classified as “strictly confidential” and the requirements for the classification are applied accordingly.
- Since the key management system is used over the whole product lifecycle including years after end of production, it shall be ensured that the key management system as well as all items linked to it fulfill the retention requirements for Product Development Records.

### 5.19.4 Requirements for Accessible Data

If data is accessible to the customer by a tool (e.g. service tester), it is only allowed to provide information which are classified as:

- Public
- Internal

Any other accessible information shall be evaluated per case and need to be approved by management.

### 5.20 Incident and Escalation Management for Product Cybersecurity

The incident and escalation management for Product Cybersecurity is based on a comparable process as shown for the company cybersecurity (see chapter 5.18). Table 2 illustrates the comparison of incident and escalation management for company and product cybersecurity.

Company cybersecurity	Product cybersecurity
Reporting and Assignment of a Security Incident	Incidents reported by customer / OEM Responsible: Customer liaison within plant AND monitoring of incident databases Responsible: Product Cybersecurity Manager
Risk Assessment	Based on reported / monitored incident Threat analysis and Risk Assessment (TARA) is performed Responsible: Product Cybersecurity Engineer
Incident Investigation	Based on TARA the potential impact of the incident is evaluated and it is checked if potential attack is successful Responsible: Product Cybersecurity Engineer
Low Impact Incident Recovery	Trigger Global Escalation Responsible: Product Cybersecurity Manager
Moderate and High Impact Incident Handling	
Updates	Based on results of Global Escalation the product is updated accordingly Responsible: Product Cybersecurity Manager

Table 2: Comparison of Incident and Escalation Management for company and product cybersecurity

The relation between product and company cybersecurity is shown in Figure 32.

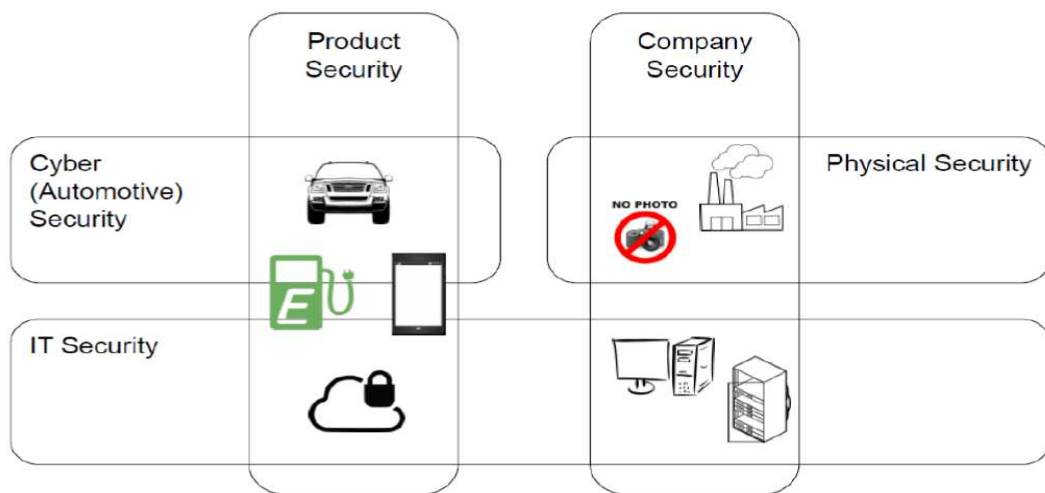


Figure 32. Relation between product and company cybersecurity<sup>65</sup>

<sup>65</sup> Own depiction

## 5.21 Lessons Learned

By means of lessons learned, following processes shall be instituted and maintained:

- a) Experiences gained from previous applications, including experience gathered from observation of internal and external information shall be reflected to existing processes, templates and documentation
- b) Learning from information obtained regarding products of similar application in the field shall be used to adapt the existing processes, templates and documentation
- c) Derived improvements shall be applied during the cybersecurity activities regarding subsequent projects;
- d) Lessons learned shall be communicated to the appropriate persons; and
- e) Adequacy of the rules and processes shall be evaluated

Moreover, with lessons learned, the company shall take proactive measures by making any necessary updates/alignment. Attack goals, attack paths and possible threats (i.e. TARA template) shall be updated based on lessons learned from previous projects and observation of internal/external information. Closed cybersecurity incidents shall be used as a source of lessons learned.

## 6. Validation

In order for a master thesis and the related study to be reliable, the content shall be validated. Due to the qualitative nature of this academic work, as a validation method, a credibility-check by means of expert reviews is chosen. Based on this approach, 4 cybersecurity experts of Magna Powertrain were requested to review the generated overall cybersecurity management policy document. The comments were provided directly in the draft document which was stored in a global Sharepoint and the findings were corrected by the author of this thesis. By this mean, all the experts were able to see the previous comments as well as include their own additional comments. After each review round, a follow up session with the reviewer was conducted to ensure all the findings were taken into account and mitigated. Moreover, additional face to face meetings were scheduled whenever necessary to discuss with the experts in detail. The overview of the validation process can be found in Figure 33, where inspection stands for the detailed review by the cybersecurity experts and preparation reflects the draft version which was sent for review.



Figure 33: Validation Process

The validation process described above, resulted in 38 findings, hence changes, that were incorporated into the overall cybersecurity management policy document.

Furthermore, the content was checked against ISO/SAE 21434 to ensure compliancy with the standard, which is accepted as the state of the art since it is developed in cooperation with many companies (OEM, Tier1-n) throughout the world.

## 7. Conclusion

The motivation of the thesis roots from one of the biggest challenges in automotive industry, namely how to deal with cybersecurity risks and the impact of those risks on projects. Although the impact of cybersecurity could be so big that could be sufficient to demolish the company, most companies are not aware how to deal with those risks, in addition to how to reduce the project related cybersecurity risks.

As proven by the quantitative survey, which was conducted by SAE and Synopsys with 593 participants, the companies are either not aware of the potential harms of cybersecurity or they do not establish program or team to deal with the related risks, although they see a highly likelihood of a malicious attack. Furthermore, the quantitative data (i.e. moderation of a break-out session at the OSS.5 conference) unearthed the importance of overall cybersecurity policy in automotive industry, which was justified by the brainstorming sessions with the experts and academicians from the automotive industry.

The existing state of the art standard ISO/SAE 21434 underscores the topics to be covered in an overall cybersecurity strategy and emphasize the importance of cybersecurity in automotive industry; nonetheless, it does not support companies substantially when it comes to realizing the overall cybersecurity policies.

The aim of the thesis was to reduce the potential cybersecurity risks in a project by creating an overall cybersecurity policy. For this purpose, first the importance of the topic was analyzed by means of a quantitative survey, a moderation session of a conference and self-assessment, which was conducted by a well-known consulting company. Moreover, in addition to the analysis of the status quo, all the important terms related with cybersecurity were explained to help people without a technical background in the field to comprehend the topic.

As shown in Figure 6 and 7, most of the recommendations regarding overall cybersecurity management require low effort to implement and their risk reduction effects are mainly high. This also indicates the fact that creation of an overall cybersecurity management policy and addressing the recommendations of Figure 6 and 7, will help companies to reduce their cybersecurity related project risks extensively that requires less than 3 months to implement. The overall cybersecurity management policy shall be the first priority of the companies. By considering all the explanations given above, an overall cybersecurity management policy will reduce the cybersecurity related project and company risks, which comprises the coordinated activities to direct and control an organization with regard to cybersecurity risks.



The personal opinion of the author is that, cybersecurity will be even more critical in the future. A company specific overall cybersecurity policy will smooth the way to deal with the cybersecurity risks as it contains all the relevant topics such as mission, vision and principles of the company about cybersecurity, responsibility distribution (RASIC), role structure, definition of necessary roles, cybersecurity governance, information classification, handling and sharing, competence management, cybersecurity monitoring, incident response, quality management, tool management, escalation management and lessons learned. So far, in the literature there is no publicly available solution which explains the companies how to deal with cybersecurity risks at a project and how to create an overall cybersecurity management policy.

The main contribution of the author is explaining about all these topics that are mentioned in ISO/SAE 21434 at a high level as well as defining strategies and requirements how to realize them. Furthermore, the people who do not have technical know-how on cybersecurity were familiarized by providing all the necessary background including the required definitions. Moreover, what can contribute the most on cybersecurity risk reduction, which is cheap, quick to implement yet still very effective was analyzed, which lead to the creation of this overall cybersecurity management policy.

In order to give a better insight about the thesis, the conclusion will focus on answering 3 main questions: *Why*, *How* and *What*.

**WHY** As can be concluded from the quantitative survey and moderation of a break-out session at a conference (i.e. qualitative data), an overall cybersecurity policy is very significant to deal with the cybersecurity risks. The quantitative survey emphasized the fact that the automotive industry is neither ready nor they know how to proceed. There is a lot of vulnerabilities especially at the supplier level, which shall be addressed. The ongoing standard ISO/SAE 21434 lists only the topics that are significant for cybersecurity, but it does not guide the companies how to deal with the related cybersecurity risks in detail. Therefore, there is no sound solution proposal to deal with the cybersecurity risks.

**HOW** In order to reduce potential cybersecurity related project risks, the easiest, most effective and quickest way is creation of an overall cybersecurity policy. By using the policy provided in this thesis, each (automotive) company can adapt/create a company-specific cybersecurity policy. It is recommended to use the synopsis provided to define the topics to be covered.

**WHAT** Creation of an overall cybersecurity management policy based on quantitative and qualitative data in order to reduce the potential project risks. Furthermore, ensuring the created

cybersecurity policy is in compliance to the ISO/SAE 21434 standard as to be able to claim following the state of the art as part of product liability.

The why, how and what parts already answers in general how the research questions were answered. Due to the fact that there are cybersecurity vulnerabilities at different companies and projects (see chapter 2.2), a systematic overall solution is required to deal with the corresponding risk. This overall cybersecurity management policy shall be in compliance with the existing state of the art (i.e. ISO/SAE 21434). Hence, the framework of the policy (Figure 25) as shown with a synopsis is based on the ISO/SAE 21434 standard. The synopsis also comprises the content to be covered in an overall cybersecurity management policy. The qualitative and quantitative data collected not only highlighted the importance of such an overall cybersecurity policy, but also how this policy can reduce the cybersecurity risks at a project. Therefore, the created project and company overall cybersecurity policy aims at reducing the project cybersecurity risks. Finally, the concept was validated by a qualitative validation method in the form of expert reviews, which were conducted by many cybersecurity experts who are working at Magna Powertrain Transmission Systems and Driveline Systems Divisions.

It is recommended as a next step, to elaborate the defined policy in order to write cybersecurity processes including the people who are responsible, creating the necessary templates for the relevant work products and defining project and/or location specific guidelines. Furthermore, the overall cybersecurity management policy shall be a living document with a constant progress. As the threat, risk, state of the art (e.g. ISO/SAE 21434) changes, the document has to be adapted accordingly. Therefore, the overall cybersecurity management policy was created as a screen shot of the available information during the course of this academic work. The proposed relation between the policy, process and guidelines are shown in Figure 34.

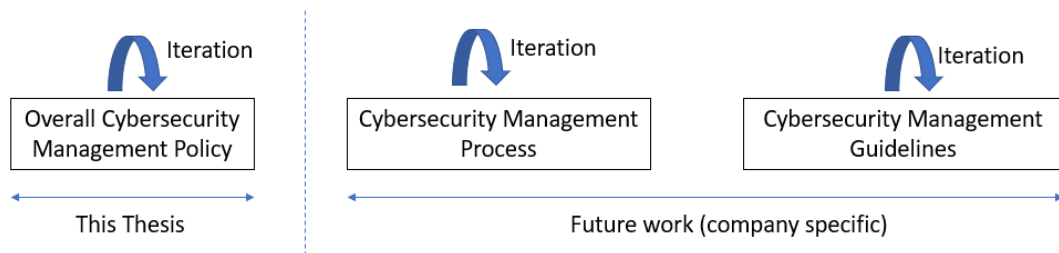


Figure 34: Proposed relation between the cybersecurity policy, process and guidelines

This thesis identified the cybersecurity risks qualitatively, future studies could address the risk reduction quantitatively to better understand the implications of these results. Besides, a further study can reveal the relation between project risks and the related costs and how much costs can be reduced by means of applying an overall cybersecurity management policy.

## Bibliography

Atle Refsdal, Bjørnar Solhaug, Ketil Stølen (2015): Cyber-Risk Management, ISBN 978-3-319-23570-7 (eBook), Springer

British Standards Institution (2016), BS ISO/IEC 27000:2016: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. British Standards Institution, London, UK.

David Bailey (2018), Quantitative Cybersecurity Risk Management for Autonomous Vehicle Systems, Technical University of Munich, pp. 9-22

Dietmar P. F. Möller, Roland E. Haas (2019): Guide to Automotive Connectivity and Cybersecurity, Trends, Technologies, Innovations and Applications, ISBN 978-3-319-73512-2 (eBook), Springer

Hendershot, S. (2014): Cyberattack Growth Means Sophisticated Cybersecurity | PM Network,” PM Network, Project Management Institute, Newtown Square, PA

International Organization for Standardization. ISO 31000 - Risk management. <https://www.iso.org/iso-31000-risk-management.html>, 2018b

ISO/SAE 21434 – Road vehicles – Cybersecurity engineering, draft for intended DIS, ISO/TC 22/SC 32/WG 11 N 960, 10.12.2019

John Adams (2005): Risk Management: It's not rocket science - it's much more complicated

Kelly, B., LaSalle, R., Dal Cin, P. (2019): The cost of cybercrime, Ninth Annual Cost of Cybercrime Study, Ponemon Institute LLC and Accenture, pp. 10-12

Kyriakidis, M., Happee, R., & Winter, J.M. (2015): Public opinion on automated driving: Results of an international questionnaire among 5000 respondents.

Lamas, Sacaluga, Ferrín, Froján (2012): “Project Risk Management in Automotive Industry. A Case Study”; pp. 1-2, <https://pdfs.semanticscholar.org/e2da/c23949761ca147c255c182944ad703fe6853.pdf> - accessed on 03.08.2019

Larry Ponemon (2017): Will Privacy & Security Concerns Stall the Adoption of Autonomous Automobiles?

Moore, T., Tandy, Dynes, S., & Chang, F. (2015): Identifying How Firms Manage Cybersecurity Investment, pp. 1-9

National Initiative for Cybersecurity Careers and Studies (2009), adapted from CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review

National Institute of Standards and Technology, Federal Information Processing Standard 200 (2006): Minimum Security Requirements for Federal Information and Information Systems

Peter Sabo (2016): Official project launch in automotive companies without R&D. Master thesis, Vienna University of Technology

Presley, Steven S. and Landry, Jeffrey P. (2016): "A Process Framework for Managing Cybersecurity Risks in Projects", SAIS 2016 Proceedings. 8, pp. 1-2

Project Management Institute (PMI) (2013): A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Fifth Edition, Project Management Institute, Newtown Square, PA, USA

SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, Joint ISO/TC 22/SC 32 - SAE WG, Automotive security engineering, January 2016

Schellekens, Maurice. (2016): Car hacking: Navigating the regulatory landscape. Computer Law & Security Review. 32. 10.1016/j.clsr.2015.12.019.

Sepúlveda Estay, D. A. (2017): Managing cyber-risk and security in the global supply chain: a systems analysis approach to risk, structure and behaviour. DTU Management Engineering, pp. 9-10

Solhaug, B. (2015): Tool-Supported Cyber-Risk Assessment, SINTEF ICT, SASSI, Berlin

United States Department of Defense (US DoD) (Jan. 2015), Department of Defense Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System, United States Department of Defense, Washington DC

United States Department of Defense (US DoD) (Sept. 2015): DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, Version 1.08, Office of the Secretary of Defense, September 2015. United States Department of Defense, Washington, DC, USA

Süzer, O. (2018): Vector Consulting Services, Automotive Cybersecurity Training, Stuttgart

Webster, J. and Watson, R.T., (2002): Analysing the past to prepare for the future: Writing a literature review. MIS quarterly, pp. xiii-xxiii

Zorn, T. and Campbell, N., (2006): Improving the writing of literature reviews through a literature integration exercise. Business Communication Quarterly, 69(2), pp.172-183

## References

[1] Akshay Bhargava: Cyber Risk: A Boardroom Priority

<https://boardmember.com/cyber-risk-a-boardroom-priority/> - accessed on 25.01.2020

[2] Angela Barber (2018): Status of Work in Process on ISO/SAE 21434 Automotive Cybersecurity Standard

<https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1525889601.pdf> - accessed on 20.10.19

[3] Brad Egeland (2015): How much will cybercrime affect project management in 2016?

<https://www.projectsart.co.uk/how-much-will-cybercrime-affect-project-management-in-2016.php> - accessed on 22.09.19

[4] Cambridge Dictionary (2019): Likelihood?

<https://dictionary.cambridge.org/dictionary/english/likelihood-> accessed on 13.12.19

[5] Chancellor Herzog (2006): Major Information Security Incident Response Policy

[https://supportcenter.ct.edu/Service/CCC\\_policies/MajorIncidentResponsePolicy.pdf](https://supportcenter.ct.edu/Service/CCC_policies/MajorIncidentResponsePolicy.pdf) - accessed on 25.01.2020

[6] Hack2Secure (2017): Cybersecurity vs. Information Security

<https://www.hack2secure.com/blogs/cyber-security-vs-information-security> accessed on 20.10.19

[7] Infineon (2018): Cybersecurity Mechanism for Connected Vehicles

[https://www.infineon.com/dgdl/Infineon-ISP-Use-Case-Cyber-security-mechanisms-for-connected-vehicles-ABR-v02\\_18-EN.pdf?fileId=5546d462647e95a60164889affd74a5e](https://www.infineon.com/dgdl/Infineon-ISP-Use-Case-Cyber-security-mechanisms-for-connected-vehicles-ABR-v02_18-EN.pdf?fileId=5546d462647e95a60164889affd74a5e) - accessed on 12.12.19

[8] kVA (2016): An Overview of Functional Safety for Automotive

<http://techlav.ncat.edu/Presentations/Jody%20Nelson.pdf> – accessed on 25.01.2020

[9] Magic: Subject Matter Expert (SME) Roles and Responsibilities

<http://www.dfa.ms.gov/media/9207/subject-matter-expert-sme-roles-and-responsibilities.pdf> - accessed on 25.01.2020

[10] Members of Auto Alliance and Global Automakers (2016): Framework for Automotive Cybersecurity Best Practices

<https://www.globalautomakers.org/OldSiteContentAssets/press-release/Automakers-Develop-Framework-for-Automotive-Cybersecurity-Best->

Practices-assets/framework-autocyberbestpractices-14jan20161-pdf - accessed on 20.10.19

[11] National Cybersecurity Centre (2018): What is a cyber incident?

<https://www.ncsc.gov.uk/information/what-cyber-incident> - accessed on 13.12.2019

[12] OSS.5 Europe (2019): World Cafes Sessions, What is a World Café?

<https://www.oss-5.com/sessions/world-cafes-sessions-oss-5-europe> - accessed on 25.01.2020

[13] Paul Rosenzweig (2017): The Evolving Landscape of Cybersecurity Liability

<https://www.chertoffgroup.com/blog/the-evolving-landscape-of-cybersecurity-liability> - accessed on 13.10.19

[14] Renee Tarun (2018): A Layered Approach to Cybersecurity: People, Processes, and Technology

<https://www.csoonline.com/article/3326301/a-layered-approach-to-cybersecurity-people-processes-and-technology.html> - accessed on 03.11.19

[15] SAE and Synopsys (2018): Securing the modern vehicle: A study of cybersecurity automotive practises

<https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/securing-the-modern-vehicle.pdf> - accessed on 03.08.19

[16] Sean Duca (2019): Supply chain remains the weakest link in cybersecurity.

<https://www.supplychaindigital.com/technology/supply-chain-remains-weakest-link-cybersecurity> - accessed on 15.09.19

[17] Taryn Oesch (2019): Building a "Human Firewall": Cybersecurity Awareness Training That Works

<https://trainingindustry.com/articles/compliance/building-a-human-firewall-cybersecurity-awareness-training-that-works/> - accessed on 25.01.2020

[18] Vangie Beal (2019): What is cyberspace?, Webopedia

<https://www.webopedia.com/TERM/C/cyberspace.html> - accessed on 13.12.19

[19] Vector (2019): Automotive Cybersecurity Webinar

[https://assets.vector.com/cms/content/consulting/publications/Webinar\\_Security.pdf](https://assets.vector.com/cms/content/consulting/publications/Webinar_Security.pdf) - accessed on 13.10.19

[20] Vector (2016): Functional Safety with ISO 26262 Webinar

[https://assets.vector.com/cms/content/consulting/publications/Webinar\\_Safety.pdf](https://assets.vector.com/cms/content/consulting/publications/Webinar_Safety.pdf) - accessed on 25.01.2020



## List of figures

<i>Figure 1: The average annual cost of cybercrime by industry<sup>6</sup></i>	6
<i>Figure 2: Overview of the research approach and methodology</i>	8
<i>Figure 3: Overview of the master thesis structure</i>	9
<i>Figure 4: Reduction of the start risk to an acceptable level in cybersecurity</i>	11
<i>Figure 5: Descriptions for priority, risk reduction and overall level of effort needed for implementation</i>	14
<i>Figure 6: Recommendations on different focus areas with respect to priority, risk reduction and overall effort from Self-Assessment Study (Points 1-12)</i>	15
<i>Figure 7: Recommendations on different focus areas with respect to priority, risk reduction and overall effort from the Self-Assessment Study (Points 13-20)</i>	16
<i>Figure 8: The relation between asset, attack, attack potential, threat and security goal</i>	19
<i>Figure 9: The relation between threat source, threat, vulnerability and risk</i>	19
<i>Figure 10: Specific automotive asset categories</i>	20
<i>Figure 11: The relation between risk, incident, asset, likelihood and party<sup>35</sup></i>	21
<i>Figure 12: The relation between information security, information and communication technology security and cybersecurity</i>	23
<i>Figure 13: The relation between safety critical and cybersecurity critical systems (SAE J3061)</i>	24
<i>Figure 14: Overview of standards, assessments, software coding standards, organisations and methods related to cybersecurity</i>	25
<i>Figure 15: Difference between legally binding requirements and ISO Standards</i>	27
<i>Figure 16: Status of cybersecurity according to survey</i>	30
<i>Figure 17: Awareness of potential cybersecurity harms and concerns voiced<sup>53</sup></i>	30
<i>Figure 18: Overview of the answers provided to the survey questions</i>	31
<i>Figure 19: Answers to the first question by the experts during the moderation of the break-out session at the OSS.5 Conference</i>	34
<i>Figure 20: Answers to the second question by the experts during the moderation of the break-out session at the OSS.5 Conference</i>	35
<i>Figure 21: Difference between the functional safety and cybersecurity risk dimensions</i>	35
<i>Figure 22: Answers to the third question by the experts during the moderation of the break-out session at the OSS.5 Conference</i>	36
<i>Figure 23: Answers to the fourth question by the experts during the moderation of the break-out session at the OSS.5 Conference</i>	37
<i>Figure 24: Answers to the fifth question by the experts during the moderation of the break-out session at the OSS.5 Conference</i>	38
<i>Figure 25: Synopsis of the overall cybersecurity policy</i>	40
<i>Figure 26. Cybersecurity RASIC Overview</i>	43
<i>Figure 27. Cybersecurity measures that can be applied at different sections of the vehicle</i>	46
<i>Figure 28. Layered security concept with the associated security concepts<sup>61</sup></i>	46
<i>Figure 29. Mapping between ISO/SAE 21434 and MPT Work products</i>	52
<i>Figure 30. Overview of the cybersecurity governance proposal</i>	53
<i>Figure 31. MPT High Level ISO/SAE 21434 Compliance Strategy</i>	54



<i>Figure 32. Relation between product and company cybersecurity</i> .....	70
<i>Figure 33: Validation Process</i> .....	72
<i>Figure 34: Proposed relation between the cybersecurity policy, process and guidelines</i> .....	75
<i>Figure 35: ISO/SAE 21434 Overview<sup>23</sup></i> .....	83
<i>Figure 36: ISO 26262 Overview</i> .....	84
<i>Figure 37: Comparison of the cybersecurity and functional safety V-Model development</i> .....	84
<i>Figure 38: Concept level comparison of the cybersecurity and functional safety development</i> .....	108
<i>Figure 39: System level comparison of the cybersecurity and functional safety development</i> .....	108
<i>Figure 40: Hardware level comparison of the cybersecurity and functional safety development</i> .....	109
<i>Figure 41: Software level comparison of the cybersecurity and functional safety development</i> .....	109

## List of tables

Table 1: Skill matrix for product cybersecurity related roles .....	64
Table 2: Comparison of Incident and Escalation Management for company and product cybersecurity.....	70

# Appendices

## A.1 ISO/SAE 21434 and ISO 26262 Overview (2 Page)

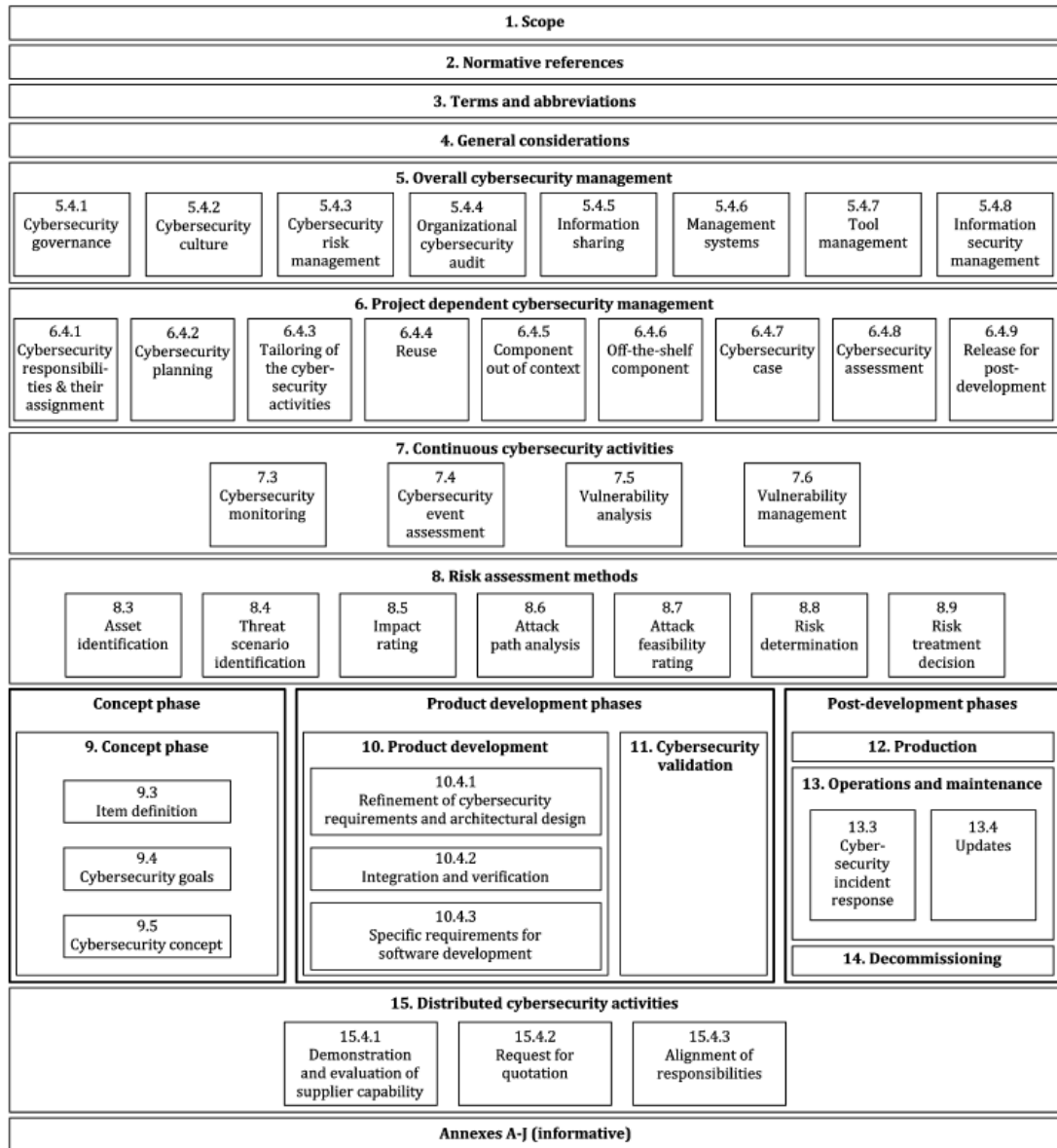


Figure 35: ISO/SAE 21434 Overview<sup>23</sup>

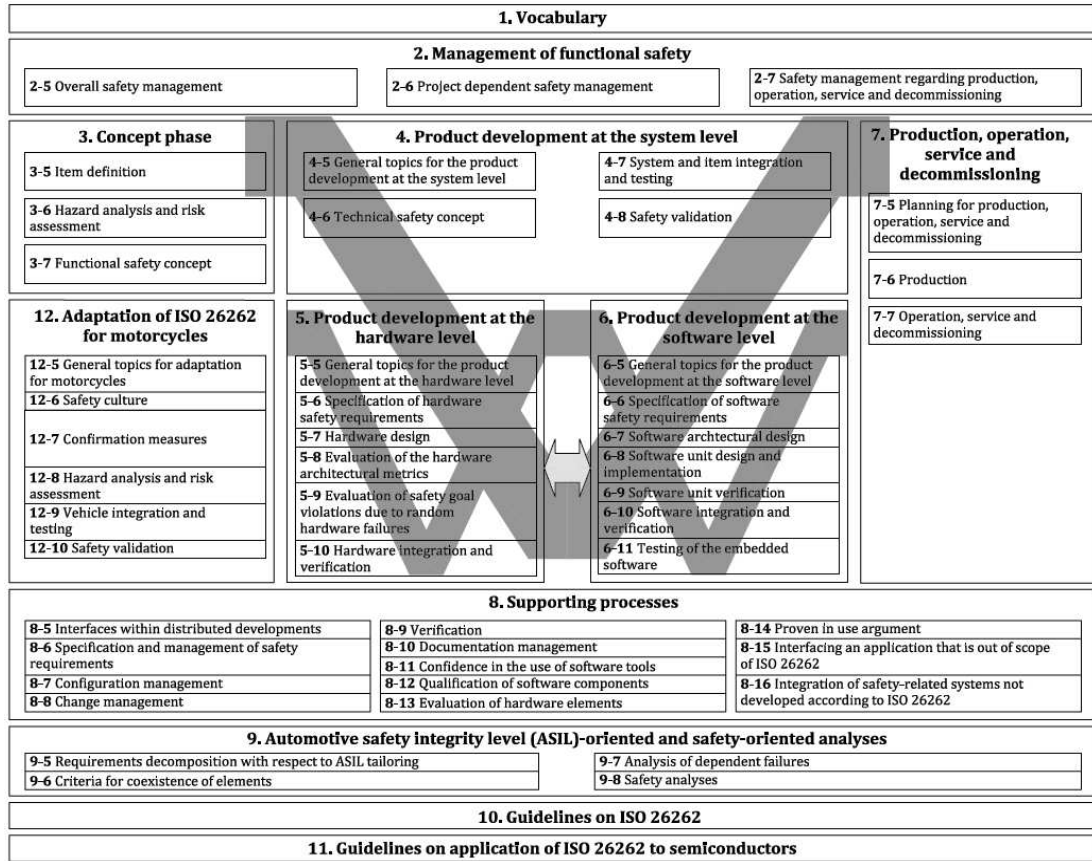


Figure 36: ISO 26262 Overview

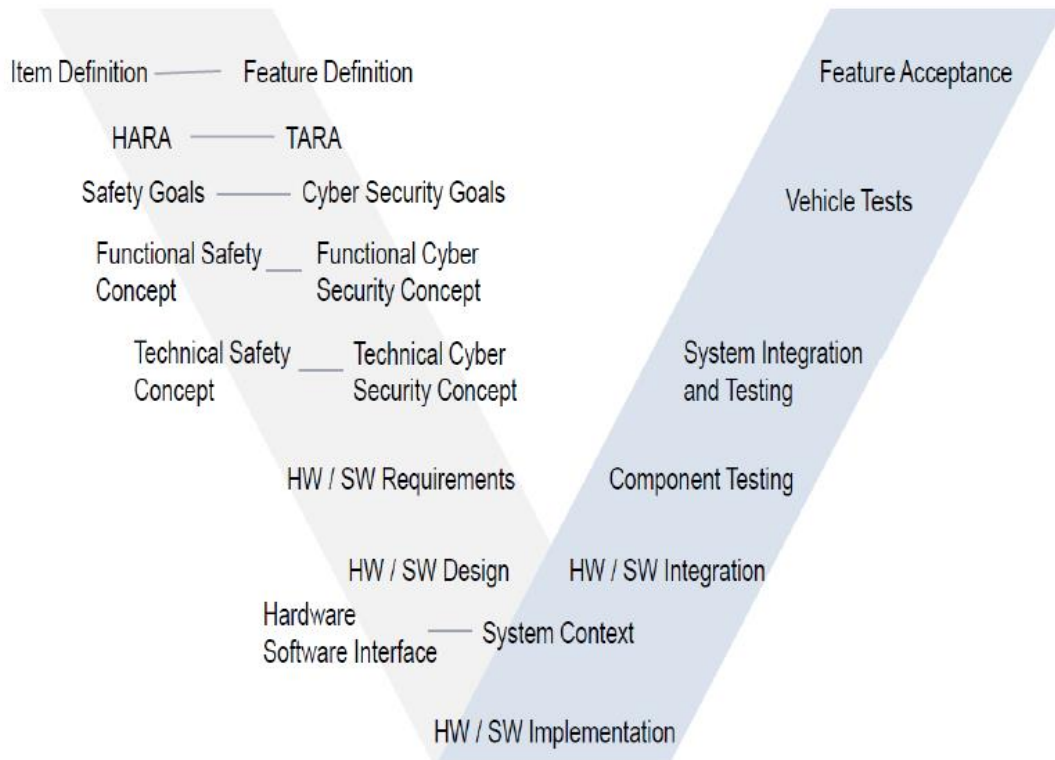


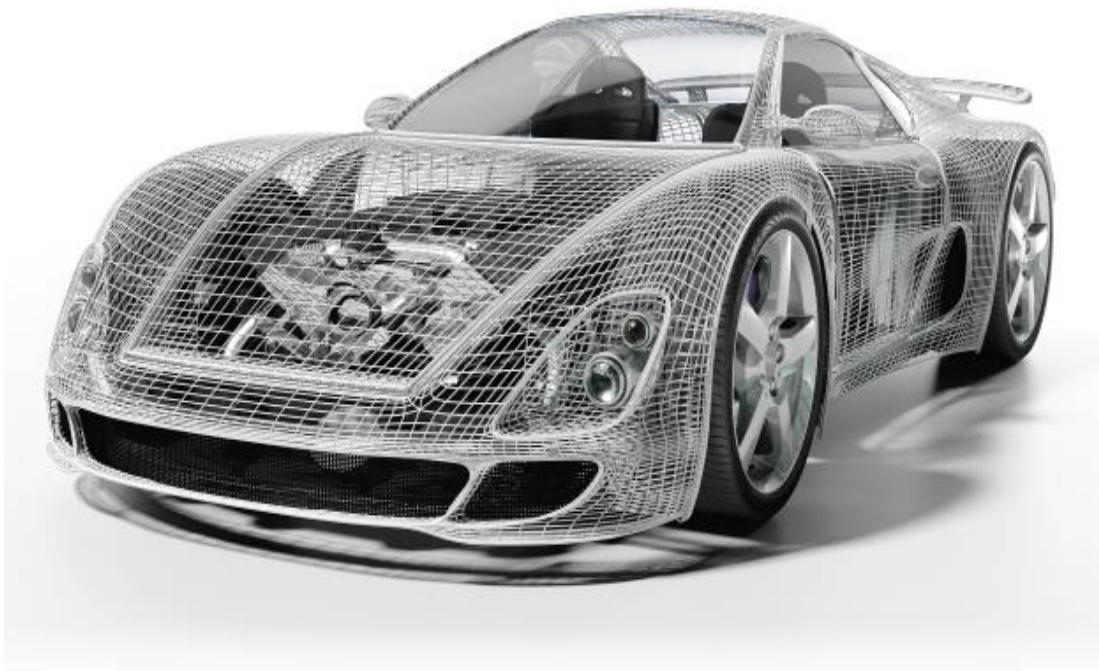
Figure 37: Comparison of the cybersecurity and functional safety V-Model development

**A.2 Survey (19 Pages)**

**A Study of Automotive Industry Cybersecurity Practises<sup>32</sup>**



# Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices



An independent study commissioned by



Die approbierte gedruckte Originalversion dieser Masterarbeit ist an der TU Wien Bibliothek verfügbar.  
The approved original version of this thesis is available in print at TU Wien Bibliothek.



# Table of Contents

Executive Summary.....	1
Organizational Dynamics and Challenges .....	3
Technical Dynamics and Challenges.....	6
Product Development and Security Testing Practices .....	9
Supply Chain and Third-Party Component Challenges.....	13
Conclusions.....	14
Methods.....	15
Appendix: Detailed Survey Results .....	18
Ponemon Institute .....	29



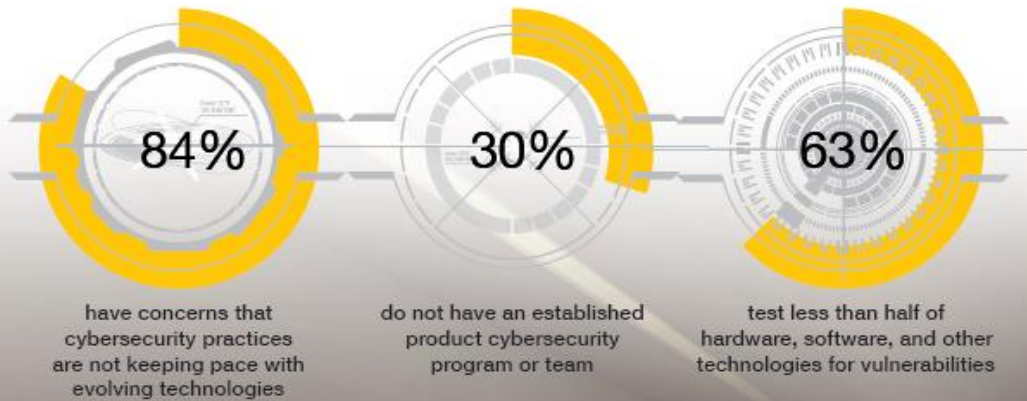
# Executive Summary

Today's vehicle is a connected, mobile computer, which has introduced an issue the automotive industry has little experience dealing with: cybersecurity risk. Automotive manufacturers have become as much software as transportation companies, facing all the challenges inherent to software security.

Synopsys and SAE International partnered to commission this independent survey of the current cybersecurity practices in the automotive industry to fill a gap that has existed far too long—the lack of data needed to understand the automotive industry's cybersecurity posture and its capability to address software security risks inherent in connected, software-enabled vehicles. Ponemon Institute was selected to conduct the study. Researchers surveyed 693 professionals responsible for contributing to or assessing the security of automotive components.

## Software Security Is Not Keeping Pace with Technology in the Auto Industry

When automotive safety is a function of software, the issue of software security becomes paramount—particularly when it comes to new areas such as connected vehicles and autonomous vehicles. Yet, as this report demonstrates, both automobile OEMs and their suppliers are struggling to secure the technologies used in their products. Eighty-four percent of the respondents to our survey have concerns that cybersecurity practices are not keeping pace with the ever-evolving security landscape.





Automotive companies are still building up needed cybersecurity skills and resources. The security professionals surveyed for our report indicated that the typical automotive organization has only nine full-time employees in its product cybersecurity management program. Thirty percent of respondents said their organizations do not have an established product cybersecurity program or team. Sixty-three percent of respondents stated that they test less than half of hardware, software, and other technologies for vulnerabilities.

Pressure to meet product deadlines, accidental coding errors, lack of education on secure coding practices, and vulnerability testing occurring too late in production are some of the most common factors that render software vulnerabilities. Our report illustrates the need for more focus on cybersecurity; secure coding training; automated tools to find defects and security vulnerabilities in source code; and software composition analysis tools to identify third-party components that may have been introduced by suppliers.

## Software in the Automotive Supply Chain Presents a Major Risk

While most automotive manufacturers still produce some original equipment, their true strength is in research and development, designing and marketing vehicles, managing the parts supply chain, and assembling the final product. OEMs rely on hundreds of independent vendors to supply hardware and software components to deliver the latest in vehicle technology and design.

Seventy-three percent of respondents surveyed in our report say they are very concerned about the cybersecurity posture of automotive technologies supplied by third parties. However, only 44 percent of respondents say their organizations impose cybersecurity requirements for products provided by upstream suppliers.

## Connected Vehicles Offer Unique Security Issues

Automakers and their suppliers also need to consider what the connected vehicle means for consumer privacy and security. As more connected vehicles hit the roads, software vulnerabilities are becoming accessible to malicious hackers using cellular networks, Wi-Fi, and physical connections to exploit them. Failure to address these risks might be a costly mistake, including the impact they may have on consumer confidence, personal privacy, and brand reputation.

Respondents to our survey viewed the technologies with the greatest risk to be RF technologies (such as Wi-Fi and Bluetooth), telematics, and self-driving (autonomous) vehicles. This suggests non-critical systems and connectivity are low-hanging fruit for attacks and should be the main focus of cybersecurity efforts.

## Conclusion

As will be clear in the following pages, survey respondents in a myriad of sectors of the industry show a significant awareness of the cybersecurity problem and have a strong desire to make improvements. Of concern is the 69 percent of respondents who do not feel empowered to raise their concerns up their corporate ladder, but efforts such as this report may help to bring the needed visibility of the problem to the executive and boardroom level.

Just as lean manufacturing and ISO 9000 practices both brought greater quality to the automotive industry, a rigorous approach to cybersecurity is vital to achieve the full range of benefits of new automotive technologies while preserving quality, safety, and rapid time to market.



# Organizational Dynamics and Challenges



Even though they see a clear danger, respondents do not feel they can raise their concerns about cybersecurity to upper management.

Sixty-two percent of those surveyed say a malicious or proof-of-concept attack against automotive technologies is likely or very likely in the next 12 months, but 69 percent reveal that they do not feel empowered to raise their concerns up their chain of command.

As shown in Figure 1, more than half (52 percent) of respondents are aware of potential harm to drivers of vehicles because of insecure automotive technologies, whether developed by third parties or by their organizations. However, only 31 percent say they feel empowered to raise security concerns within their organizations.

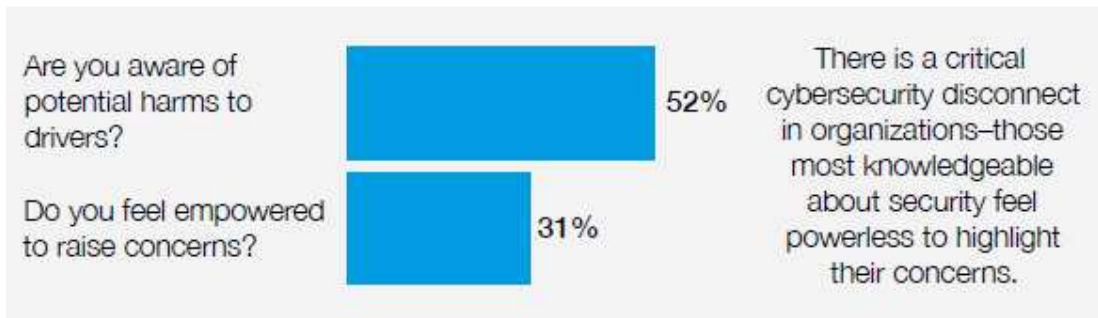


Figure 1. Awareness of potential harms to drivers exists but concerns are not voiced.  
\*Yes\* responses presented



Despite those concerns, there is a lack of product cybersecurity teams and programs.

In your opinion, how likely is a malicious or proof-of-concept (i.e. security research) attack to occur against automotive software/technology/components developed or in use by your organization over the next 12 months?	• <i>Very likely</i>	27%
	• <i>Likely</i>	35%
	• Somewhat likely	23%
	• Not likely	15%
Do you feel empowered to raise concerns about the security of automotive technology in your organization?	• Yes	31%
	• No	69%

Thirty percent of respondents overall say their organizations do not have an established product cybersecurity program or team. Only 10 percent say their organizations have a centralized product cybersecurity team that guides and supports multiple product development teams.

Which of the following best describes your organization's approach to product cybersecurity? Please select one choice only.	• Product cybersecurity is part of the traditional IT cybersecurity team (typically under a global CISO)	20%
	• Product cybersecurity is part of the functional safety team	17%
	• We have a centralized product cybersecurity team (i.e. center of excellence) that guides and supports multiple product development teams	10%
	• We have a decentralized product cybersecurity team, with cybersecurity experts attached to specific product development teams	23%
	• <b>We do not have an established product cybersecurity program or team</b>	<b>30%</b>

When these data are broken down by OEM or supplier (Figure 2), 41 percent of respondents in suppliers do not have an established product cybersecurity program or team of any kind. In contrast, only 18 percent of OEMs do not have a product security program or team.

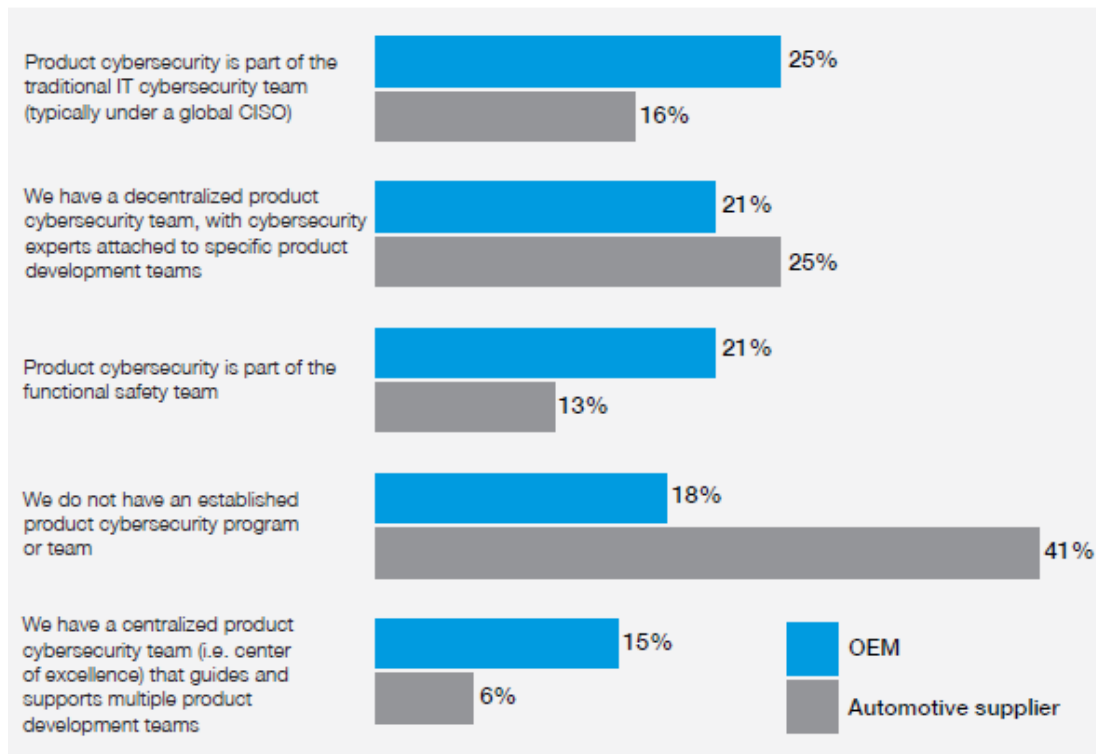


Figure 2. Which of the following describes your organization's approach to product cybersecurity?



A significant percentage of suppliers are overlooking a well-established best practice: to employ a team of experts to conduct security testing throughout the product development process, from the design phase through decommissioning.



## Automotive companies lack necessary cybersecurity resources and skills.

The majority of the industry respondents believe they do not have appropriate levels of resources to combat the cybersecurity threats in the automotive space.

On average, companies have only nine full-time employees in their product cybersecurity management programs. Sixty-two percent of respondents say their organizations do not have the necessary cybersecurity skills. More than half (51 percent) say they do not have enough budget and human capital to address cybersecurity risks.

Does your organization allocate enough resources (i.e. budget and human resources) to cybersecurity?	• Yes	49%
	• <b>No</b>	<b>51%</b>
Does your organization have the necessary cybersecurity skills in product development?	• Yes	38%
	• <b>No</b>	<b>62%</b>
How many FTEs participate in product cybersecurity management programs in your organization?	• <b>Less than 5</b>	<b>30%</b>
	• <b>5 to 10</b>	<b>44%</b>
	• <b>11 to 20</b>	<b>18%</b>
	• More than 20	8%



# Technical Dynamics and Challenges

Vehicles are now essentially a mobile IT enterprise that includes control systems, rich data, infotainment, and wireless mesh communications through multiple protocols. That connectivity can extend to the driver's personal electronic devices, to other vehicles and infrastructure, and through the Internet to OEM and aftermarket applications, making them targets for cyberattacks. Unauthorized remote access to the vehicle network and the potential for attackers to pivot to safety-critical systems puts at risk not just drivers' personal information but their physical safety as well.

Automotive engineers, product developers, and IT professionals highlighted several major security concern areas as well as security controls they use to mitigate risks.



A majority (84 percent) of respondents are concerned that cybersecurity practices are not keeping pace with changing technology.

How concerned are you that your organization's cybersecurity practices are not keeping pace with changing automotive technologies?  1 = not concerned to 10 = very concerned	• 1 or 2	5%
	• 3 or 4	11%
	• 5 or 6	25%
	• 7 or 8	22%
	• 9 or 10	37%

Technologies viewed as causing the greatest risk are RF technologies, telematics, and self-driving vehicles. Of the technological advances making their way into vehicles, these three are seen to pose the greatest cybersecurity risks. Organizations should be allocating a larger portion of their resources to reducing the risk in these technologies.

Respondents say that pressure to meet product deadlines (71 percent), lack of understanding/training on secure coding practices (60 percent), and accidental coding errors (55 percent) are the most common factors that lead to vulnerabilities in their technologies. Engaging in secure coding training for key staff will target two of the main causes of software vulnerabilities in vehicles.

Which technologies pose the greatest cybersecurity risk?  Select all that apply.	• Infotainment systems	31%
	• Powertrain control units	46%
	• SOC system on chip-based components	44%
	• <b>Self-driving (autonomous) vehicles</b>	58%
	• Software-focused service provider (e.g. cloud, insurance provider, streaming service, etc.)	51%
	• <b>Telematics</b>	60%
	• Steering systems	45%
	• Electrification components	17%
	• Cameras	29%
	• <b>RF technologies (e.g. Wi-Fi, Bluetooth, Hot spots)</b>	63%

<p>What are the primary factors that lead to vulnerabilities in the automotive technologies developed or in use by your organization.</p> <p>Select the top four factors.</p>	• <b>Accidental coding errors</b>	55%
	• The use of insecure/outdated open source software components	40%
	• Malicious code injection	23%
	• Lack of internal policies or rules that clarify security requirements	26%
	• <b>Lack of understanding/training on secure coding practices</b>	60%
	• <b>Pressure to meet product deadlines</b>	71%
	• Lack of quality assurance and testing procedures	50%
	• Product development tools have inherent bugs	39%
	• Incorrect permissions	19%
	• Back end systems	15%



### Security patches and updates are a challenge.

Only 39 percent of respondents say their software update delivery model addresses critical security vulnerabilities in a timely manner.

Does your organization's software update delivery model address critical security vulnerabilities in a timely manner?	• Yes	39%
	• <b>No</b>	61%

As shown in Figure 3, 65 percent say security patches and updates for vehicles in-market are delivered through procured software, components, and systems. Fifty-one percent say this happens through wireless communications connected to personal electronic/computing devices.

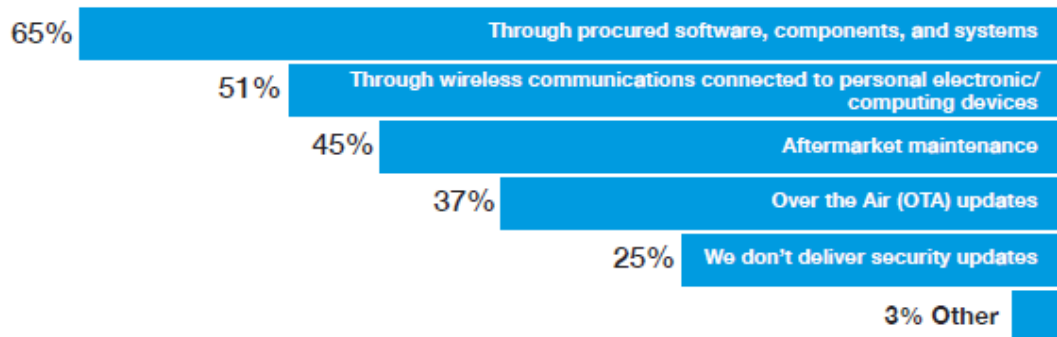


Figure 3. How does your organization deliver security patches and updates for vehicles in-market?

Only 37 percent say they use over-the-air (OTA) updates to deliver security patches, but more than 50 percent say they will do so in the next 5 years. This suggests the need for an industry standard for secure OTA updates.

If you don't deliver OTA updates, do you plan to in the future?	• Yes, in 1 to 3 years	33%
	• Yes, in 3 to 5 years	23%
	• Greater than 5 years	9%
	• No plans to deliver OTA updates	35%

 **Firewalls and gateways are the most common security controls incorporated into vehicles.**

Sixty-four percent of respondents incorporate firewalls and 59 percent use gateways as key security controls.

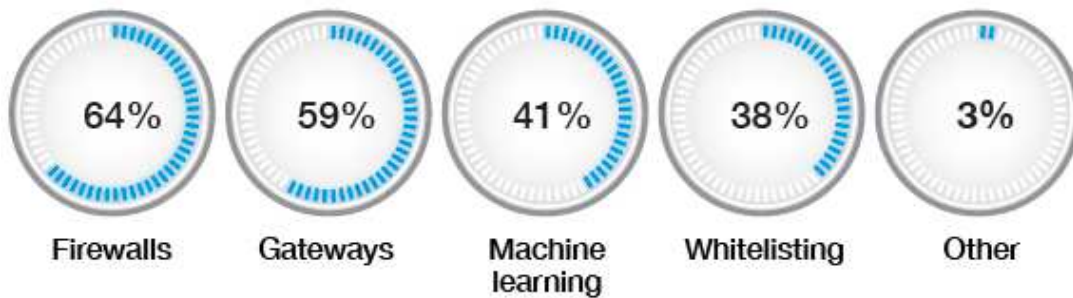



Figure 4. Does your organization incorporate security counter measures in its vehicles?

 **A majority of companies use key management systems, but 43 percent still use a manual process.**

Sixty-three percent of respondents say their organizations use key management systems (the management of cryptographic keys, including generation, exchange, storage, use, and replacement of keys). As shown in Figure 5, 56 percent use a central key management system/server while 45 percent have a formal key management policy. Yet 43 percent use a manual process for key management, limiting its usefulness and hampering security.

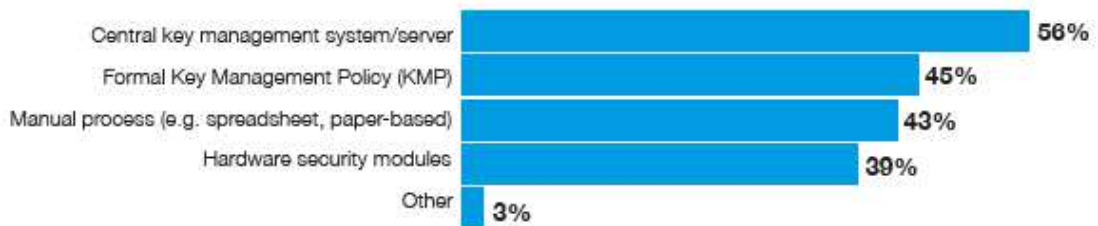


Figure 5. What key management systems does your organization presently use?



# Product Development and Security Testing Practices

Our survey questions targeted the security practices that companies employ in their product development. An established best practice is to use a risk-based, process-driven approach to cybersecurity, integrating it into the entire product development life cycle.



The survey found security vulnerabilities are being assessed far too late in the product release process.

Only 47 percent of companies assess vulnerabilities in the *requirements and design* phase or the *development and testing* phase (see Figure 6).



**Figure 6.** When during the development life cycle does your organization assess automotive software/technology/components for security vulnerabilities?

This process is contrary to the guidance of SAE J3061™ *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*,<sup>1</sup> which advocates for a risk-based, process-driven approach to cybersecurity throughout the entire product development life cycle.



### Advantages of Integrating Security into Product Development

1. Integrating security concepts into product design achieves higher security than applying security controls post production.
2. Risks and vulnerabilities are identified early, and appropriate security controls can be applied.
3. This is a vastly more efficient way to apply limited cybersecurity resources and normalizes cybersecurity costs as a critical piece of the product development discipline.

J3061 is the world's first automotive cybersecurity standard, and it is a valuable tool to incorporate cybersecurity processes into product development.

<sup>1</sup> SAE J3061™ *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, SAE International, January 2016



## Failure to perform adequate security tests leads to vulnerabilities.

**Sixty-three percent** of respondents state that they test less than 50 percent of hardware, software, and other technologies for vulnerabilities. Additionally, 71 percent believe that pressure to meet product deadlines is the primary factor leading to security vulnerabilities. These responses suggest that few software/technology/components are being tested in order for organizations to meet deadlines.

What percentage of automotive technology used by your organization is tested for cybersecurity vulnerabilities?	• <b>None</b>	<b>25%</b>
	• <b>Less than 25%</b>	<b>12%</b>
	• <b>26% to 50%</b>	<b>26%</b>
	• 51% to 75%	23%
	• 76% to 100%	14%
	Total	100%

What negative business impacts are caused by insecure automotive technology used by your organization?	• Security-related recalls	21%
	• Damage to supply chain partner relationships	64%
	• <b>Delayed or missed release dates</b>	<b>67%</b>
	• <b>Unintended interaction between components during integration testing</b>	<b>59%</b>
	• Regulatory impacts, sanctions, or fines	6%
	• Not aware of any adverse events	29%

What are the primary factors leading to vulnerabilities in the automotive technologies used by your organization?	• Accidental coding errors	56%
	• The use of insecure/outdated open source software components	40%
	• Malicious code injection	23%
	• Lack of internal policies or rules that clarify security requirements	28%
	• Lack of understanding/training on secure coding practices	60%
	• <b>Pressure to meet product deadlines</b>	<b>71%</b>
	• Lack of quality assurance and testing procedures	50%
	• Product development tools have inherent bugs	39%
	• Incorrect permissions	19%
	• Back end systems	16%

The pressure to meet deadlines leads to inadequate security testing, which causes the very vulnerabilities that companies seek to avoid.



## Vulnerabilities and quality issues are a result of the lack of consistent use of secure software development life cycle (SSDLC) practices.

Over 33 percent of the industry is not using accepted SSDLC practices, and 60 percent say their companies have a lack of understanding or training on secure coding practices.

Does your organization follow an internally or externally published Secure Software Development Life Cycle (SDLC) process for automotive software/technology/components?	• Yes, internally	36%
	• Yes, externally	29%
	• No	36%

Sixty percent of respondents say a lack of understanding/training on secure coding practices leads to vulnerabilities in automotive software/technology/components. Fifty-five percent cite accidental coding errors.

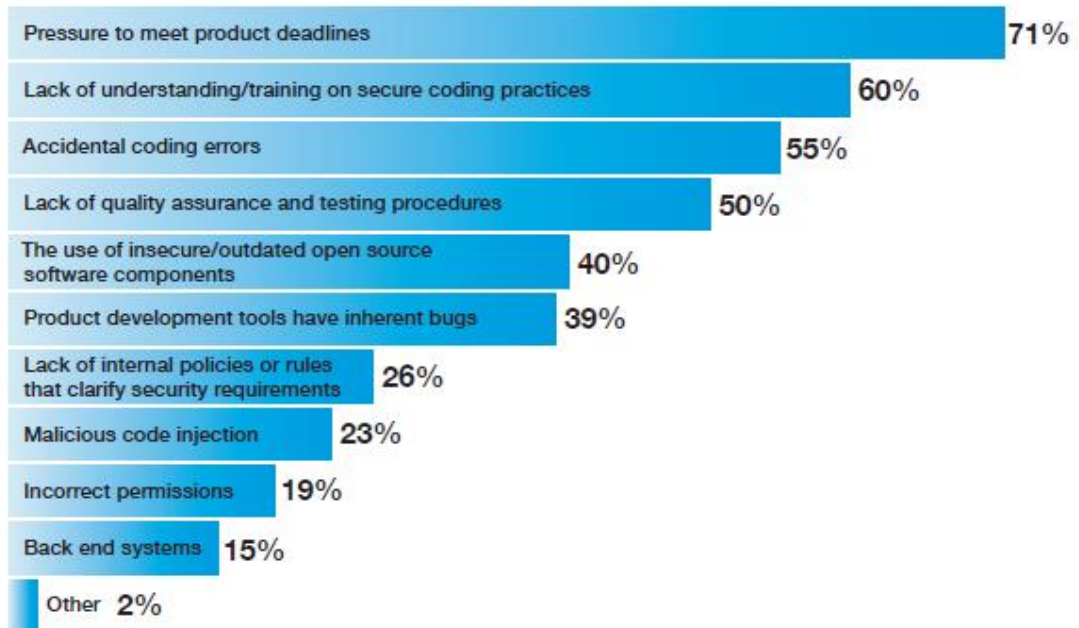


Figure 7. What are the primary factors that lead to vulnerabilities in automotive software/technology/components?







## The industry's most common security activities are security patch management, penetration testing, and dynamic security testing (DAST).

Respondents state the most common techniques to secure automotive technologies are security patch management (61 percent), penetration testing (56 percent), and dynamic security testing/DAST (49 percent). Interestingly, these are all techniques used at later stages of the life cycle.

This is another illustration of the general theme that cybersecurity is not being fully integrated throughout the system development life cycle—in particular, at the early requirements, design, and testing and development phases.

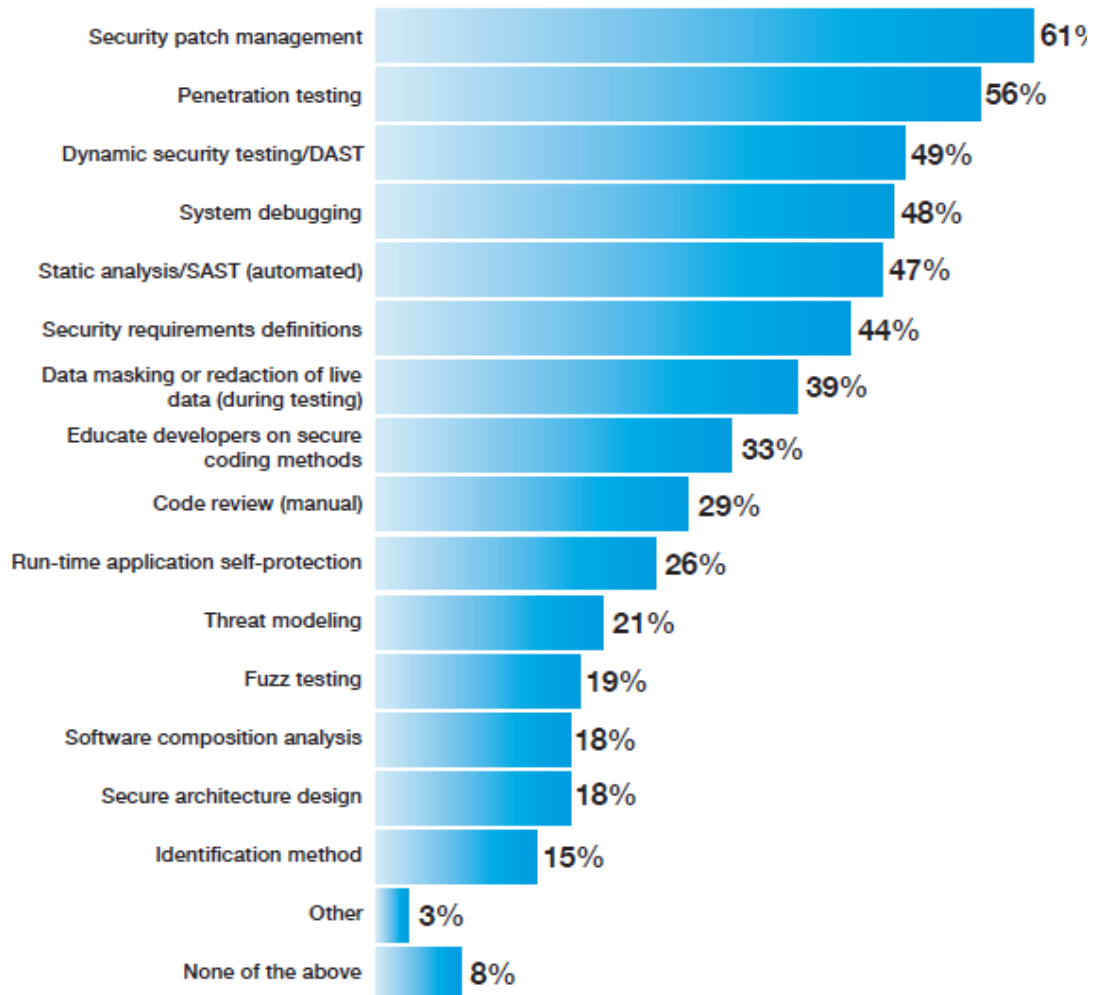


Figure 8. What activities does your company use to secure automotive software/technology/components?

# Supply Chain and Third-Party Component Challenges

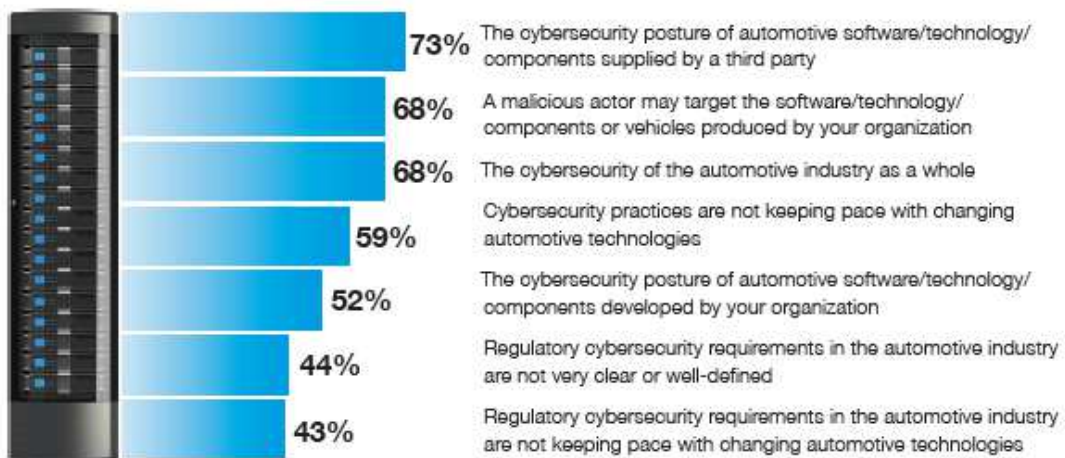
The automotive industry's complex and disparate supply chain is a major culprit in causing quality issues rendering security vulnerabilities. The frequent integration of third-party components, software, communications protocols, and applications often introduces threat vectors that OEMs must address. Several key takeaways are related to these factors.



## Vulnerabilities in the automotive supply chain present a major risk.

Seventy-three percent of respondents are very concerned about the cybersecurity posture of automotive technologies supplied by third parties. Sixty-eight percent are also very concerned about the cybersecurity posture of the industry as a whole.

Only 44 percent say their organizations impose cybersecurity requirements for products provided by upstream suppliers. A target initiative for manufacturers should be to develop appropriate security requirements along with other technical requirements for suppliers' software, hardware, and systems.



**Figure 9.** Very high concerns about cybersecurity practices and posture  
1 = not concerned to 10 = very concerned, 7+ responses presented



## Education on secure coding methods is not being prioritized.

Only 33 percent of respondents say their organizations educate developers on secure coding methods. Sixty percent say a lack of understanding or training on secure coding practices is a primary factor that leads to vulnerabilities.

What activities does your organization employ to secure automotive software/technology/components?	Percentage
Educate developers on secure coding methods	33%

# Conclusions

---

Survey respondents show a significant awareness of the cybersecurity challenges facing them and a desire to improve, tempered by concerns that they do not feel empowered to raise these issues to senior management. Respondents have an excellent understanding of perhaps the most important tenet of the cybersecurity discipline: engaging in cybersecurity throughout product development.

Finding the right combination of people, processes, and technology is the key to success. Solutions exist to deepen the ability of security professionals currently engaged in security initiatives as well as those new to the process of developing an efficient and effective approach to security, such as these resources:

- SAE J3061™ *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* describes a cybersecurity process framework from which an organization can develop an internal cybersecurity process to design and build cybersecurity into vehicle systems.
- The National Institute of Science and Technology (NIST) is a valuable and free resource for security knowledge and best practices (e.g. the [NIST Special Publication 800 series](#)).
- The [Building Security In Maturity Model \(BSIMM\)](#) and the [Synopsis Automotive Security resource page](#) can help organizations develop a security initiative and meet security, safety, reliability, and compliance requirements for automotive software.

These solutions advocate developing and utilizing a risk-based, process-driven approach that binds cybersecurity to the entire product development life cycle and the secure software development life cycle.

Cybersecurity training is also a critical investment that not only targets one pain point respondents shared in the survey but also pays dividends far into the future, helping to build a culture of security throughout an enterprise.

The automotive industry also has resources to enhance knowledge of emerging security issues and trends, develop professional networks, and contribute to industry-wide security.

- The [Automotive Information Sharing and Analysis Center \(Auto-ISAC\)](#) is a valuable forum for security professionals to share and analyze intelligence about emerging cybersecurity risks to the vehicle, and to collectively enhance automotive industry cybersecurity.
- [SAE International](#) has several cybersecurity groups developing standards, guidelines, and best practices, provides professional development training, and hosts conferences and events to keep the industry abreast of the state of the practice.

The concerns about supply chain risks noted in this report can be addressed or even mitigated by paying close attention to the requirements phase of the development life cycle. This may involve working closely with suppliers to identify weaknesses in the design or architecture of relevant components. Additional assurances can be achieved by conducting periodic reviews of suppliers' cybersecurity processes or imposing cybersecurity assurance requirements on supplier agreements.

Cybersecurity shouldn't be viewed as a cost center and tacked on at the end of production, but instead should be programmed into every step of the systems engineering process that guides the entire product development life cycle—notably, the secure software development life cycle (SSDLC). Automotive companies can enjoy a wide range of solutions through guidance, best practices, and standards that have already been developed in other industries.

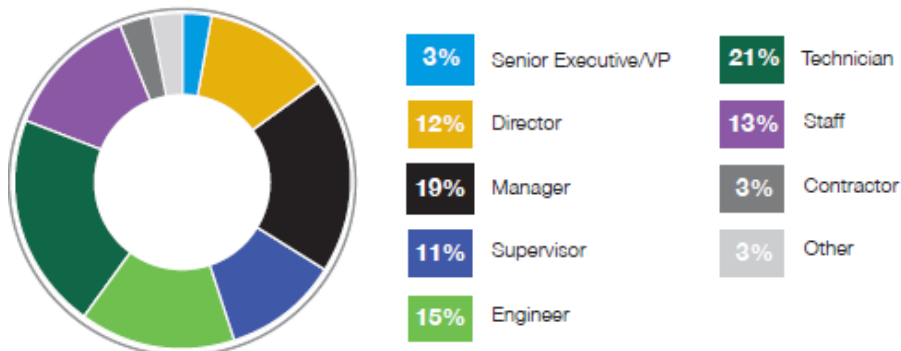
This rigorous approach to cybersecurity is vital to achieve enhanced safety while ensuring security, quality, and rapid time to market.

# Methods

A sampling frame of 16,900 IT security practitioners and engineers in the automotive industry were selected as participants in this survey. To ensure knowledgeable responses, all respondents are involved in contributing to or assessing the security of an automotive component. Table 1 shows 677 total returns. Screening and reliability checks required the removal of 84 surveys. Our final sample consisted of 593 surveys, or a 3.7 percent response rate.

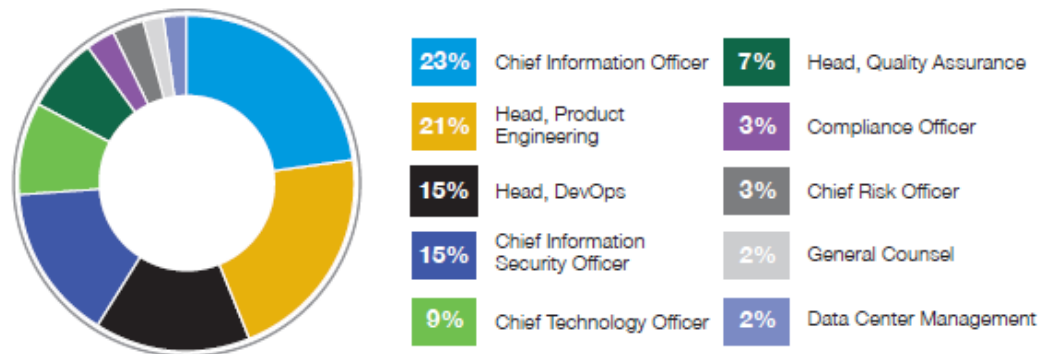
Table 1. Sample response	Freq.	Pct%
• Total sample frame	16,900	100.0%
• Total returns	677	4.3%
• Rejected surveys	84	0.6%
• Final sample	593	3.7%

Pie Chart 1 reports the respondents' position in participating organizations. By design, more than half (60 percent) hold engineer or higher-ranked positions.



**Pie Chart 1.** Current position within the organization

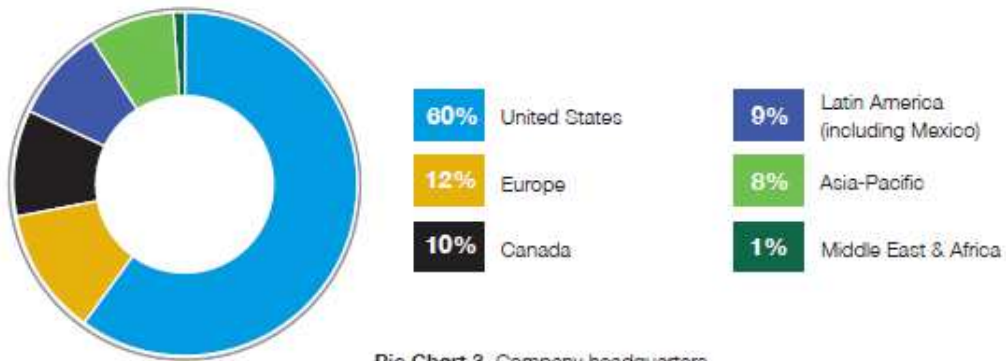
As shown in Pie Chart 2, 23 percent of respondents report to the chief information officer, 21 percent report to the head of product engineering, 15 percent report to the head of DevOps, and 15 percent report to the chief information security officer.



**Pie Chart 2.** Primary person you or your leader reports to

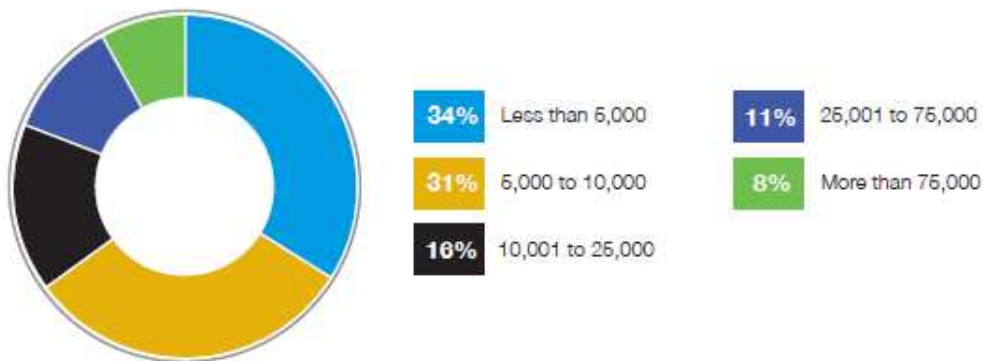


As shown in Pie Chart 3, the majority of respondents' organizations (60 percent) are headquartered in the United States. Another 12 percent have headquarters in Europe, and 10 percent are located in Canada.



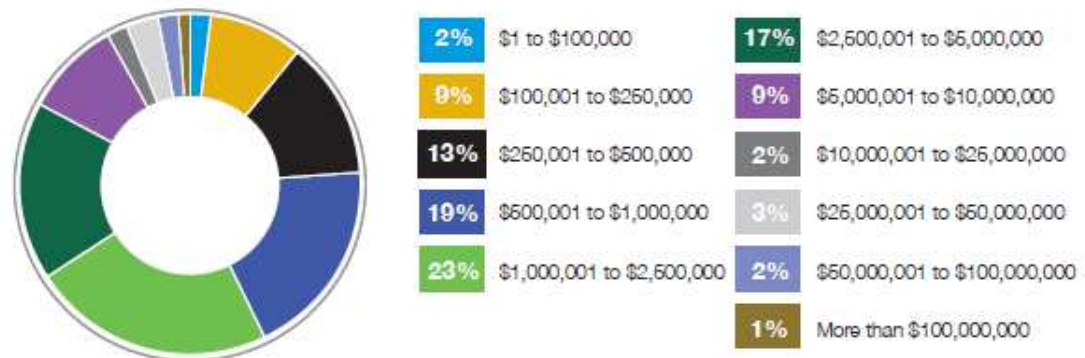
**Pie Chart 3.** Company headquarters

As shown in Pie Chart 4, 66 percent of respondents are from organizations with a global headcount of more than 5,000 employees.



**Pie Chart 4.** Worldwide headcount of the organization

When asked to choose the range that best approximates the total investment in terms of technologies, personnel, managed or outsourced services, and other cash outlays, 57 percent of respondents said their organizations are spending over \$1 million, as shown in Pie Chart 5.



**Pie Chart 5.** Spending on automotive component security each year. Extrapolated value \$6,098,000

## Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of IT security practitioners and engineers in the automotive industry who are involved in contributing to or assessing the security of an automotive component. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.



## A.3 Photos from the OSS.5 Europe Conference World-Café Session (Moderation of a Break-Out Session) (4 Pages)

**OSS.5 EUROPE**

**ICEBREAKER**  
WEDNESDAY, SEPTEMBER 25

**EVENT DAY 1**  
THURSDAY, SEPTEMBER 26

**EVENT DAY 2**  
FRIDAY, SEPTEMBER 27

Navigation icons: Home, People, Document, Share

Session categories:

- ALL SESSIONS
- NETWORKING
- FAIL-OPERATIONAL
- FUNCTIONAL SAFETY
- CONNECTIVITY + COOPERATIVE SAFETY
- CYBERSECURITY
- ARCHITECTURES
- OPERATIONAL SAFE SYSTEMS
- PRESENTATIONS
- INTERACTION
- SYSTEM SAFETY
- SIMULATION + MODELLING
- TESTING AND VALIDATION
- AI + MACHINE LEARNING
- SOFTWARE SAFETY
- VERIFICATION + VALIDATION
- HAZARD ANALYSIS + RISK ASSESSMENT
- SAFETY CASES + ARGUMENTATION
- OPERATIONAL SAFETY
- SOTIF
- NORMS + STANDARDS

**11:40 - 13:10** INTERACTION

START WORLD CAFE ROUND (1) (2) (3)

We start with the first 3 rounds, each round is about 35 minutes long. After each round, participants change the roundtable, according to the arrangement of your coffee cups on their name badge.

**11:40 - 15:10** WORLD CAFÉS SESSIONS - OSS.5 EUROPE

**11:40 - 15:10** (4) CYBERSECURITY CAFÉ

**CYBERSECURITY**

**FUNCTIONAL SAFETY**

**INTERACTION**

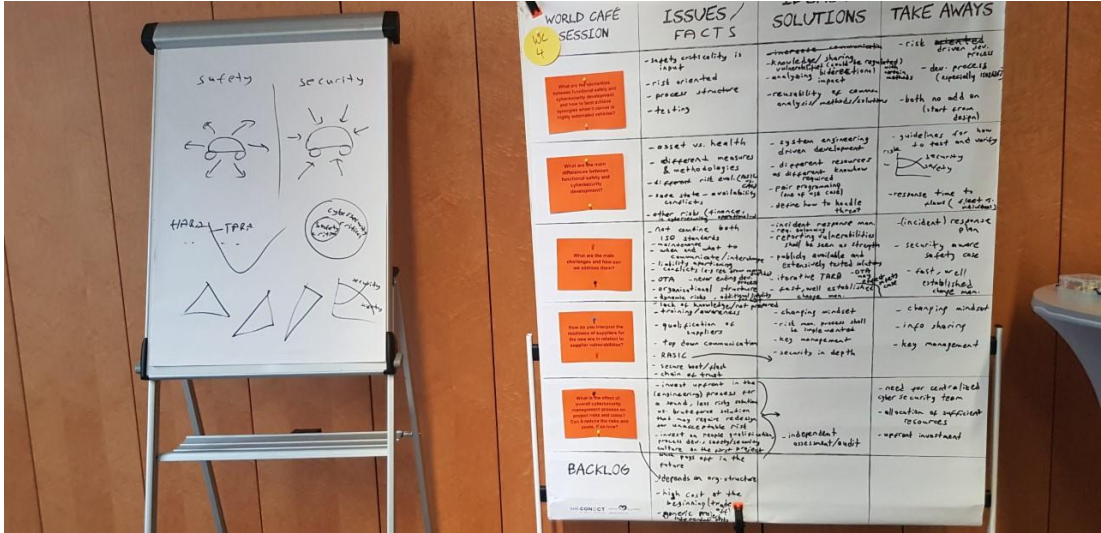
**SYSTEM SAFETY**

**The Golden Triangle between Cybersecurity, ISO 26262, and ISO/PAS 21448 for Highly Automated Vehicles**

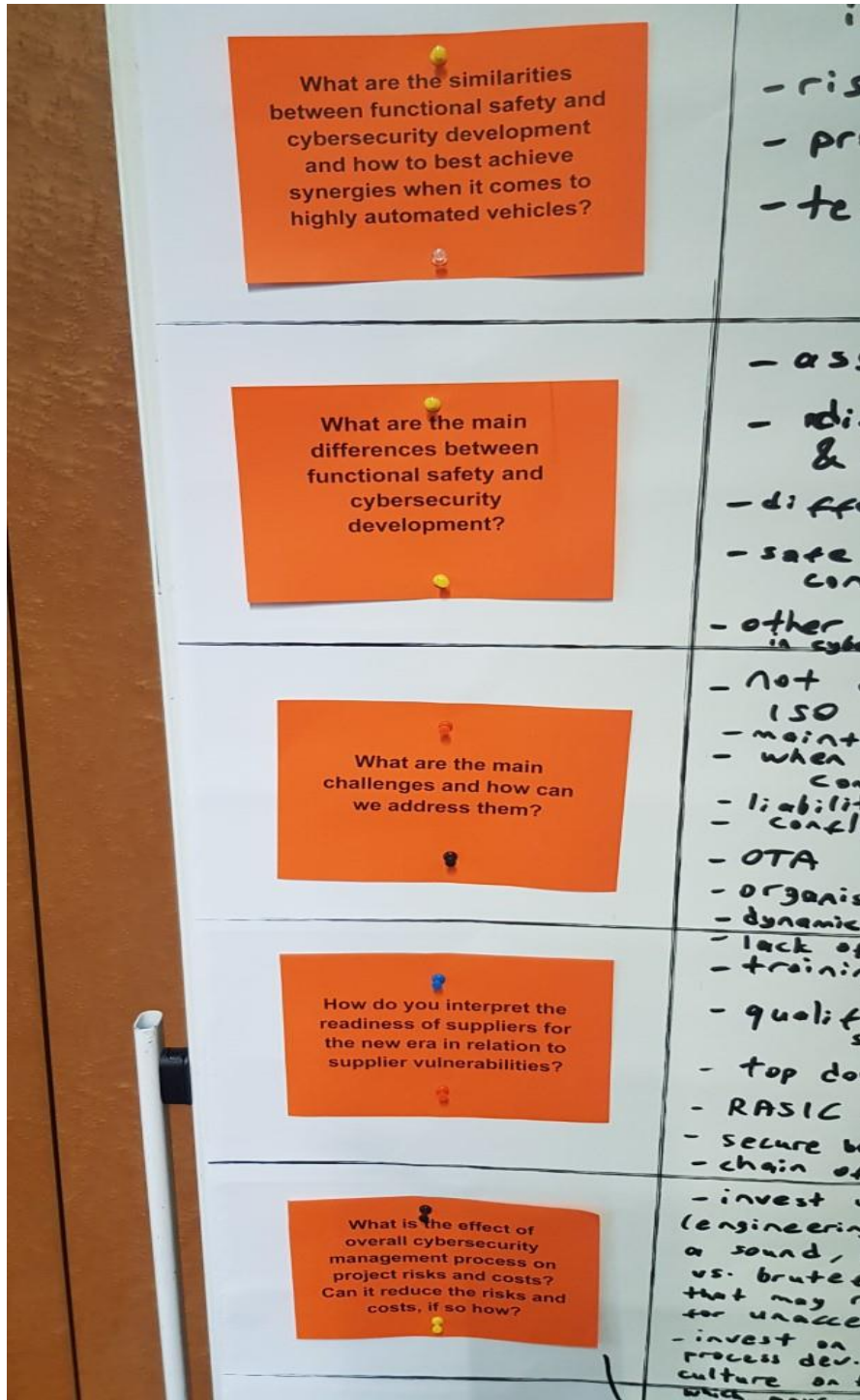
**Emrah Eminoglu**  
Global Functional Safety Manager  
Magna Powertrain GmbH

- What are the similarities between functional safety and cybersecurity development and how to best achieve synergies when it comes to highly automated vehicles?
- What are the main differences between functional safety and cybersecurity development?
- What are the main challenges and how can we address them?
- How do you interpret the readiness of suppliers for the new era in relation to supplier vulnerabilities?
- What is the effect of overall cybersecurity management process on project risks and costs? Can it reduce the risks and costs, if so how?



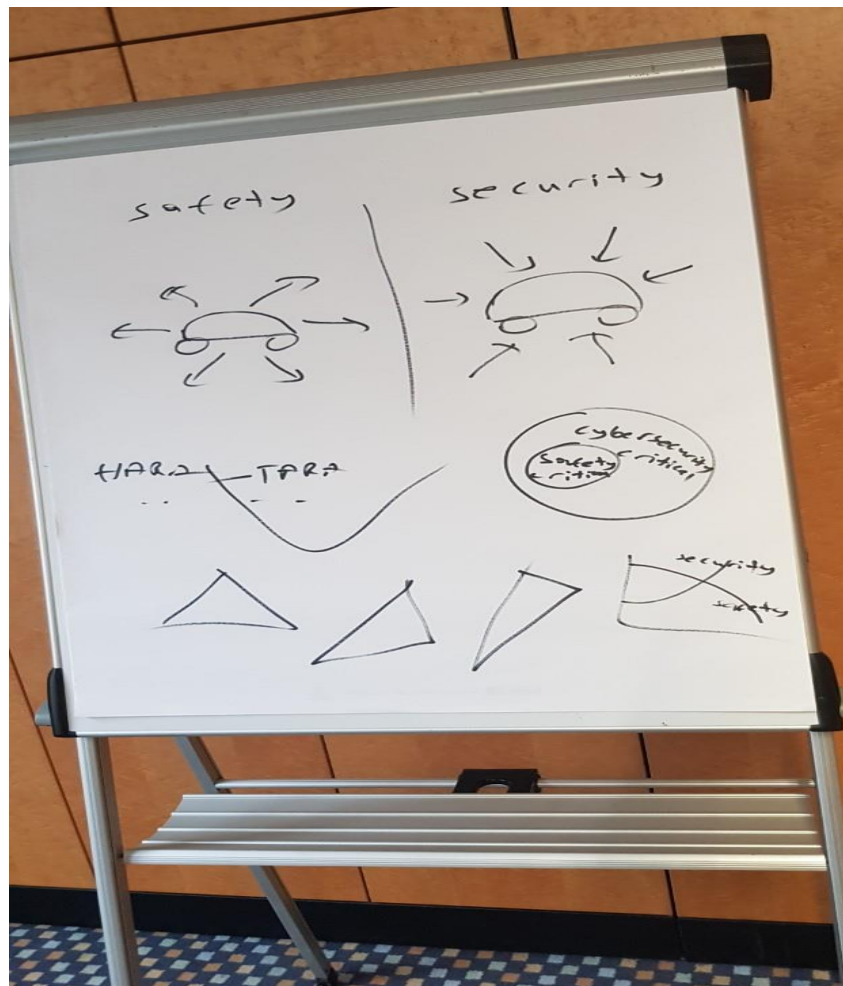


WORLD CAFE SESSION	ISSUES / FACTS	IDEAS & SOLUTIONS	3 KEY TAKE AWAYS
<p>What are the similarities between functional safety and cybersecurity development, and how to best achieve synergies when it comes to highly automated vehicles?</p>	<ul style="list-style-type: none"> <li>- safety criticality is input</li> <li>- risk oriented</li> <li>- process structure</li> <li>- testing</li> </ul>	<ul style="list-style-type: none"> <li>- increase communication</li> <li>- knowledge/sharing (especially regulatory)</li> <li>- analyzing interdependencies</li> <li>- reusability of common analysis/methods/solutions</li> </ul>	<ul style="list-style-type: none"> <li>- risk oriented driven security process (especially needed)</li> <li>- dev. process methods (especially needed)</li> <li>- both no add on (start from design)</li> </ul>
<p>What are the main differences between functional safety and cybersecurity development?</p>	<ul style="list-style-type: none"> <li>- asset vs. health</li> <li>- different measures &amp; methodologies</li> <li>- different risk eval. (ASIC vs. SW)</li> <li>- state - availability</li> <li>- other risk (finance, cybersecurity operational)</li> </ul>	<ul style="list-style-type: none"> <li>- system engineering driven development</li> <li>- different resources as different knowhow required</li> <li>- pair programming (one of use case)</li> <li>- define how to handle threat</li> </ul>	<ul style="list-style-type: none"> <li>- guidelines for how risk to best and verify security</li> <li>- response time to plans (electronic)</li> </ul>
<p>What are the main challenges and how can we address them?</p>	<ul style="list-style-type: none"> <li>- not combine both ISO standards</li> <li>- maintain what to communicate/interchange</li> <li>- conflicts (e.g. real time vs. OTA)</li> <li>- OTA - near ending design</li> <li>- organizational structure</li> <li>- dynamic risks - additional/ability</li> <li>- lack of knowledge/not prepared</li> <li>- bringing awareness</li> </ul>	<ul style="list-style-type: none"> <li>- incident response man. - reporting vulnerabilities shall be seen as strength</li> <li>- publicly available and extensively tested safety</li> <li>- iterative TARA - fast well established change man.</li> </ul>	<ul style="list-style-type: none"> <li>- (incident) response plan</li> <li>- security aware safety case</li> <li>- fast, well established change man.</li> </ul>
<p>How do you interpret the requirement of suppliers for the new org in relation to supplier awareness?</p>	<ul style="list-style-type: none"> <li>- qualification of suppliers</li> <li>- top down communication</li> <li>- RASIC</li> </ul>	<ul style="list-style-type: none"> <li>- changing mindset</li> <li>- risk man. process shall be implemented</li> <li>- key management</li> <li>- security in depth</li> </ul>	<ul style="list-style-type: none"> <li>- changing mindset</li> <li>- info sharing</li> <li>- key management</li> </ul>
<p>What is the effect of overall cybersecurity management process on product risks and costs? Can it reduce the costs and costs, if so how?</p>	<ul style="list-style-type: none"> <li>- secure boot/fleet</li> <li>- chain of trust</li> <li>- invest upfront in the (engineering) process for a sound, less risky solution</li> <li>- invest in people qualification</li> <li>- process dev. cybersecurity culture in the organization</li> </ul>	<ul style="list-style-type: none"> <li>- invest upfront in the (engineering) process for a sound, less risky solution that may require re-design for unacceptable risk</li> <li>- invest in people qualification</li> <li>- process dev. cybersecurity culture in the organization</li> <li>- independent assessment/audit</li> </ul>	<ul style="list-style-type: none"> <li>- need for centralized cyber security team</li> <li>- allocation of sufficient resources</li> <li>- upfront investment</li> </ul>
<p>BACKLOG</p>	<ul style="list-style-type: none"> <li>- depends on org. structure</li> <li>- high cost of the beginning stage</li> <li>- organic process</li> </ul>		





<p>How do you interpret the readiness of suppliers for the new era in relation to supplier vulnerabilities?</p>	<ul style="list-style-type: none"> <li>- organisational structure</li> <li>- dynamic risks, additional liability</li> <li>- lack of knowledge/not prepared</li> <li>- training/awareness</li> <li>- qualification of suppliers</li> <li>- top down communication</li> <li>- RASIC</li> <li>- secure boot/fresh</li> <li>- chain of trust</li> </ul>	<ul style="list-style-type: none"> <li>- fast, well established change man.</li> <li>- changing mindset</li> <li>- risk man. process shall be implemented</li> <li>- key management</li> <li>- security in depth</li> </ul>	<ul style="list-style-type: none"> <li>- established change man.</li> <li>- changing mindset</li> <li>- info sharing</li> <li>- key management</li> </ul>
<p>What is the effect of overall cybersecurity management process on project risks and costs? Can it reduce the risks and costs, if so how?</p>	<ul style="list-style-type: none"> <li>- invest upfront in the (engineering) process for a sound, less risky solution vs. brute force solution that may require redesign for unacceptable risk</li> <li>- invest on people qualification process dev. safety/security culture on the start project will pay off in the future</li> </ul>	<ul style="list-style-type: none"> <li>- independent assessment/audit</li> </ul>	<ul style="list-style-type: none"> <li>- need for centralized cyber security team</li> <li>- allocation of sufficient resources</li> <li>- upfront investment</li> </ul>
<p><b>BACKLOG</b></p>	<ul style="list-style-type: none"> <li>- depends on org. structure</li> <li>- high cost at the beginning (trade off)</li> <li>- generic project independent</li> </ul>		



## A.4 Interaction and Communication Channels between Functional Safety and Cybersecurity (2 Pages)

Figure 38-41 are derived based on SAE J3061.

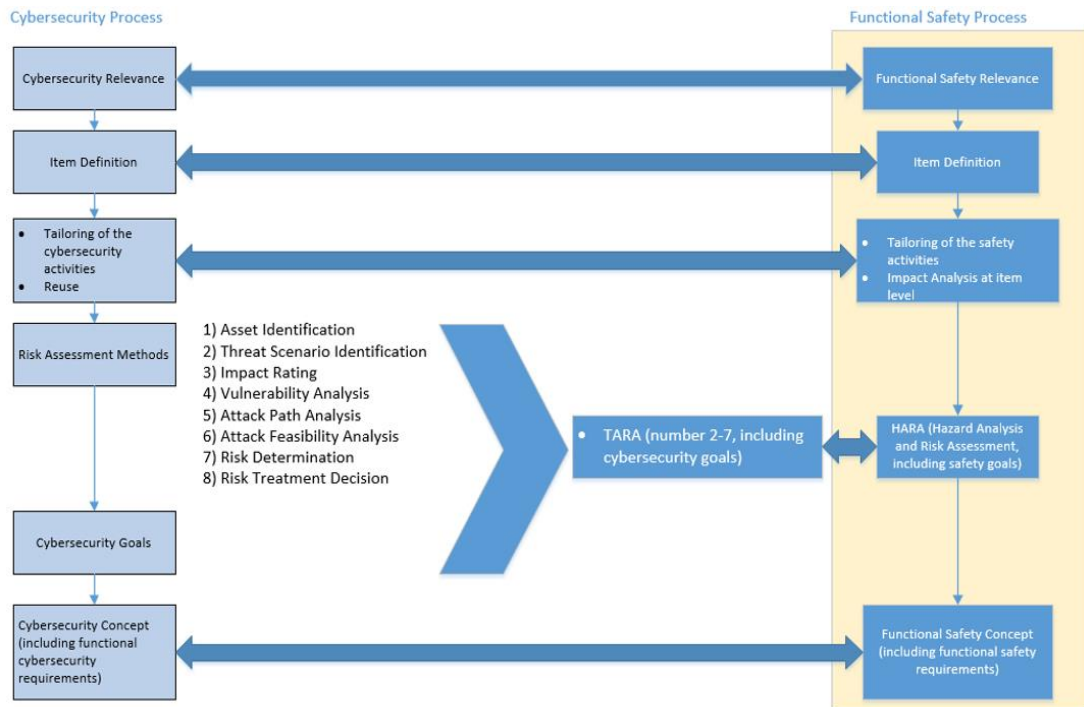


Figure 38: Concept level comparison of the cybersecurity and functional safety development

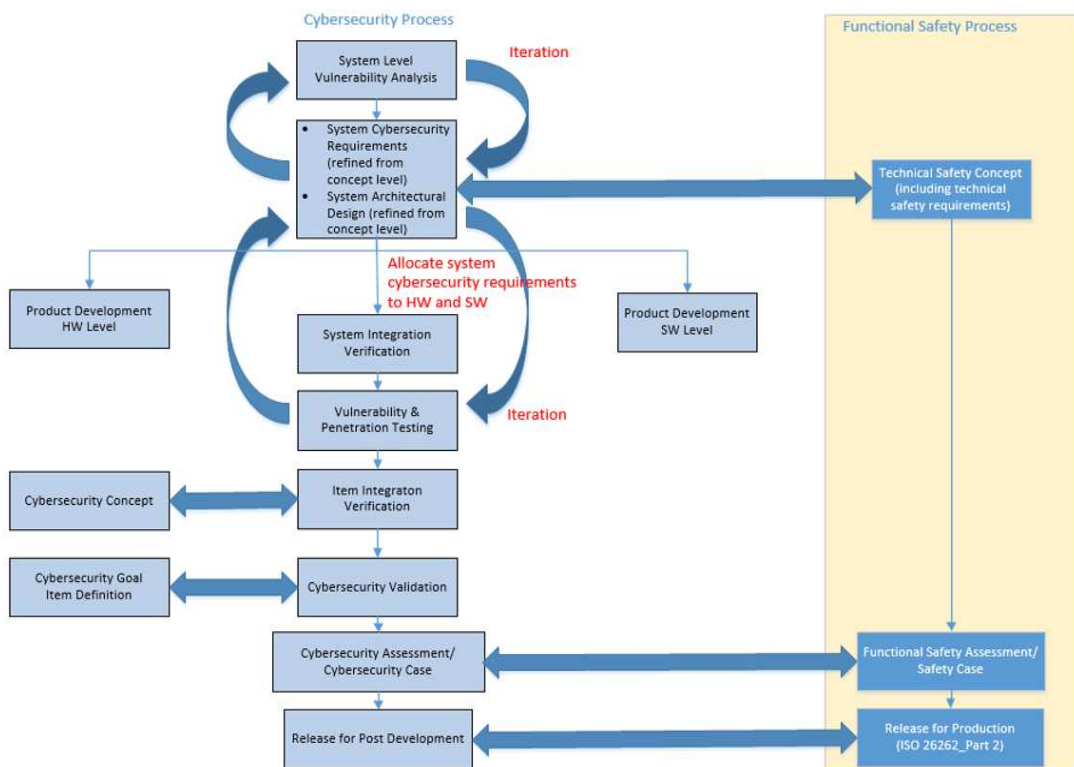


Figure 39: System level comparison of the cybersecurity and functional safety development



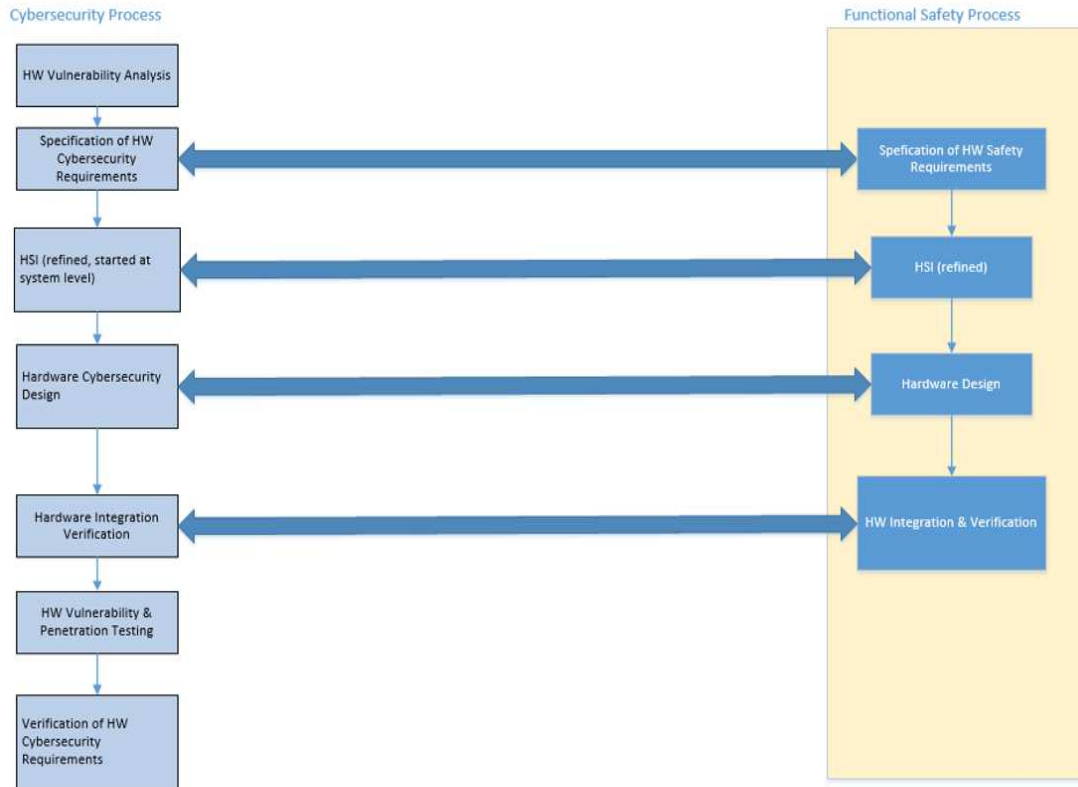


Figure 40: Hardware level comparison of the cybersecurity and functional safety development

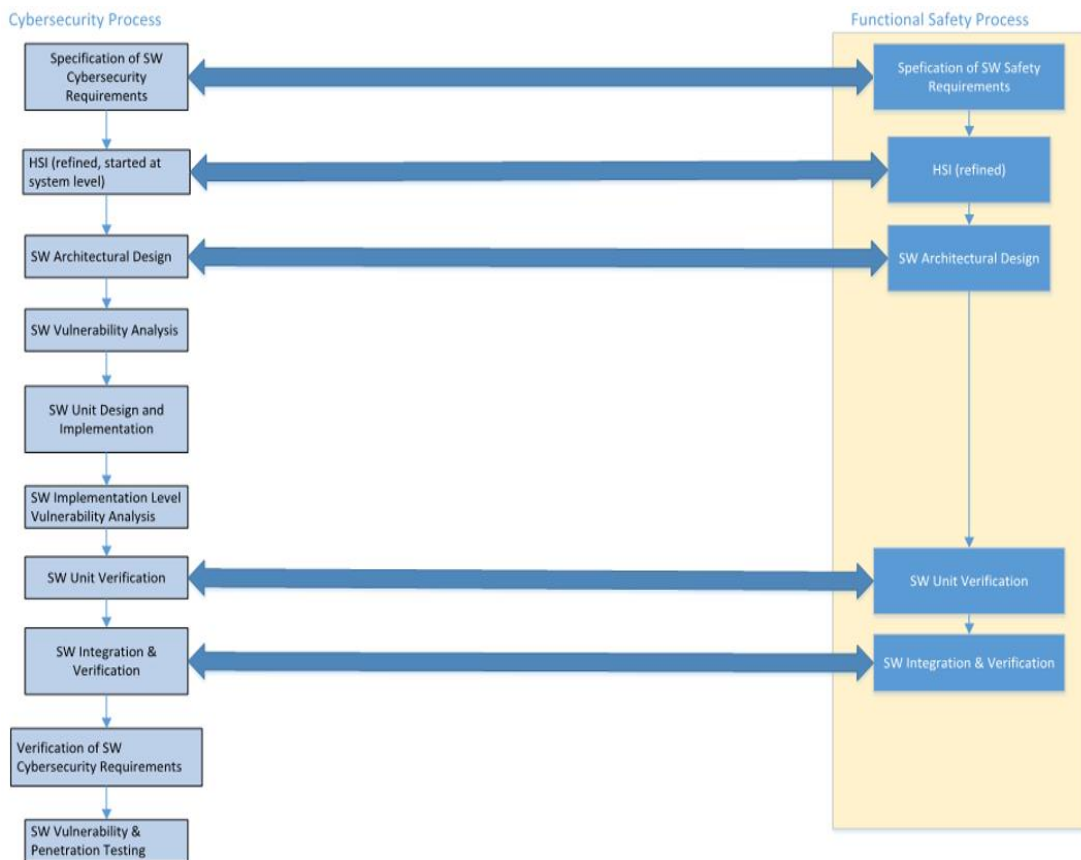


Figure 41: Software level comparison of the cybersecurity and functional safety development