Integrated design for tackling safety and security challenges of smart products and digital manufacturing

Andreas Riel, Christian Kreiner, Georg Macher, Richard Messnarz

Elsevier Editorial System(tm) for CIRP Annals - Manufacturing Technology
Manuscript Draft

Manuscript Number: 2017-Dn-09R2

Title: Integrated design for tackling safety and security challenges of smart products and digital manufacturing

Article Type: STC Dn

Keywords: design; integration; safety

Corresponding Author: Dr. Andreas Erik Riel, Ph.D.

Corresponding Author's Institution: Grenoble Institute of Technology

First Author: Andreas Erik Riel, Ph.D.

Order of Authors: Andreas Erik Riel, Ph.D.; Christian J Kreiner, Ph.D.; Georg Macher, Ph.D.; Richard Messnarz, Ph.D.

Abstract: The Internet of Things (IoT) is the key facilitator for digital manufacturing (Industry 4.0, Cyber-physical Systems), as well as for smart, intelligent products, services and processes. In the IoT, increasingly many product and process functions become safety-critical and exposed to IT security attacks. This adds tremendous complexity to product and process design, which this paper shows by using the automotive sector as a particularly challenging example. The article proposes a new logic and method for tackling the major challenges of design for functional safety and IT security which is essentially based on reducing the design solutions' complexities by integration.

This is a very important and emerging area in design under 'design for security'.

No changes.

Section 3 should also include latest research on cyber-secure industrial control systems.

We extended Section 3 by one paragraph elaborating on the CPS and ICS and citing three of the still very few key references on the subject of the integration of cybersecurity and functional safety in the design of ICS (new references [5,6,7]). To make the transition to the automotive sector, we have added a statement explaining the since industry is still the min driving force in the cybersecurity/safety integration, most relevant works can be found in sector-specific research and industry practice publications.

You need to discuss role of people, hardware and software in the security of ESCL.

We interpret this as a supporting remark, since we indicate in several places that the key idea and objective of our research is to enable an integrated design view on cybersecurity and functional safety aspects. Integrated design is essentially about enabling human experts from several different fields to collaborate efficiently in the design process, which is exactly what we search to facilitate by our method. Furthermore, in table 1 we established a vehicular vocabulary leveraging the communication between cybersecurity and safety experts.

Also link between safety and cyber security is well presented. Good work.

No changes.

The paper introduces a new logic to drive safety and security concerns in cyber-physical systems. The proposed method is applied on an industrial case.

No changes.

The promised methodology is too shallow by far; New logic engineering methods for CPS.

Deliberately and due to the requirements we were having for this research, we have based our method and our related research methodology on two emerging industry standards. Therefore, it is true that what we propose is rather a novel method than a profound methodology. We also agree to the reviewer that this methods represents a now logic of applying existing engineering methods for achieving integration n design. In order to take this explicitly into account, we have replaced the word “methodology” both in the abstract and the body of the text by “method” and/or “new logic of engineering methods”.

Contents lists available at SciVerse ScienceDirect

CIRP Annals Manufacturing Technology

Journal homepage: www.elsevier.com/locate/cirp

Integrated design for tackling safety and security challenges of smart products and digital manufacturing

Andreas Riel[1] (2), Christian Kreiner[2], Georg Macher[3], Richard Messnarz[4]

[1] *Grenoble Alpes University, G-SCOP Laboratory, Grenoble, France*
[2] *Graz University of Technology, Institute for Technical Informatics, Graz, Austria*
[3] *AVL LIST GmbH, Graz, Austria*
[4] *ISCN GmbH, Graz, Austria*

The Internet of Things (IoT) is the key facilitator for digital manufacturing (Industry 4.0, Cyber-physical Systems), as well as for smart, intelligent products, services and processes. In the IoT, increasingly many product and process functions become safety-critical and exposed to IT security attacks. This adds tremendous complexity to product and process design, which this paper shows by using the automotive sector as a particularly challenging example. The article proposes a new logic and method for tackling the major challenges of design for functional safety and IT security which is essentially based on reducing the design solutions' complexities by integration.

design; integration; safety

1. Introduction

Digital manufacturing and smart, completely customizable product-service systems go hand in hand with each other in what is widely called the fourth industrial revolution (Industry 4.0). The key element enabling and driving these paradigms is the high integration of complex interconnected embedded systems of electronics and software in traditional manufacturing systems and products. Through this integration, such cyber-physical systems (CPS) are increasingly taking over control of essential value-added functions. In applications like automotive, aeronautics, medical, nuclear power plants, etc. such functions are often safety-critical, i.e. any failures linked to these functions might harm human health. The same applies to manufacturing environments where high levels of automation and autonomy of machines and robots lead to the necessity of taking safety criticality into account in the very design of Industrial Control Systems (ICS) and their operating environments.

At the same time, safety-critical embedded systems are increasingly part of networks of systems which interact among each other in order to provide added-value functions on system level. This interaction takes place via computer networks which are either private to the system, or linked to an information technology (IT) cloud, or both. A key challenge of such networks is the assurance of cybersecurity, i.e. the protection of these networks against malicious intrusions aiming at modifying the intended behaviour of the network and/or the linked devices. The Industrial Internet of Things (IIoT) and the growing reliance on automation and big data have rendered cybersecurity the biggest risk factor in manufacturing [2].

While not every secure system is necessarily safety-critical, the opposite always holds true: safety-critical systems have to be secure as well, otherwise the built-in safety features might be compromised by intruders. In several industry sectors, though, functional safety and cybersecurity have evolved separately from each other as their treatment in design requires very special knowledge.

This paper uses the example of an automotive electronic steering column lock system (ESCL) to propose a method and logic of integrating functional safety and cybersecurity in the early design, i.e. the requirements and constraints analysis phase, of CPS. Section 2 explains the context, the research objectives and methodology. Section 3 introduces essential related work in the automotive domain. Section 4 suggests an integrated approach to safety and cybersecurity requirements elicitation applied to the ESCL. Section 5 builds on this approach in order to identify trust boundaries in the system as a fundamental basis for the design of safe and secure CPS. Finally, section 6 concludes with a summary of the paper's key contributions and an outlook.

2. Target and methodology

Designing CPS increasingly requires integrated design methods [3] due to the high degree of dependability of these CPS in terms of their functional safety, cybersecurity, reliability, availability, integrity, maintainability and other essential system properties [4]. The key objective of this research is to propose a universal actionable method of enabling the integrated design of CPS with a particular focus on the identification and evaluation of functional safety and cybersecurity requirements and constraints in the early design phases. In order to assure the required high level of industry relevance, we have had to align our method with the constraints imposed by two recent industry standards addressing the automotive domain. We actually combined the two core safety and cybersecurity requirements elicitation methods imposed by these two standards with the originally military concept of defence-in-depth as a facilitator for the integration of safety and security experts as well as electronic and software engineers. This concept uses multiple successive diverse layers of failure and/or attack prevention/detection rather than one single protective layer which therefore would have to be perfect. In the context of a larger research initiative, we applied this approach to the design of various automotive systems in collaboration with work groups composed of experts representing leading automotive tier-1 suppliers.

3. Essential related work in ICS and the automotive sector

A broad treatment of research activities in the area of cybersecurity for CPS and IPS in several application contexts can be found in [5]. Stouffer et al. [6] take a more instructive approach to explaining essential Cybersecurity aspects of ICS, however without taking into functional safety. Cybersecurity and safety integration in ICS through successive consideration of the effect of decisions is discussed in [7]. In general, we found that cybersecurity-safety integration is a very new subject that is still mainly driven by industry, which is probably why the most helpful and exhaustive published works we found are issued from in domain-specific research, in our case automotive.

CPS are considered the most important driver for innovation in the automotive domain as they are the enablers of new and improved functionalities such as steer- and brake-by-wire and advanced driver assistance systems (ADAS) leading towards the autonomous vehicle. While functional safety has been addressed quite exhaustively in the automotive domain over the last decade, cybersecurity has come up as a top design priority only recently. Research and industry practice has led to the internationally recognized functional safety standard ISO 26262 [8] which is based on the ISO 61508, the corresponding standard for industrial automation. There is no comparable standard for automotive cybersecurity yet, the SAE guideline J3061 [9] is the only published industry agreement at this stage.

In terms of essential published research, Ward et al. [10] suggest a risk assessment method for security risk in the automotive domain named threat analysis and risk assessment, based on the Hazard and Risk Analysis (HARA) specified in [8]. Roth et al. [11] and Steiner et al. [12] deal with safety and security analysis, however focus on state/event fault trees for modelling the system under development. Schmittner et al. [13] present a failure mode and failure effect model for safety and security cause-effect analysis. Bloomfield et al. [14] mention a security-informed risk assessment with a focus on a "security-informed safety case" and the impact of security on an existing safety case.

4. Integrated safety/cybersecurity requirements elicitation

Integration in design starts with the definition of a common vocabulary containing vehicular terms that can be used to foster mutual understanding of domain experts. Table 1 shows a mapping of safety and cybersecurity oriented engineering terms regarding the initial requirements analysis step, which is the HARA [8] and TARA (Threat Analysis and Risk Assessment) [9].

Table 1 Vehicular safety/cybersecurity requirements analysis terms.

Analysis		Safety	Cybersecurity
Subject	Risk	Hazard	Threat
	System inherent deficiency	Malfunction	Vulnerability
	External enabling condition	Hazardous situation	Attack
Category	Impact analysis	Severity	Threat criticality
	External risk control analysis	Controllability	Attacker skills, know-how
	Occurrence analysis	Exposure	attack resources & surfaces
Re-sult	Design goal	Safety goal	Security target
	Design goal criticality	ASIL	SecL

Thanks to this shared vocabulary it is possible to perform the first step in the safety/cybersecurity development life cycle from an integrated perspective [15]. In order to illustrate this, we will use the concrete example of an ESCL.

Modern ESCL systems provide highly representative safety and security relevant use-cases, thanks to their comparatively low system complexity, yet strong safety and security relevance. The basic function of the ESCL is the following: When the driver gets into the car, the vehicle immobilizer (IM) receives an ignition key signal. When the driver starts the car, an ignition-on message is communicated via the controller area network (CAN) bus. When this signal is received by the ESCL and the IM enables the ESCL, an electric motor moves the locking bolt and unblocks the steering column. The inverse process, locking the steering column, happens by a bolt movement by the electric motor in the opposite direction as soon as the vehicle is in standstill and the driver switches off the ignition.

From a security point of view, the system shall lock the steering column when the ESCL's diagnostic functions reveal an inconsistency of the relevant control signals, which might be the result of an attack. From a safety perspective, however, the steering column must not be locked during driving. Moreover, forcing a safety-critical system to go into a known safe-state can provide additional attack vectors if security considerations do not also cover safe-states and reactions of safety-critical systems. These considerations have been taken into account in the HARA and TARA depicted in table 2 and 3 respectively.

Table 2 HARA of the ESCL.

ID	Possible malfunction	Situation	ASIL	Safety Goal
EH_1	Unwanted actuation of steering lock	Driving at high speed, steering action required	D	SG1: Prevent unwanted locking
EH_2	No steering column locking	Vehicle parked, ignition off	QM	---

Table 3 TARA of the ESCL (based on the STRIDE threat model [16]).

ID	STRIDE function	Attack description	SecL	Related Safety Goal	ASIL
ET_1a	Spoofing	Sending keyless-go off signal, vehicle speed 0 km/h, engine off	3	SG1	D
ET_1b	Spoofing	Same as ET_1a via OTA feature	4	SG1	D
ET_2b	Denial of Service	Sending vehicle speed always > 5 mph and ignition never turned off via OTA feature	3	---	---

Based on the assumption that particular cybersecurity attacks must take place in a specific order to enable more sophisticated attacks, we propose an architectural model with several static layers of defence. Any such automotive defence layer (AutoDL) represents typical steps an attacker would have to walk through to get increasing impact on the target system. This static defence layer model, shown in Fig. 1, helps to reveal attack patterns. In the portrayed scenario, an information disclosure attack on the maintenance tool can overcome AutoDL 1 and thus enable spoofing of identity and elevation of privilege attacks. These attacks facilitate other attacks and finally result in the attack 'spoofing of commands leading to unintended locking of steering column' which violates a safety goal rated ASIL D (highest level).

The key added value of this layer-based approach lies in the facilitation of the analysis of a limited number of attack patterns rather than a huge number of potential individual attacks, some of which are not even known at the design stage. With respect to the integration of safety and security, it becomes possible to focus the TARA on the threats on the violation of the most critical safety

goals. Furthermore, the defence in depth approach allows to defend a system against any particular attack using several independent and diverse defence methods (cf. Fig. 1). If any of the layers fails to protect, then the subsequent layer is in place.

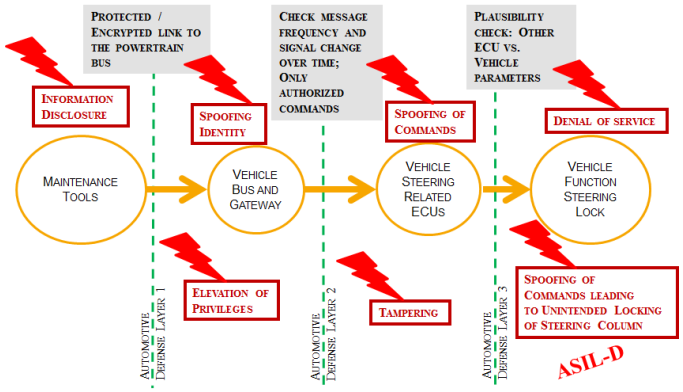


Figure 1. Static defence layers of the ESCL system [17].

In order to determine where to actually implement the individual sequential defence layers in the vehicle system architecture, designers have to analyse each system function (e.g. the ESCL's locking function) in terms of their data and signal flows against potential attack flows. Fig. 2 shows two possible attack flows through the defence layers defined for the ESCL.

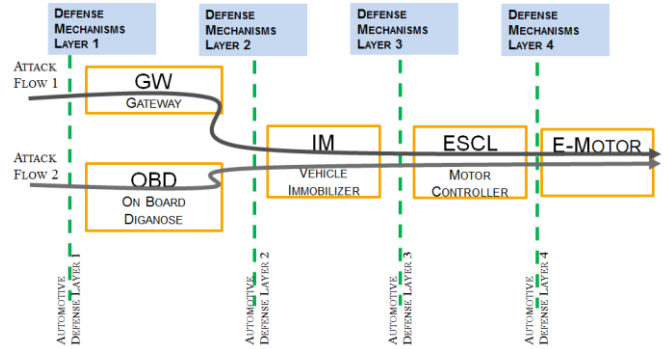


Figure 2. ESCL data flow representation including AutoDL layers [17].

The two attack scenarios depicted follow a certain data flow through the affected elements of the vehicle's system architecture. This approach is suitable for the analysis of the isolation of software functions executed on the same electronic control unit (ECU) and is based on a data flow representation.

5. Trust boundary identification

Trust boundary identification completely differs in safety and security engineering. For the safety-related aspects of automotive systems, trust boundaries are determined by a function-oriented definition of system borders where dangerous malfunctions are controlled ("item" in ISO 26262 terminology). In cybersecurity, by contrast, trust boundaries are used to describe a boundary where program execution or data protection change their levels of "trust". This term refers to any distinct boundary within which a system trusts all other sub-systems that are within this boundary. Trust boundaries can be related to privileges, integrity, control units or communication networks, and can also refer to points or attack surfaces where attackers can intervene. In order to clearly distinguish (sub)system boundaries, the term "feature definition" is used for the cybersecurity aspects of a product or system [9].

Based on the concept of the layered cybersecurity defence approach introduced earlier, we propose a way to identify trust boundaries and attack vectors via signal interfaces based on the hardware-software interface (HSI), a key development artefact of the ISO 26262 functional safety development process [8]. Defining the transition of electronic signals to software variables, the HSI represents an essential vehicular work product of the automotive system design process linking hardware and software designers. Establishing the HSI requires mutual knowledge of hardware and software components and their interactions.

Safety and/or cybersecurity relevant signals inherit their ASIL ratings from the HARA and/or their security level from the TARA. Depending on the related security level/ASIL, the signal shall be protected against cybersecurity attacks according to a defence in depth pattern as mentioned earlier in this work. The enhancing of the HSI definition with supplementary cybersecurity information and related signals provides the systematic basis to determine trust boundaries and attack vectors by focusing on signals and thus identifying controllers which can intervene with the involved signals.

To this aim, all signals required for the system are analysed. Based on this analysis, all control units having access to these signals are identified. These control units are within the same trust boundary and thus are equally trusted. The access to the trust boundary is enabled via dedicated devices (gateways) which also have connections outside the trust boundaries. The gateways are required to prevent the misuse of trust, and thus they protect the control units within a trust boundary from outside attacks. The identification of trust boundaries and gateways protecting these boundaries is both crucial and cumbersome for complex system and network structures. Using the HSI definition for this purpose, however, provides a structured and methodical pattern for the identification.

Fig. 3 depicts the block diagram of the ESCL from a safety perspective (item definition [8]). It shows the main architectural components of the ESCL. The required sensor signals are a redundant feedback channel of the bolt position (represented by the endpos signal), power supply and ignition key status information (CL30 and CL15), and vehicle status information via the CAN bus (ignition key status, vehicle speed signal, gear lever position).

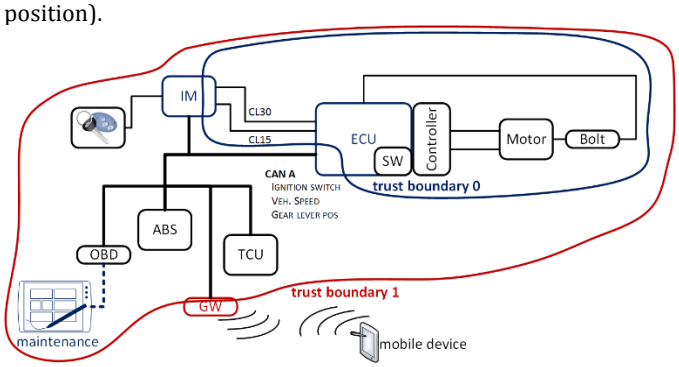


Figure 3. Block diagram of the built-in ESCL including trust boundaries.

From the HSI of the ESCL system (cf. table 4) it can be seen that the SecL of the three signals directly connected to the ESCL ECU (endpos, CL15, and CL30) are treated as 0 (not security relevant) while the three signals provided via CAN bus (thus provided from outside of trust boundary 0 in Fig. 3) have a security level of SecL =2. This results from the fact that in order to raise a security attack, these signals would have to be manipulated in the vehicle directly at the ESCL system and that these signals are within the same trust boundary 0. On the other hand, the SecL=2 indicates a possible cybersecurity vulnerability and thus requires built-in security solutions exhibiting a defence-in-depth approach.

Departing from this and based on the rough ESCL system architecture specified in the item definition depicted in Fig. 3, we

Table 4 Excerpt of the ESCL's HSI definition with relevant signals and safety/security classification for the determination of trust boundaries.

Signal name	**CL30**	**CL15**	**endpos**	**ignition key status**	**vehicle speed signal**	**gear lever position**
Description	supply voltage	ignition-starter switch	end position ESCL bolt	ignition-starter switch	actual vehicle speed	actual gear lever position
Direction	in	in	in	In	in	In
ASIL	ASIL B	ASIL B(D)	ASIL B (D)	ASIL B(D)	ASIL B(D)	ASIL B(D)
SecL	0	0	0	2	2	2
Source	ANA	ANA	DIG	CAN	CAN	CAN
...	**...**	**...**	**...**	**...**	**...**	**...**

can proceed by determining the trust levels of the ESCL components having direct access to the ESCL signals. These controllers either generate the signals directly (such as the vehicle immobilizer IM) or are connected to the same communication bus (antilock braking system ABS, on-board diagnosis connector OBD, transmission control unit TCU and wireless gateway GW). The second step identifies the inner trust boundary 0 which includes signals directly connected to the ESCL and simultaneously the gateways to the trust boundary (IM and ECU), which are required to ensure protection of the integrity of the trust boundary 0. These steps are repeated for the remaining signals to establish further trust boundaries. As can be seen in Fig. 3, trust boundary 1 covers the first layer of all signals related to the ESCL system and also includes the wireless gateway (GW), which appears as a gateway to trust-boundary 1 and therefore enables remote cybersecurity attacks on the ESCL. Additionally, if the on-board diagnostic connector (OBD) does not provide protection mechanisms for trust-boundary 1 (which is the case in current vehicle designs), any maintenance system using this connector are included in trust boundary 1 as well. This security exposure could be missed easily without performing an integrated trust boundary analysis.

Conclusion and outlook

In this paper we propose a method for the integration of functional safety and cybersecurity aspects in the early phases of industrial embedded systems design, with a focus on the automotive sector and a related case study. This sector can be considered a reference for many other industrial sectors, as it is currently undergoing a radical transformation which is mainly driven by the ubiquitous presence of smart networked embedded electronic systems, which are also at the heart of the CPS that are about to transform industrial production [18]. As increasingly many products and manufacturing processes are moving into the (I)IoT for being increasingly autonomous and smart, functional safety and cybersecurity are about to become the most essential horizontal quality characteristics. Our method is based on two core elements: (1) the introduction of a static defence layer concept that enables the identification of security attack patterns as well as the analysis of dynamic functional flows with respect to the vulnerability of architectural system elements needed to implement those functions; (2) the use of the embedded system's vehicular hardware-software interface specification to determine the trust borders which are essential for the embedded system's architectural design under safety and security constraints. Since these elements are applicable to whatever industrial embedded system, our concept is universally applicable. We have shown its feasibility using the example of a real automotive subsystem having the highest possible safety integrity level as well as a significant exposure to security attacks.

The next steps in our research are focussed on the identification of architectural design patterns that take into account both functional safety and cybersecurity by design, and can be deployed in several different industrial contexts.

Acknowledgements

The research leading to these results has received funding from the ARTEMIS Joint Undertaking under the grant agreement 621429 (project EMC^2). We also want to express our gratitude to our supporting industry partners, all members of the German SOQRATES initiative (www.soqrates.de).

References

[1] Monostori L, Kadar B, Bauernhansl T, Kondoh S, Kumara S, Reinhart G, Sauer O, Schuh G, Sihn W, Ueda K. (2016) Cyber-physical systems in manufacturing. CIRP Annals - Manufacturing Technology 65(2):621–641.
[2] BDO Manufacturing Risk Factor Report (2016) retrieved from https://www.bdo.com/insights/industries/manufacturing-distribution/2016-bdo-manufacturing-riskfactor-report on 08/01/2016.
[3] Tichkiewitch S, Véron M (1997) Methodology and product model for integrated design using a multiviews system. Annals of the CIRP 46(1):81-84.
[4] Ghemraoui R, Mathieu L, Tricot N (2009) Design method for systematic safety integration. CIRP Annals - Manufacturing Technology 58(1):161–164.
[5] Bécue A, Cuppens-Boulahia, N, Cuppens F, Katsikas S, Lambrinoudakis C (Eds.) (2016) Security of Industrial Control Systems and Cyber Physical Systems. Springer Series Vol. 9588, ISBN 978-3-319-40384-7.
[6] Stouffer K, Falco J, Scarfone K (2015) Guide to Industrial Control Systems (ICS) Security. In NIST Special Publication 800.82 (2015), available from http://dx.doi.org/10.6028/NIST.SP.800-82r2, last visited on 25/03/2017.
[7] Ellis A (2015) Integrating Industrial Control System (ICS) safety and security — A potential approach. In Proceedings of the 10th IET System Safety and Cyber-Security Conference 2015, IEEEXplore Digital Library, pp. 1-7.
[8] ISO - International Organization for Standardization (2011) ISO 26262 Road vehicles Functional Safety Part 1-10.
[9] SAE Vehicle Electrical System Security Committee (2015) SAE J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems. SAE Standard, Work-in-Progress.
[10] Ward D, Ibarra I, Ruddle A (2013) Threat Analysis and Risk Assessment in Automotive Cyber Security. SAE International Journal of Passenger Cars – Electronics & Electrical Systems 2(6):507–513.
[11] Roth M, Liggesmeyer P (2013) Modeling and Analysis of Safety-Critical Cyber Physical Systems using State/Event Fault Trees. In SAFECOMP 2013, 32nd International Conference on Computer Safety, Reliability and Security.
[12] Steiner M, Liggesmeyer P (2013) Combination of Safety and Security Analysis - Finding Security Problems that Threaten the Safety of a System. In SAFECOMP 2013, 32nd International Conference on Computer Safety, Reliability and Security.
[13] Schmittner C, Gruber T, Puschner P, Schoitsch E (2014) Security Application of Failure Mode and Effect Analysis (FMEA). In Bondavalli A, Di Giandomenico F (2014) Computer Safety, Reliability, and Security, Vol. 8666 of Lecture Notes in Computer Science, Springer International Publishing, pp. 310-325.
[14] Bloomfield R, Netkachova K, Stroud R, Gorbenko A, Romanovsky A, Kharchenko, V (2013) Security-Informed Safety: If It's Not Secure, It's Not Safe. Software Engineering for Resilient Systems, Springer Berlin Heidelberg.
[15] Macher G, Sporer H, Berlach R, Armengaud E, Kreiner C (2015) SAHARA: A security-aware hazard and risk analysis method. In Design, Automation Test in Europe Conference Exhibition (DATE), pp. 621-624.
[16] Microsoft (2005) The STRIDE Threat Model, https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx, last visited on 10/01/2016.
[17] Messnarz R, Kreiner C, Riel A (2016) Integrating Automotive SPICE, Functional Safety, and Cybersecurity Concepts: A Cybersecurity Layer Model, ASQ Software Quality Professional 3(17):13–23.
[18] Abramovici M, Göbel C, Bao Dang H (2016) Semantic data management for the development and continuous reconfiguration of smart products and systems. CIRP Annals - Manufacturing Technology 65(1):185–188.

Figure

Figure 1

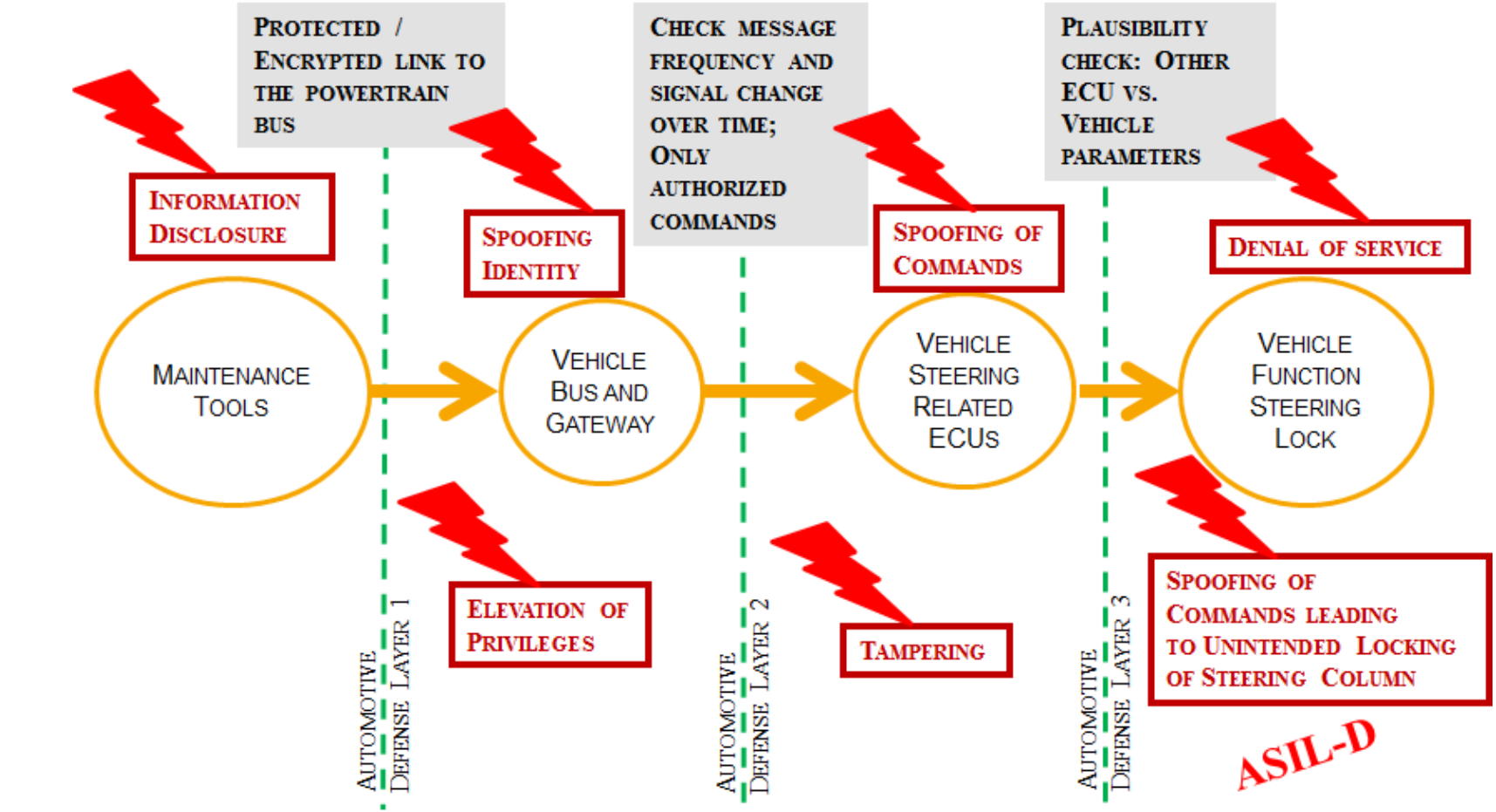


Figure 2

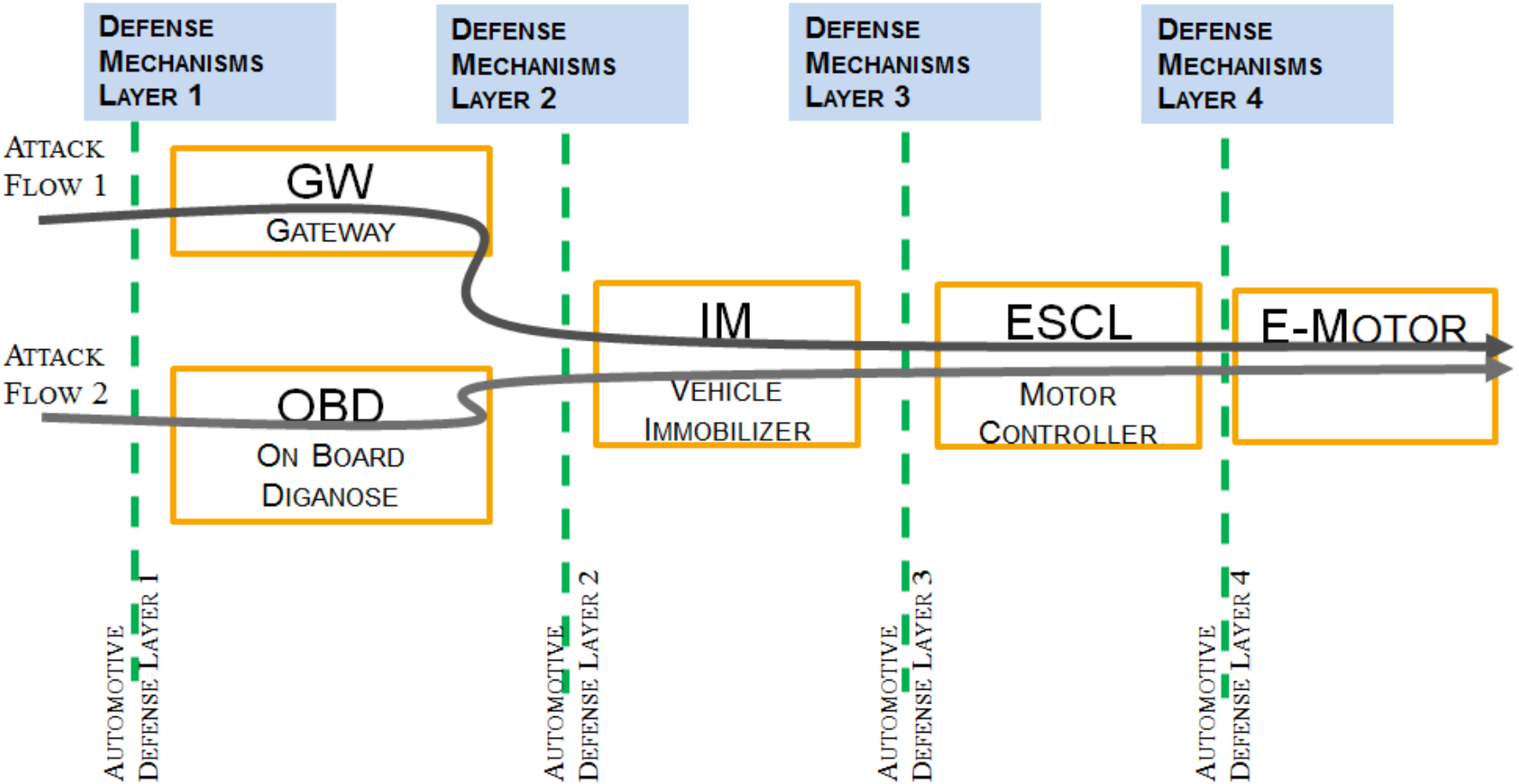
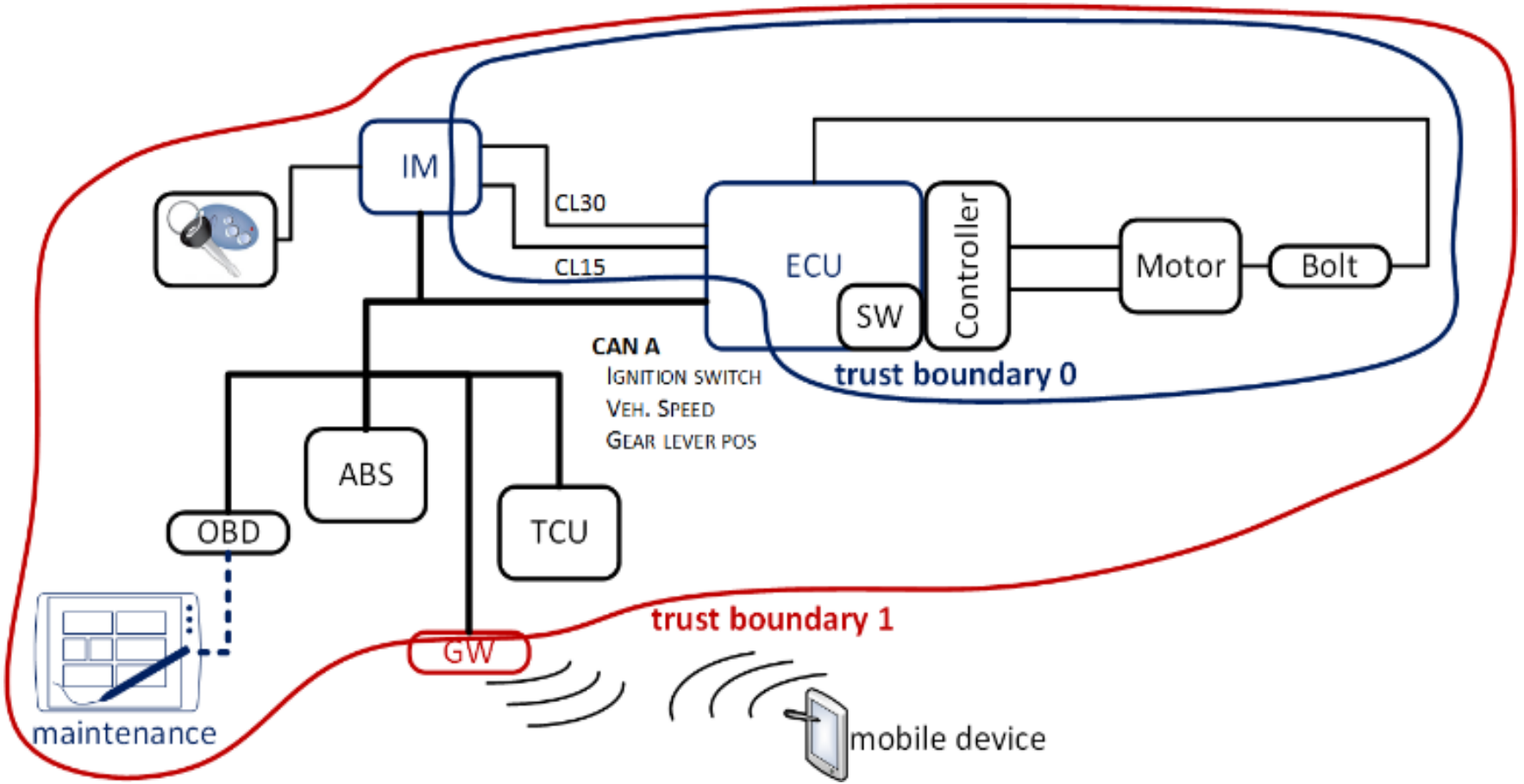

DEFENSE MECHANISMS LAYER 1
DEFENSE MECHANISMS LAYER 2
DEFENSE MECHANISMS LAYER 3
DEFENSE MECHANISMS LAYER 4
ATTACK FLOW 1
ATTACK FLOW 2
GW
GATEWAY
OBD
ON BOARD DIGANOSE
IM
VEHICLE IMMOBILIZER
ESCL
MOTOR CONTROLLER
E-MOTOR
AUTOMOTIVE DEFENSE LAYER 1
AUTOMOTIVE DEFENSE LAYER 2
AUTOMOTIVE DEFENSE LAYER 3
AUTOMOTIVE DEFENSE LAYER 4

Figure 3


IM
CL30
CL15
ECU
SW
Controller
Motor
Bolt
CAN A
IGNITION SWITCH
VEH. SPEED
GEAR LEVER POS
trust boundary 0
ABS
OBD
TCU
GW
trust boundary 1
maintenance
mobile device