An architectural approach to the integration of safety and security requirements in smart products and systems design

Andreas Riel, Christian Kreiner, Richard Messnarz, Alexander Much

To cite this version:

Andreas Riel, Christian Kreiner, Richard Messnarz, Alexander Much. An architectural approach to the integration of safety and security requirements in smart products and systems design. CIRP Annals - Manufacturing Technology, 2018, 67 (1), pp.173-176. 10.1016/j.cirp.2018.04.022 . hal-01964579

HAL Id: hal-01964579
https://hal.science/hal-01964579

Submitted on 22 Dec 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

Manuscript Number: 2018-Dn-10R2

Title: An architectural approach to the integration of safety and security requirements in smart products and systems design.

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 Kreiner, Ph.D.; Richard Messnarz, Ph.D.; Alexander Much

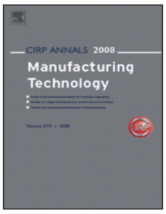
Abstract: Assuring functional safety and IT security is rapidly becoming an essential key challenge to the design of any connected smart product and industrial manufacturing system. This paper proposes an architectural approach to the integrated consideration of functional safety and IT security requirements in the design process of smart products and the (Industrial) Internet of Things (IIoT). Based on Axiomatic Design and Signal Flow Analysis, it shows that such requirements have related impacts on system architectural design choices rendering integrated design necessary to meet the desired risk reduction levels effectively and efficiently. A case study in the automotive domain is presented in order to illustrate and validate the proposed approach.

Manuscript
Click here to view linked References

Contents lists available at SciVerse ScienceDirect

CIRP Annals Manufacturing Technology

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



An Architectural Approach to the Integration of Safety and Security Requirements in Smart Products and Systems Design

Andreas Riel[1] (2), Christian Kreiner[2]†, Richard Messnarz[3], Alexander Much[4]

[1] Grenoble Alps University, G-SCOP Laboratory, Grenoble, France
[2] Graz University of Technology, Institute for Technical Informatics, Graz, Austria
[3] ISCN GmbH, Graz, Austria
[4] Elektrobit Automotive GmbH, Erlangen, Germany

Assuring functional safety and IT security is rapidly becoming an essential key challenge to the design of any connected smart product and industrial manufacturing system. This paper proposes an architectural approach to the integrated consideration of functional safety and IT security requirements in the design process of smart products and the (Industrial) Internet of Things (IIoT). Based on Axiomatic Design and Signal Flow Analysis, it shows that such requirements have related impacts on system architectural design choices rendering integrated design necessary to meet the desired risk reduction levels effectively and efficiently. A case study in the automotive domain is presented in order to illustrate and validate the proposed approach.

design; integration; safety

1. Introduction

Smart products and modern digital manufacturing systems are characterised by their integration in networks, most notably the Internet of Things (IoT) and/or Industrial Internet of Things (IIoT). Such cyber-physical systems (CPS) are increasingly taking over control of essential value-added functions which are often safety-critical, i.e. any failures linked to these functions might harm human health. This leads to the necessity of taking functional safety into account in the very design of these systems and the infrastructure they depend on. At the same time, their integration in integrated technology (IT) networks exposes CPS to cybersecurity risks, i.e. malicious intrusions aiming at modifying the intended behaviour of the network and/or the linked devices.

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, cybersecurity and related standards have evolved separately from each other as their treatment in design requires very special knowledge.

This paper uses the example of an automotive electric power steering system (EPS) to propose a systematic approach to integrating functional safety and cybersecurity in the early design based on Axiomatic Design (AD) [1] and Signal Flow Analysis (SFA) [2]. Section 2 explains the context, the research objectives and methodology. Section 3 introduces essential related work in the automotive domain. Section 4 illustrates an integrated approach to safety and cybersecurity requirements elicitation based on AD and SFA applied to the EPS. Section 5 shows the integration of this concept in the three most dominant automotive development standards through a framework. Based on this, section 6 suggests a core element for the extension of these standards to also cover requirements linked to the cyber-infrastructure. Finally, section 7 concludes with a summary of this 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]. We have published our results of the application of integrated design methods to the integration of both functional safety and cybersecurity requirements of automotive embedded systems essentially based on the hardware-software-interface (HSI) specification in [5]. In this paper, we build on this work in order to investigate how to use SFA in combination with AD in order to integrate requirements to functional safety and cybersecurity, as well as requirements linked to the cyber-infrastructure in the design of CPS. We use AD in order to enable design complexity reduction on system architecture level, while deploying SFA for the identification of the key functional requirements (FR) that are linked to the product and the larger context of the latter's cyber-infrastructure. In order to assure the practical applicability of our approach, we align our methodology with the systematic integration of current and upcoming functional safety and cybersecurity design standards in a leading industry domain.

3. Essential related work in the automotive context

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. Functional safety development aspects are currently addressed by the ISO 26262 [6] 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 [7] is the only published industry agreement at this stage. The Industrial Internet Consortium has published a generic reference architecture for the design of CPS manufacturing systems [8].

In terms of published research, Ward et al. [9] 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 [6]. Steiner et al. [10] deal with safety and security analysis, however focus on state/event fault trees for modelling of the system under development. Bloomfield et al. [11] 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. SFA and AD for integrated safety/security design

In [3] we explain the hazard and risk analysis (HARA) using the ESCL example. Here we apply the same principle to an EPS in which an electric motor provides steering power support (instead of a hydraulic pump driven by the combustion engine). The HARA results in an ASIL D rating (i.e., highest possible safety criticality) and a safety goal (i.e., high-level functional safety requirement):

- FR1: "*There must be no unwanted steering actuation*".

When carrying out a system analysis, this safety goal needs to be decomposed to system safety FRs. The safety experts and system analyst usually look at the potential faults that can lead to this failure (e.g. based on an FMEA) and define Functional Safety Concept requirements to diagnose and avoid these faults. In order to render this process systematic, we propose signal-flow analysis as depicted in Figure 1.

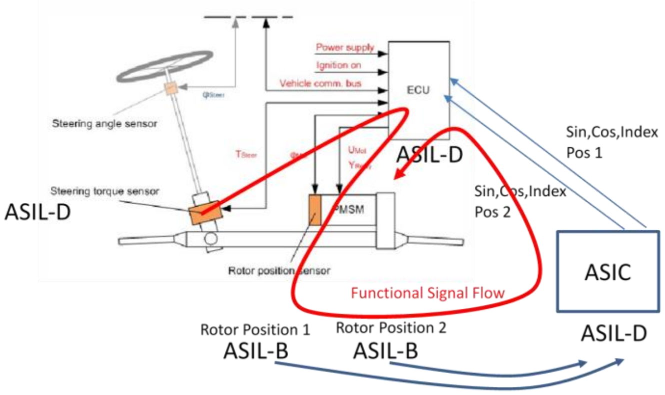

Power supply
Ignition on
Vehicle comm. bus
ECU
Steering angle sensor
φ_{Steer}
T_{Steer}
U_{Mot}
Y_{Relay}
ASIL-D
Sin,Cos,Index
Pos 1
Steering torque sensor
ASIL-D
PMSM
Sin,Cos,Index
Pos 2
Rotor position sensor
Functional Signal Flow
ASIC
Rotor Position 1
ASIL-B
Rotor Position 2
ASIL-B
ASIL-D

Figure 1. Signal flow analysis of the EPS system.

The signal flow analysis starts from the steering torque sensor rather than from the steering angle sensor that is typically provided by the vehicle manufacturer (OEM) rather than the EPS supplier. This fact also has strong consequences on the FR's and DP's linked to the safety goal FR1 analysed here.

Based on this analysis we find that two potential sources of violating the safety goal FR1 are erroneous values for the steering angle demand or the torque applied to the steering wheel by the driver. Hence, we can decompose FR1 to

- FR1-1: "*The steering angle has to be measured with ASIL-D quality.*"
- FR1-2: "*The driver demand torque has to be measured with ASIL-D quality.*"

In the following, we will limit decomposition considerations [6] to FR1-1. For the reason explained above, the decomposition continues on Technical Safety Concept level as follows:

- FR1-1-1: "*The internal steering angle is calculated from the rotor angle.*"
- FR1-1-2: "*The index position has to be provided with ASIL-D quality.*"

In the technical safety design in system architecture level, we can identify the following design parameters (DP), based on decomposition according to [4]:

- DP1: The internal steering angle calculation is done with two rotor position sensors fulfilling ASIL-B quality goals.
- DP2: The rotor position sensor signals are compared against each other using an ASIL-D rated ASIC delivering sin and cos angle information and index counter.
- DP3: Diversity and independency are assured in the hardware design (not having the same fault behaviour) and algorithms (sin and cos function).

This design choice induces the following technical software requirement:

- FR1-1-3: "*Every 1 ms the sin and cos and index counters have to be measured and the redundant steering angles calculated*".
- FR1-1-4: "*Both steering angles must match within a 5 degrees range (plausibility-check). This comparison has to be executed and monitored independently of the calculation linked to FR1-1-3*".

In autonomous driving, however, the demand value for steering will be provided by the cyber-infrastructure and/or the vehicle's central electronic control (ECU) rather than by the driver. Consequently, we have to extend our system boundaries and the related analyses as illustrated in Figure 2.

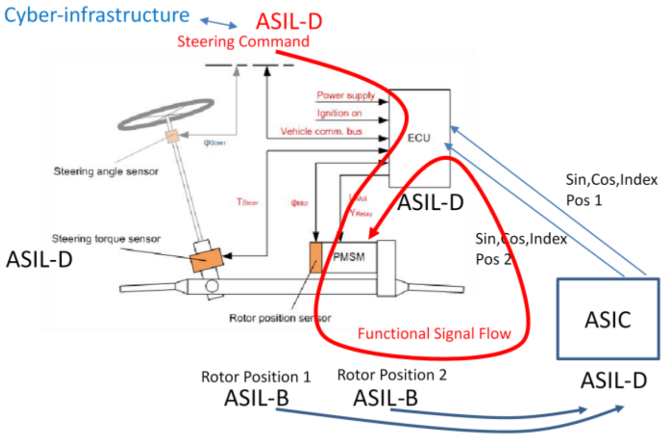

Cyber-infrastructure
ASIL-D
Steering Command
Power supply
Ignition on
Vehicle comm. bus
ECU
Steering angle sensor
φ_{Steer}
T_{Steer}
φ_{Mot}
U_{Mot}
Y_{Relay}
ASIL-D
Sin,Cos,Index
Pos 1
Steering torque sensor
ASIL-D
PMSM
Sin,Cos,Index
Pos 2
Rotor position sensor
Functional Signal Flow
ASIC
Rotor Position 1
ASIL-B
Rotor Position 2
ASIL-B
ASIL-D

Figure 2. EPS signal flow analysis in an autonomous vehicle.

This change has a significant impact on the ASIL ratings, as well as the top-level safety goal:

- FR2: "*The EPS must steer exactly according to the external steering command.*"

The external steering command contains the requested steering angle, which the steering controller (ASIC) translates to a steering torque before comparing the actually achieved internal steering angle with the externally requested one. Moreover, the system's safe state on vehicle level has to change, since there is no driver to hand over steering control in the event of EPS failure:

- DP3: Use redundant and diverse motor concepts (e.g. 6 phase, 12 phase) to allow a limp-home mode to a garage.

Adding cybersecurity requirements to this involves the analysis of both static and dynamic dependencies between functional safety FR's and the results of the cybersecurity threat analysis and risk assessment (TARA) [7]. In this contribution, we will focus on the signal (attack) flow analysis, i.e., the dynamic part only. Figure 3 shows the signal flow analysis of two selected potential attacks, one originating in the cyber-infrastructure, the other one—more classically—originating in the service garage via the vehicle's traditional diagnostic interface. This analysis has been used in order to identify the requirements for the design of diverse defence layers implementing the defence-in-depth design pattern. Linking design patterns with AD is particularly interesting in the cybersecurity domain where researchers and industry experts have come up with numerous attack/threat and defence patterns over the last 15 years. Particularly outstanding, Hafiz et al. [12] sum up 96 such patterns without which it is very difficult for system analysts to identify and integrate cybersecurity requirements. Thomas et al. [13] build on this work in order to make these (bottom-up) design patterns usable in AD (top-down). We applied their unique approach to our case study.

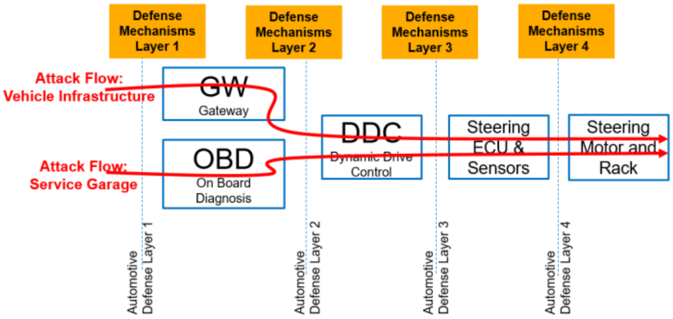

Defense Mechanisms Layer 1
Defense Mechanisms Layer 2
Defense Mechanisms Layer 3
Defense Mechanisms Layer 4
Attack Flow: Vehicle Infrastructure
Attack Flow: Service Garage
GW
Gateway
OBD
On Board Diagnosis
DDC
Dynamic Drive Control
Steering ECU & Sensors
Steering Motor and Rack
Automotive Defense Layer 1
Automotive Defense Layer 2
Automotive Defense Layer 3
Automotive Defense Layer 4

Figure 3. EPS attack data flow analysis for the defence-in-depth pattern.

The key DPs affected by the defence-in-depth pattern are the following:

- location of each layer (shielding of system components),
- properties of each layer (defence mechanisms).

The power of AD lies in the integration of all DPs in a design matrix in order to analyse and improve the complexity of design decisions made for each FR in each domain (functional safety and cybersecurity in particular).

5. Integration applied to applicable industry standards

In order for our research results to be accepted and actually deployed in industrial application, our industry research partners pushed and helped us integrate our concepts in the three currently applicable industry standards Automotive SPICE [14] and [6,7]. This translates itself in a completely integrated treatment of requirements for the system, as well as its electronics hardware and software components while taking into account the three standards.

The methodology we applied is based on a systematic investigation of each standard's practices in terms of the design tasks they require in order to achieve each specialist domain's objectives. Subsequently we analysed the complementarity of these practices and ways of integrating them such that they help architects adopt a systemic view on designing CPS that are both safe and secure. Figure 4 shows a top-level overview of the results of this exhaustive research work on system level (processes SYS.1–5). We have achieved a similar mapping on software (SWE.1–6) and electronic hardware levels (HWE.1–4).

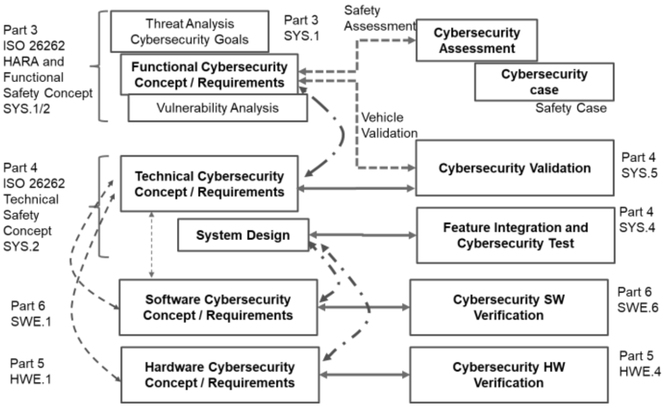

Part 3
ISO 26262
HARA and
Functional
Safety Concept
SYS.1/2
Threat Analysis
Cybersecurity Goals
Part 3
SYS.1
Functional Cybersecurity Concept / Requirements
Vulnerability Analysis
Safety Assessment
Cybersecurity Assessment
Cybersecurity case
Safety Case
Vehicle Validation
Part 4
ISO 26262
Technical
Safety
Concept
SYS.2
Technical Cybersecurity Concept / Requirements
Cybersecurity Validation
Part 4
SYS.5
System Design
Feature Integration and Cybersecurity Test
Part 4
SYS.4
Part 6
SWE.1
Software Cybersecurity Concept / Requirements
Cybersecurity SW Verification
Part 6
SWE.6
Part 5
HWE.1
Hardware Cybersecurity Concept / Requirements
Cybersecurity HW Verification
Part 5
HWE.4

Figure 4. Integration of automotive development standards.

Each rectangle represents a particular design process phase along the V-cycle, which is the backbone of automotive development. The arrows indicate (explicit or implicit) dependencies that we could identify among these processes. In order to give a small insight into the complete framework linking the three standards, we will look at the System Requirements Analysis process (SYS.2 in Automotive SPICE 3.0 [14]).

Automotive SPICE base practice SYS.2.BP1: "Specify system requirements. Use the stakeholder requirements and changes to the stakeholder requirements to identify the required functions and capabilities of the system. Specify functional and non-functional system requirements in a system requirements specification" [14].

Complementary functional safety design tasks:

Related to [6], clauses ISO 26262-4 6.4.1.1, 6.4.1.3, 6.4.1.4:

- Make technical safety requirements consistent with functional safety requirements.
- Make technical safety requirements traceable back to their sources.
- Use semiformal notations for ASIL C and D.

Related to [6], clauses ISO 26262-4 6.4.2.1, 6.4.2.2, 6.4.2.3:

- Specify the required safety mechanisms in the technical safety concept, including control and monitoring systems to achieve all safety goals in time immediately or by a warning or degradation concept with the correct prioritization.
- Specify measures to detect all possible failures and failure combinations including all operation modes and interactions with other systems.

Related to [6], clauses ISO 26262-4 6.4.4.1, 6.4.4.2, 6.4.4.3:

- Specify safety mechanisms to prevent faults from being latent for ASIL C/D requirements.
- Specify the multiple-fault detection interval to avoid multiple-point failures and to be consistent with the avoidance of latent faults for ASIL C/D requirements.

Complementary cybersecurity design tasks:

Related to [7], clauses 8.3.6, 8.3.7, 8.4.2:

- Derive cybersecurity requirements from the system level vulnerability analysis.
- Define the cybersecurity concept including functional cybersecurity requirements, cybersecurity plan, feature definition, threat analysis and risk assessment, cybersecurity assessment.
- Organise regular cybersecurity reviews for the identification of new threats and related cybersecurity requirements.

Automotive SPICE base practice SYS.2.BP4: "Analyse the impact on the operating environment. Identify the interfaces between the specified system and other elements of the operating environment. Analyse the impact that the system requirements will have on these interfaces and the operating environment" [14].

Complementary functional safety design tasks:

Related to [6], clause ISO 26262-4 6.4.1:

- Specify technical safety requirements in accordance with the functional safety concept, the preliminary architectural assumptions of the item and the following system properties:
    a) the external interfaces, such as communication and user interfaces, if applicable;
    b) the constraints, e.g. environmental conditions or functional constraints; and
    c) the system configuration requirements.
- Specify the hardware-software interface (HSI).

Complementary cybersecurity design tasks:
Related to [7], clause 8.3.1:

- Identify the feature's physical boundaries, its cybersecurity and network perimeter, as well as its trust boundaries.
- Define the feature's scope and its interfaces to the cyber-infrastructure.

This integration work addresses the huge challenge both designers and quality (safety, security) assessors are increasingly confronted with, which is having a holistic, integrated view on the functional, non-functional and process requirements induced by the three automotive development standards.

6. Extension of applicable industry standards

Our work revealed that the current standards do not yet cover the challenges imposed by CPS in the form of ADAS and autonomous vehicles. An ADAS-based cyber-infrastructure will require an additional life cycle to be considered in Automotive SPICE. Therefore we propose a new set of processes, which we call the ASI (Automotive Service Infrastructure) processes. They are connected with the related system process life cycle (SYS.1 – 5) in Automotive SPICE, as shown in Figure 5 below.

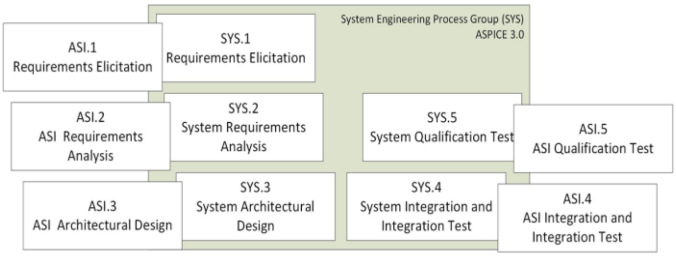

System Engineering Process Group (SYS)
ASPICE 3.0
ASI.1 Requirements Elicitation
SYS.1 Requirements Elicitation
ASI.2 ASI Requirements Analysis
SYS.2 System Requirements Analysis
SYS.5 System Qualification Test
ASI.5 ASI Qualification Test
ASI.3 ASI Architectural Design
SYS.3 System Architectural Design
SYS.4 System Integration and Integration Test
ASI.4 ASI Integration and Integration Test

Figure 5. A new A-SPICE process life cycle for the cyber-infrastructure

The previously analysed base practice SYS.2.BP4 will need a complementary part in the corresponding ASI.2 base practice:

Proposed Automotive SPICE base practice ASI .2.BP4: "Analyse the interfaces between the vehicle and the service infrastructure. Identify the interfaces between the vehicle and the service infrastructure. Analyse the impact that the service infrastructure interfaces will have with the vehicle's operating environment."

Outcomes: required Quality of Service (availability), reaction in case of no availability, criticality of information, safety integrity level, encryption and identification mechanisms.

From a more general, industry-sector independent point of view, this extension reflects the necessity for CPS development to take into account requirements purely linked to the cyber-infrastructure and directly or indirectly influencing the product's or system's behaviour [15]. Significantly more attention will have to be paid to the very clear definition of system interfaces beyond the CPS boundaries, as well as the scope and quality of service that is required by and/or provided by each CPS functionality.

Conclusion and outlook

In this paper we extend our methodology for the integration of functional safety and cybersecurity aspects in the early phases of industrial embedded systems design [5] by a systematic approach to integrated requirements elicitation based on AD and SFA on system architecture level. Our method leverages the integration of functional safety and cybersecurity design requirements on system architecture level, which is key to detailed component design that is safe and combats cyber threats effectively and efficiently. We have shown the application of our concept to the design of a modern automotive electric power steering system. In particular, we have investigated the functional safety and cybersecurity challenges linked to functions driven or at least influenced by the cyber-infrastructure. 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. The automotive industry is considered precursor in this domain, as cars are extremely complex with respect to the high number of interconnected functions and required expert domains and organisational structures. In addition to that, innovation cycles are extremely short, and the automotive sector is moving from a product-focus to a product-service-system (IPS^2) focus in terms of multi-modal mobility provision. The latter is a key driver for the advent of autonomous vehicles, which will be heavily dependent on the cyber-infrastructure even for providing basic vehicle functions such as steering. For this sector, we have also elaborated a framework for the integration of the three most prominent automotive development standards both on system architecture and detailed design levels. This framework includes an extension to cover requirements linked to the cyber-infrastructure. These results are on a good way of being adopted as an industry-wide standard.

Based on our generally applicable integration concept, the next steps in our research are focussed on the identification and characterisation 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 grant agreement 621429 (project EMC^2). Furthermore, we express our thanks to our supporting industry partners, who are all members of the German SOQRATES initiative (www.soqrates.de).

References

[1] Suh, N.P., 1990, The Principles of Design, 1st ed., Oxford University Press.
[2] Abrahams, J.R., Coverley, G.P., 1965, Signal Flow Analysis, Pergamon Press.
[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] Riel, A., Kreiner, C., Macher, G., Messnarz, R., 2017, Integrated design for tackling safety and security challenges of smart products and digital manufacturing, CIRP Annals - Manufacturing Technology, 66 (2017)/1 : 177–180.
[6] ISO - International Organization for Standardization, 2011, ISO 26262 Road vehicles Functional Safety Part 1-10.
[7] SAE Vehicle Electrical System Security Committee, 2017, SAE J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems, SAE Standard, Work-in-Progress.
[8] Industrial Internet Consortium, 2017, The Industrial Internet of Things Volume G1: Reference Architecture, IIC:PUB:G1:V1.80:20170131.
[9] 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.
[10] 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.
[11] Bloomfield, R., Netkachova, K., Stroud, R., Gorbenko, A., Romanovsky, A., Kharchenko, V., Security-Informed Safety: If It's Not Secure, It's Not Safe, 2013, Software Engineering for Resilient Systems, Springer Berlin Heidelberg.
[12] Hafiz, M., Adamczyk, P., Johnson, R.E., 2012, Growing a pattern language (for security), in: Onward! 2012 Proceedings of the ACM International Symposium. ACM New York, NY, USA. October 2012.
[13] Thomas, J., Mantri, P., 2015, Axiomatic Design/Design Patterns Mashup: Part 1&2, Procedia CRP 34 (2015), pp. 269 – 283.
[14] VDA QMC, 2017, Automotive SPICE® Process Assessment/Reference Model, Version 3.0.
[15] 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.

Response to reviewers of our paper 2018-Dn-10R1

First of all, many thanks for having critically reviewed our paper! Please find our responses below.

The proposed topic is very relevant.

No changes.

The advantages of integrating Axiomatic design int the analysis of safety and security should be clarified better in the paper and in the conclusions.

Added explanations to section 2, 4, and “Conclusions and Outlook”. We particularly highlight the importance of AD as a facilitating method for reducing the architectural design complexity of CPS with respect to safety and cybersecurity integration by design. Formulating safety and cybersecurity design requirements as FRs and mapping them to DP’s inspired by related design standards transfers the problem of complexity reduction to the mathematical space of matrix operations.

The second part of Section 5 could in principle be presented as a Table.

We did not follow this suggestion, because a table representation of the design task lists could be misleading with respect to comparing the complementary design tasks for safety and cybersecurity. However, there is no point in comparing them directly. It is much rather in complementing each clause mentioned by the additional design tasks aiming at capturing safety and cybersecurity requirements in system level. Therefore, we consider a list representation better suited (just as in the related standards).

Font size in Fig. 3 and Fig. 5 should be enlarged.

Increased from 10,5 points to 12 points.

This paper touches on an important aspect, but the paper is not very strong from research rigour point of view.

In several places (introduction, section 2, 5, 6, and Conclusions and outlook), we clearly point out that we have carried out our research in very close collaboration with industry. This has been vital to assure the practical relevance of our integration approach. Nonetheless, we followed a clear methodology which is also proven by the fact that our paper builds on the results of our previous CIRP publication.

Link with standard is good but it is not derived in a systematic manner.

We improved the explanation of our systematic approach in the second paragraph of section 5.

It is not clear how the architecture would combat cyber threats!

We have slightly modified the abstract and section 2 such that they explain better what we mean by “architectural approach” in the paper’s title. Furthermore, we added “on system architecture level” to the description of the technical safety concept in section 3, as well as to the Conclusions and outlook section. The point is that our method leverages the integration of functional safety and cybersecurity design requirements on system architecture level, which is key to detailed component design that is safe and combats cyber threats effectively and efficiently. We have added this explanation to the Conclusion and outlook section as well.

The paper has copied 350 words from 2017.eurospi.net - this is a problem too, this needs to be rewritten.

The part concerned are the base practices cited from the Automotive SPICE standard (we added a reference in the respective locations), and our analysis findings for the complementary design tasks (in the initial version formulated as questions). We have published those as questions to be asked during a safety/cybersecurity assessment in a practitioner paper at the EuroSPI 2017. (2017.eurospi.net) conference in order to disseminate them to the mostly industrial audience. In this revised version of our CIRP paper, we have re-written this part as complementary design tasks in a way that they even better complement the base practices of the Automotive SPICE standard.

Rather narrative and practice-oriented.

See justification related to practice-orientation above.

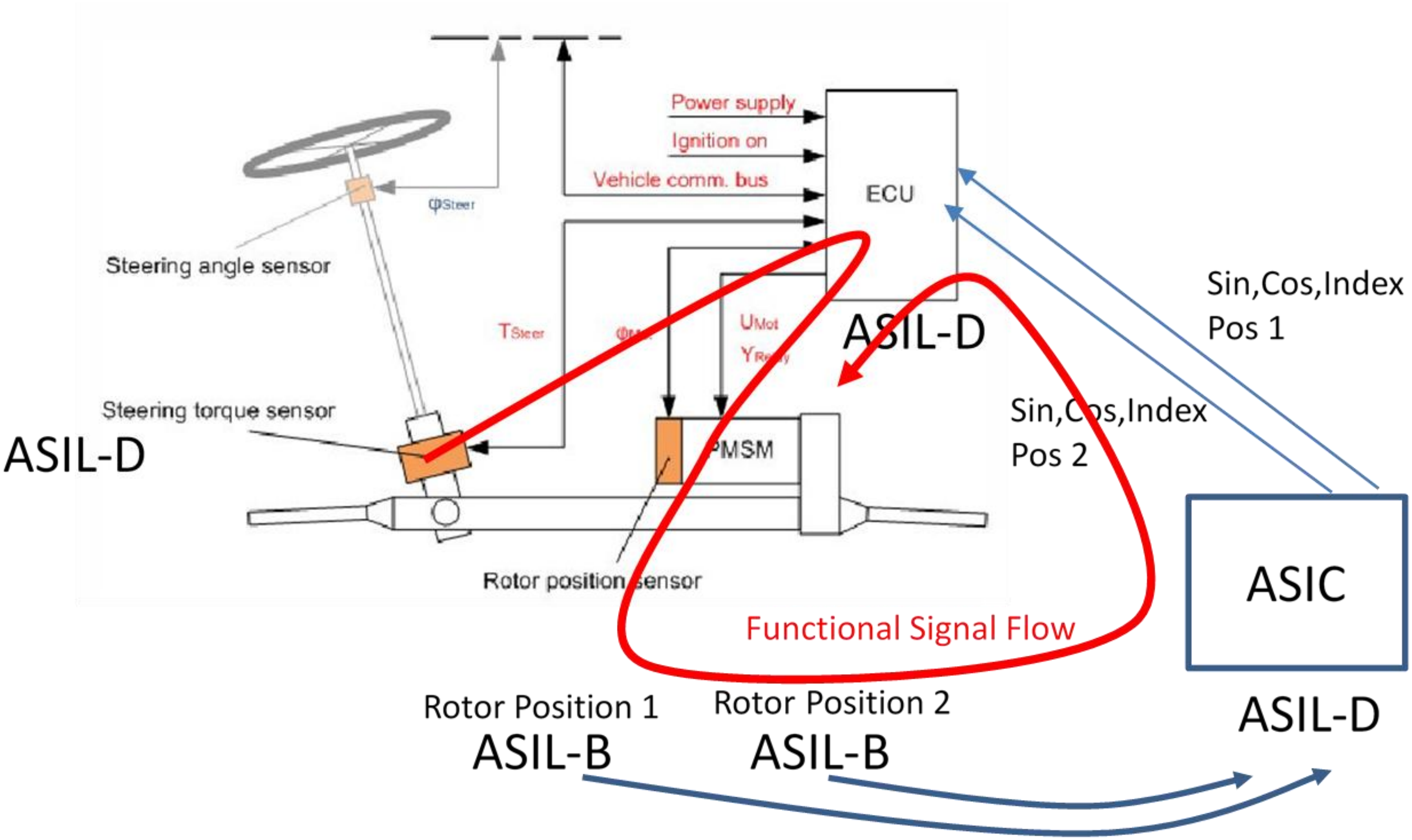
The claim (in the title) towards the architectural approach is not substantiated in the paper.

Please see the justification given for the argument “It is not clear how the architecture would combat cyber threats”.

With this, the paper leans too much on straight forward analysis and reasoning.

We agree that a significant part of our research relies on systematic analysis of design practices applied to tackle functional safety and cybersecurity challenges in automotive embedded systems design. However, we were obliged to do this in order to be able to propose an integrated approach to tackling these design challenges from a SYSTEMIC and INTEGRATED point of view that is also ACCEPTED by stakeholders in the automotive industry. To achieve this, it is vital to build research on the terminology and frameworks accepted in the industry sector.

Figure


φSteer
Power supply
Ignition on
Vehicle comm. bus
ECU
Steering angle sensor
TSteer
φMot
UMot
YReady
Steering torque sensor
PMSM
Rotor position sensor

ASIL-D

Sin,Cos,Index
Pos 1

Sin,Cos,Index
Pos 2

ASIL-D

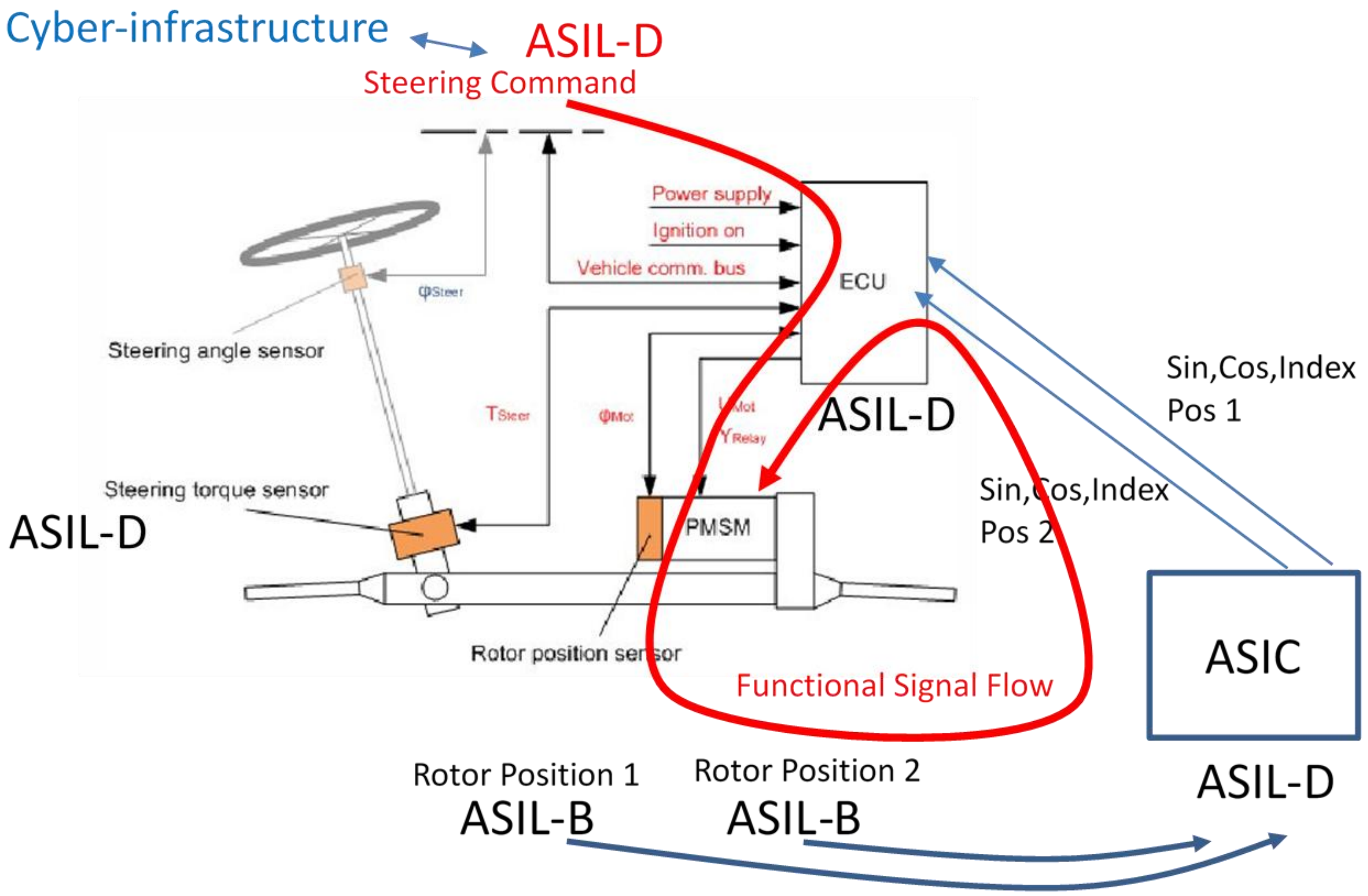
Functional Signal Flow

ASIC

ASIL-D

Rotor Position 1
ASIL-B

Rotor Position 2
ASIL-B


Power supply
Ignition on
Vehicle comm. bus
ECU
φ_{Steer}
Steering angle sensor
T_{Steer}
φ_{Mot}
U_{Mot}
Y_{Relay}
Steering torque sensor
PMSM
Rotor position sensor

Cyber-infrastructure ↔ ASIL-D

Steering Command

ASIL-D

ASIL-D

Sin,Cos,Index
Pos 1

Sin,Cos,Index
Pos 2

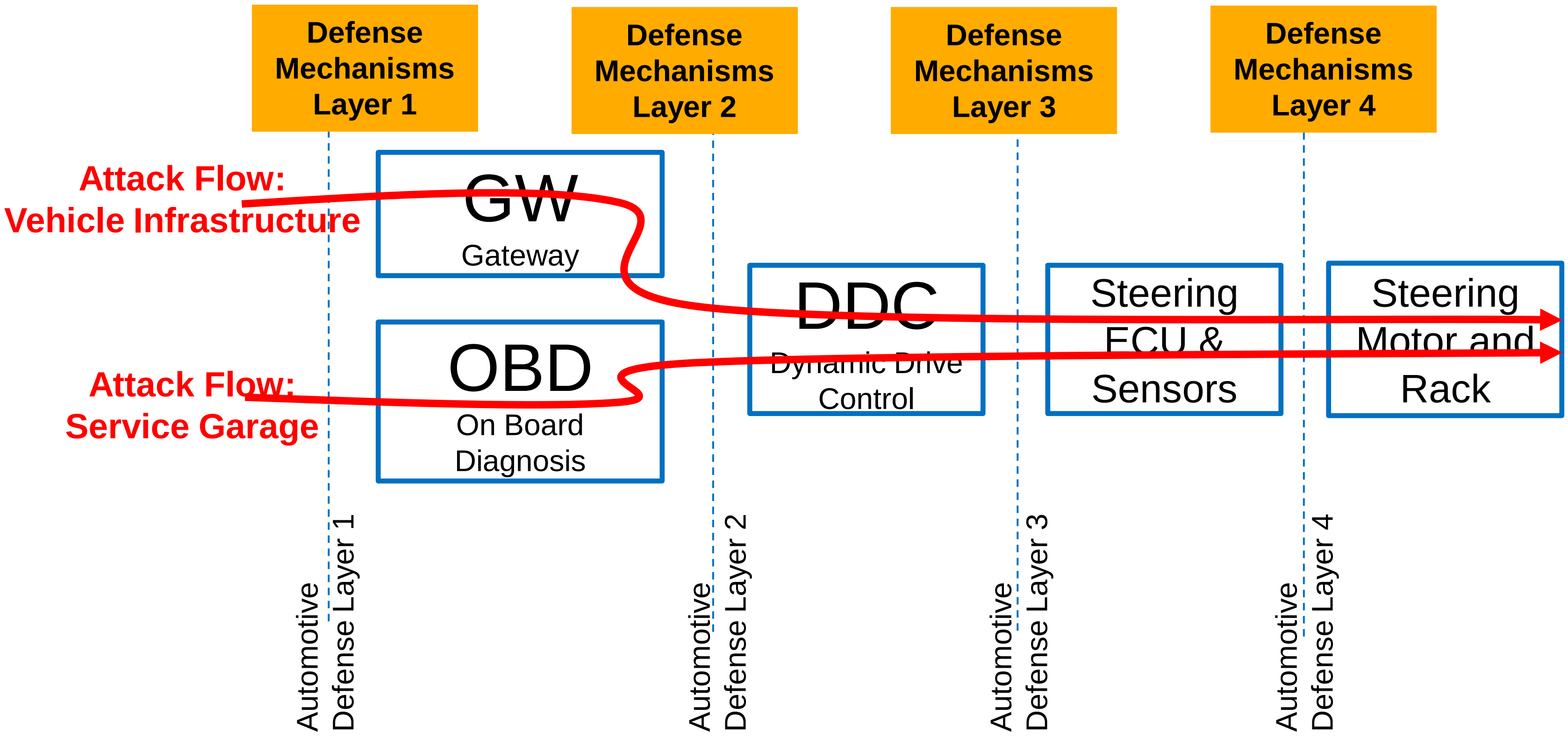
Functional Signal Flow

ASIC

ASIL-D

Rotor Position 1
ASIL-B

Rotor Position 2
ASIL-B



Defense Mechanisms Layer 1

Defense Mechanisms Layer 2

Defense Mechanisms Layer 3

Defense Mechanisms Layer 4

Attack Flow: Vehicle Infrastructure

Attack Flow: Service Garage

GW
Gateway

OBD
On Board Diagnosis

DDC
Dynamic Drive Control

Steering ECU & Sensors

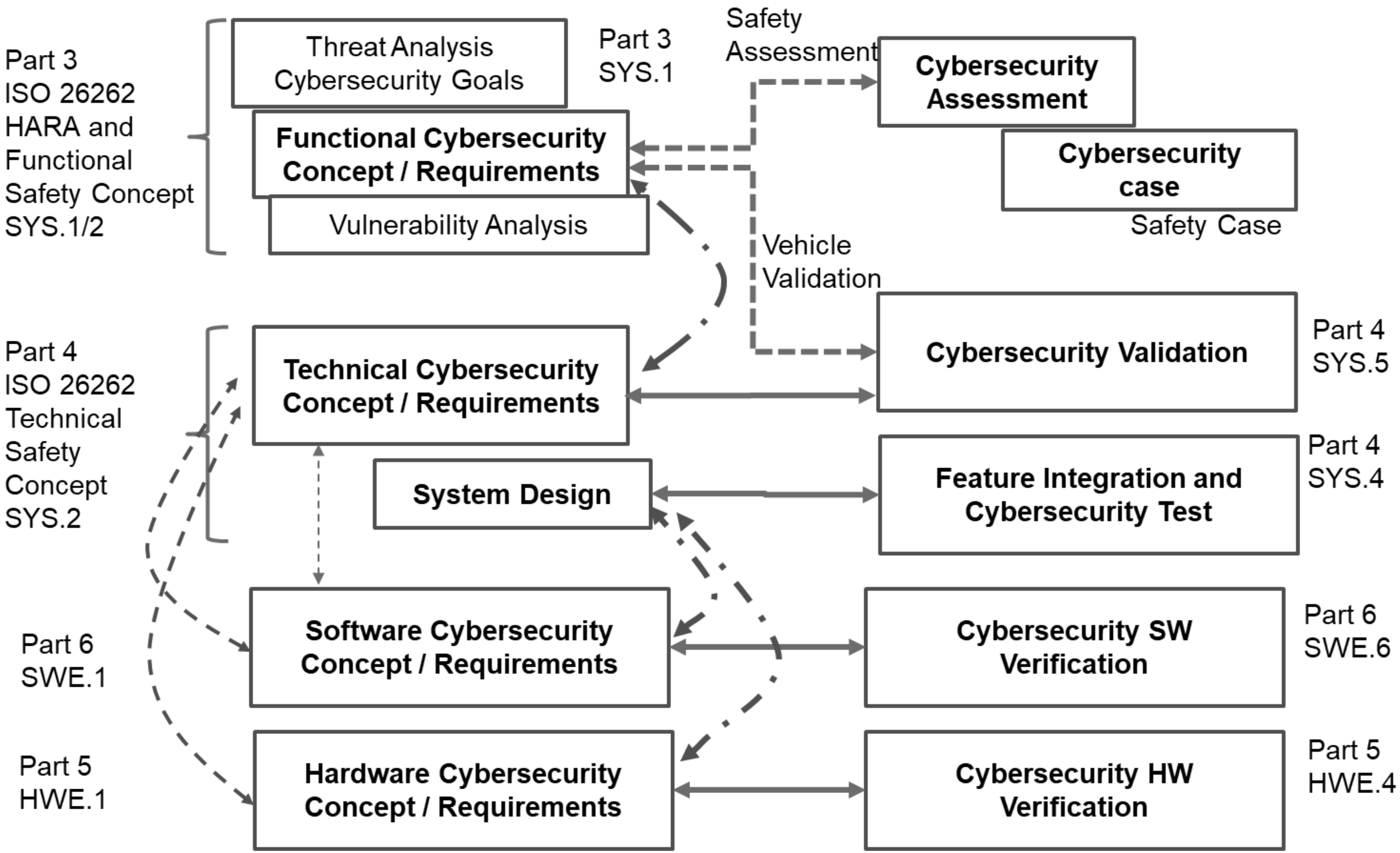
Steering Motor and Rack

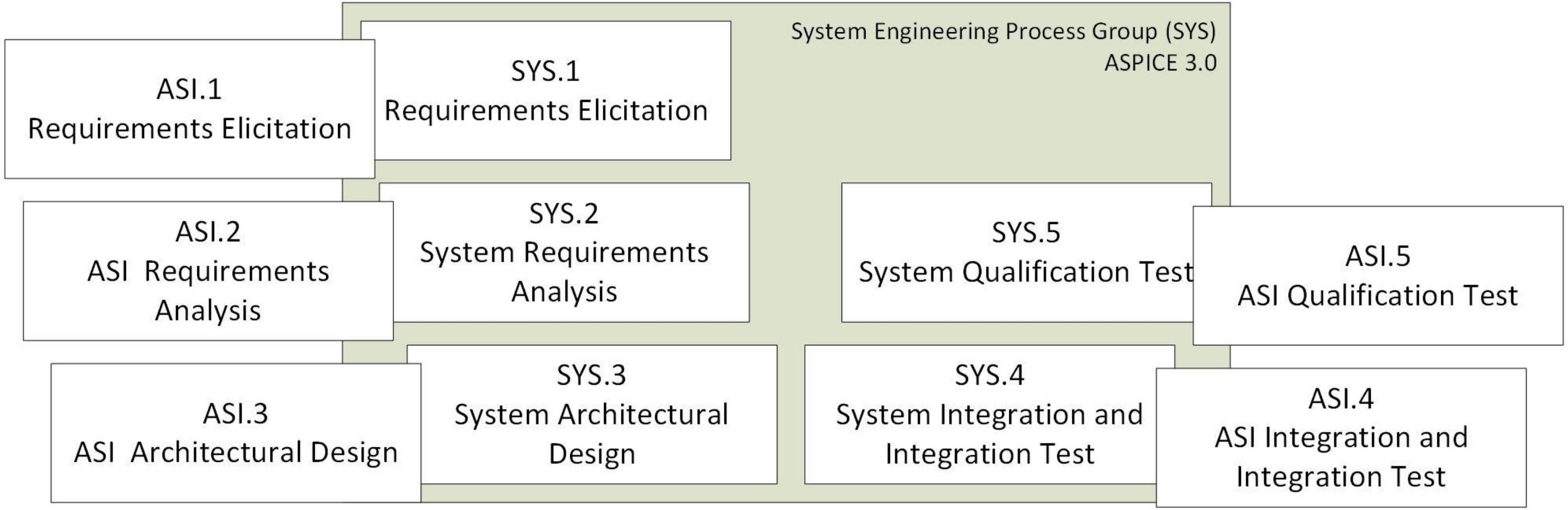
Automotive Defense Layer 1

Automotive Defense Layer 2

Automotive Defense Layer 3

Automotive Defense Layer 4


Part 3
ISO 26262
HARA and
Functional
Safety Concept
SYS.1/2
Threat Analysis
Cybersecurity Goals
Part 3
SYS.1
Safety
Assessment
Cybersecurity
Assessment
Functional Cybersecurity
Concept / Requirements
Cybersecurity
case
Vulnerability Analysis
Safety Case
Vehicle
Validation
Part 4
ISO 26262
Technical
Safety
Concept
SYS.2
Technical Cybersecurity
Concept / Requirements
Cybersecurity Validation
Part 4
SYS.5
System Design
Feature Integration and
Cybersecurity Test
Part 4
SYS.4
Part 6
SWE.1
Software Cybersecurity
Concept / Requirements
Cybersecurity SW
Verification
Part 6
SWE.6
Part 5
HWE.1
Hardware Cybersecurity
Concept / Requirements
Cybersecurity HW
Verification
Part 5
HWE.4



System Engineering Process Group (SYS)
ASPICE 3.0

ASI.1
Requirements Elicitation

SYS.1
Requirements Elicitation

ASI.2
ASI Requirements Analysis

SYS.2
System Requirements Analysis

ASI.3
ASI Architectural Design

SYS.3
System Architectural Design

SYS.4
System Integration and Integration Test

ASI.4
ASI Integration and Integration Test

SYS.5
System Qualification Test

ASI.5
ASI Qualification Test