G Model
CIRP-1755; No. of Pages 4

ARTICLE IN PRESS

CIRP Annals - Manufacturing Technology xxx (2018) xxx–xxx

Contents lists available at ScienceDirect

CIRP Annals - Manufacturing Technology

journal homepage: http://ees.elsevier.com/cirp/default.asp

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

Andreas Riel (2)[a,*], Christian Kreiner[b,1], Richard Messnarz[c], Alexander Much[d]

[a] Grenoble Alps University, G-SCOP Laboratory, Grenoble, France
[b] Graz University of Technology, Institute for Technical Informatics, Graz, Austria
[c] ISCN GmbH, Graz, Austria
[d] Elektrobit Automotive GmbH, Erlangen, Germany

ARTICLE INFO

Keywords:
Design
Integration
Safety

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.

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 Ref. [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

[*] Corresponding author.
E-mail address: andreas.riel@grenoble-inp.fr (A. Riel).
[1] Deceased.

https://doi.org/10.1016/j.cirp.2018.04.022
0007-8506/© 2018 Published by Elsevier Ltd on behalf of CIRP.

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 Ref. [6]. Steiner and Liggesmeyer [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 Ref. [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 Fig. 1.

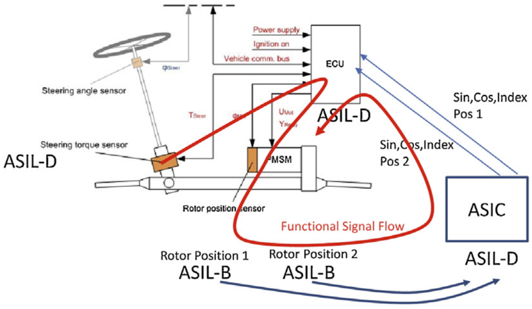

Fig. 1. Signal flow analysis of the EPS system.

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 Ref. [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 Fig. 2.

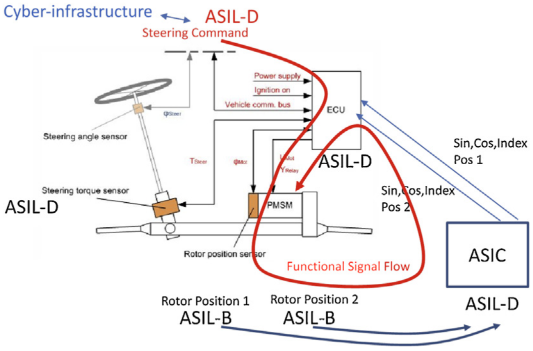

Fig. 2. EPS signal flow analysis in an autonomous vehicle.

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: