CIRP Annals - Manufacturing Technology xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

CIRP Annals - Manufacturing Technology

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

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

Andreas Riel (2)[a,*], Christian Kreiner[b], Georg Macher[c], Richard Messnarz[d]

[a] Grenoble Alpes University, G-SCOP Laboratory, Grenoble, France
[b] Graz University of Technology, Institute for Technical Informatics, Graz, Austria
[c] AVL LIST GmbH, Graz, Austria
[d] ISCN GmbH, Graz, Austria

ARTICLE INFO

Keywords:
Design
Integration
Safety

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.

© 2017 Published by Elsevier Ltd on behalf of CIRP.

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 [1].

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

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

http://dx.doi.org/10.1016/j.cirp.2017.04.037
0007-8506/© 2017 Published by Elsevier Ltd on behalf of CIRP.

Please cite this article in press as: Riel A, et al. Integrated design for tackling safety and security challenges of smart products and digital manufacturing. CIRP Annals - Manufacturing Technology (2017), http://dx.doi.org/10.1016/j.cirp.2017.04.037

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].

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.

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
Result		
Design goal	Safety goal	Security target
Design goal criticality	ASIL	SecL

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 Tables 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

Please cite this article in press as: Riel A, et al. Integrated design for tackling safety and security challenges of smart products and digital manufacturing. CIRP Annals - Manufacturing Technology (2017), http://dx.doi.org/10.1016/j.cirp.2017.04.037

Download English Version:

https://daneshyari.com/en/article/5466965

Download Persian Version:

https://daneshyari.com/article/5466965

Daneshyari.com