Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 109C (2017) 490–497

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Ambient Systems, Networks and Technologies (ANT 2017)

An Automotive Signal-Layer Security and Trust-Boundary Identification Approach

Georg Macher[a,*], Harald Sporer[b], Eugen Brenner[c], Christian Kreiner[c]

[a]AVL List GmbH, Hans-List-Platz 1, 8010 Graz, Austria
[b]pewag International GmbH, Gaslaternenweg, 8010 Graz, Austria
[c]Graz University of Technology, Inffeldgasse 16, 8010 Graz, Austria

Abstract

An important trend in the automotive domain is to adapt established functional safety processes and methods for security engineering. Although functional safety and cyber-security engineering have a considerable overlap, the trend of adapting methods from one domain to the other is often challenged by non-domain experts. Just as safety became a critical part of the development in the late 20th century, modern vehicles are now required to become resilient against cyber-attacks. As vehicle providers gear up for this challenge, they can capitalize on experiences from many other domains, but must also face several unique challenges. Such as, that cyber-security engineering will now join reliability and safety as a cornerstone for success in the automotive industry and approaches need to be integrated into the mainly safety oriented development lifecycle of the domain. The recently released SAE J3061 guidebook for cyber-physical vehicle systems focus on designing cyber-security aware systems in close relation to the automotive safety standard ISO 26262.

The key contribution of this paper is to analyse a method to identify attack vectors on complex automotive systems via signal interfaces and propose a security classification scheme and protection mechanisms on signal layer. To that aim, the hardware-software interface (HSI), a central development artefact of the ISO 26262 functional safety development process, is used and extended to support the cyber-security engineering process and provide cyber-security countermeasures on signal layer.

Peer-review under responsibility of the Conference Program Chairs.

Keywords:
ISO 26262; SAE J3061; automotive systems; hardware-software interfaces; cyber-security; functional safety

1. Introduction

In the late 1970s self-contained embedded systems called Electronic Control Units (ECUs) were introduced into production vehicles. Since then, the complexity of embedded systems in the automotive industry has grown significantly. Embedded automotive systems are estimated to account for 80 % of product innovations in the past decade and

* Corresponding author. Tel.: +43-316-787-2974.
E-mail address: georg.macher@avl.com

Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.05.317

are responsible for 25% of current vehicle costs[1]. These embedded systems are enablers for increasing the degree of digitalization, finally leading to an increase of competitiveness on existing markets as well as opening the door to new markets (e.g., data-driven business models). At the same time, the required dependability of these systems is raising: lack of safety, reliability, availability, integrity etc. of the system might lead to critical system failure having a severe impact on human health, environment, or property.

Exploiting the rising vehicle-to-vehicle and vehicle-to-infrastructure paradigms, future vehicles will have multiple inter-vehicle connections as well as capabilities for (wireless) networking with other vehicles and non-vehicle entities (such as charging stations and traffic lights)[2]. The resulting inter-connectivity increases attack surfaces and their damage potential.

Before the introduction of wireless connections and automated driving functionalities, vehicles were physically isolated machines with mechanical controls. Embedded automotive system technologies offered great benefits, but they also brought up new risks for the users safety. Therefore, functional safety engineering methods and processes become industry standard and critical part of the development.

In this context, the rising vehicle-to-vehicle and vehicle-to-infrastructure connectivity causes that automotive systems are developing from stand-alone systems towards systems of systems, interacting and coordinating with each other and influencing vehicle actions. Connections are thus not restricted to internal systems (e.g. steering, sensor, actuator, and communications) but also include other road users and the infrastructure and bringing up cyber-security issues. Consequently, new challenges regarding the manageability of systems are emerging caused by the increasing gap between cross-domain expertise required and the pervasiveness of novel technologies and software functions. An important trend in the automotive domain is to adapt established functional safety processes and methods for security engineering (e.g. the recently available SAE J3061[3]).

In the course of this paper, we follow this trend and focus on signal-layer. Therefore, analyse a way to identify trust boundaries and attack vectors on complex systems via signal interfaces based on the hardware-software interface (HSI). The HSI is a central development artefact of the ISO 26262[4] functional safety development process. This artefact is the last development artefact of the system development and the starting point for parallel development of hardware and software. The HSI definition thus requires mutual domain knowledge of hardware and software and is usually not only consisting of signal interface information but several additional device configurations and linked constraints. In relation to this approach, we propose an extension for the HSI to support the cyber-security engineering process and also propose a security classification scheme and related protection mechanisms on signal layer.

The paper is organized as follows: Section 2 presents an overview of related works. In Section 3 a description of the proposed approach and detailed information about the individual items is provided. A brief evaluation of the approach is presented in Section 4. Finally, Section 5 concludes with an overview of the approach presented.

2. Related Work

The only currently available guideline for automotive cyber-security engineering, SAE J3061[3] establishes a set of high-level guiding principles for cyber-security by: (a) defining a complete lifecycle process framework, (b) providing information on some common existing tools and methods, (c) supporting basic guiding principles on cyber-security, and (d) summarizing further standard development activities.

SAE J3061 states that cyber-security engineering requires an appropriate lifecycle process, which is defined analogous to the process framework described in ISO 26262[4]. The guidebook recommends an initial assessment of potential threats (TARA - threat analysis and risk assessment) and an estimation of risks for systems that may be considered cyber-security relevant or are safety-related systems, to determine whether there are cyber-security threats that can potentially lead to safety violations. Apart from that, no further recommendations on how to proceed with this estimated risk, set-up a security classification scheme or give guidance for required protection mechanisms is given.

The unambiguous definition of the hardware-software interfaces (HSI) is vital in the context of the road vehicles functional safety standard ISO 26262[4]. Therefore, this development artefact seems to be the perfect starting point for identification of trust boundaries and attack vectors via signal interfaces. But neither the current functional safety standard version nor automotive process reference model of Automotive SPICE[5] prescribe a specific methodology for the development of this artefact. Also publications related to HSI definition in the automotive domain are rare.