Hindawi
Security and Communication Networks
Volume 2019, Article ID 5381856, 2 pages
https://doi.org/10.1155/2019/5381856

Editorial

Safety and Security Coengineering in Embedded Systems

Daniel Schneider,[1] **Jens Braband**,[2] **Erwin Schoitsch**,[3] **Sascha Uhrig**,[4] **and Stefan Katzenbeisser**[5]

[1] *Fraunhofer IESE, Germany*
[2] *Siemens AG, Germany*
[3] *AIT Austrian Institute of Technology, Austria*
[4] *Airbus, Germany*
[5] *University of Passau, Germany*

Correspondence should be addressed to Daniel Schneider; daniel.schneider@iese.fraunhofer.de

Received 4 July 2019; Accepted 4 July 2019; Published 24 July 2019

Driven by large-scale scientific, technological, and socioeconomic developments, virtually every domain of embedded (cyberphysical) systems is presently subject to the same megatrends of increasing levels of interconnection and cooperation.

In the automotive domain, future cars will be highly automated and will cooperate to optimize the overall performance (consider, e.g., traffic flow or platooning scenarios) and to prevent accidents (consider, e.g., warnings of obstacles on the road or assistance services aimed at increasing general awareness with respect to the driving behavior and intentions of other cars, or, an even more complex issue, the behavior of vulnerable road users in urban scenarios). This opens up diverse security attack vectors, and these attacks may well affect the safety of the overall system. In the railway domain, for instance, the European Train Control System (ETCS), part of the ERTMS (European Rail Transport Management System), provides high interoperability and standardized communication and control, replacing the large number of national train control systems. Any security vulnerability would be extremely critical to railway safety. Regarding the upcoming topic of air taxis and large drones, the next air traffic management systems will be highly autonomous and rely on safe, secure, and reliable communication links between air taxi vehicles and ground stations. Hence, any security issue at these links—the ground stations or the air vehicles—will cause serious safety issues across the entire avionics domain, affecting not only local air taxis or large drones, but also general aviation as well as large airliners in the vicinity of airports. In the manufacturing and process industry domain, highly automated and partially autonomous systems of all kinds are interconnected and exchange critical data. In this domain, cyberattacks may lead to safety-critical incidents with a high impact on people, the economy, and the environment. The dependency of our society on electric energy (smart grid) or other large-scale infrastructures (gas, water, and communications) leads to the same critical implications.

Thus, in the domain of safety-critical embedded systems of systems, we presently see very high potential in new cooperation-based applications and services, but we also see significant engineering challenges regarding the indispensable assurance of trustworthiness of these systems. In particular, from a safety perspective, basic assumptions like the predictability of system behavior and environment, which are the foundation of state-of-the-practice approaches and established standards, are not sufficient anymore. One reason for this is that the significant increase in communication links (connectivity) and the potential dynamic integration of insecure systems as well as the reconfiguration in adaptive open systems provide plenty of attack surfaces from a cybersecurity point of view. However, a safety-critical system that is not secure might also be not sufficiently safe, which in turn can have an impact on the placement of the product in the market.

Consequently, safety can no longer be engineered in isolation from security, and we need integrated approaches with respect to the analysis, engineering, and validation of

safe and secure cyberphysical systems of systems. Moreover, we also need specific security mechanisms that are suitable for the considered type of systems. This special issue comprises contributions with respect to each of the aforementioned dimensions; it includes contributions on the security risk assessment of connected vehicles, on security requirements engineering for a safety-critical system, on safe and secure architectures, and on security validation utilizing fault injection, as well as on a range of concrete security mechanisms/approaches in the context of cyberphysical systems of systems. The latter consist of a secure Software Defined Network (SDN)-based communication protocol, software-based memory protection, the application of physically unclonable functions to defeat manipulation attacks in the context of tiny IoT devices, and other measures.

We conclude our editorial by briefly summarizing these different contributions to this special issue. First, there are two articles focusing on risk assessment and requirements engineering, respectively.

In their article "A Comparative Study of JASO TP15002-Based Security Risk Assessment Methods for Connected Vehicle System Design", the authors introduce the idea of asset containers and propose extending CRSS (Common Vulnerability Scoring System (CVSS) based Risk Scoring System) to a novel Risk Scoring System (RSS)s, RSS-CVSSv3, by appropriately replacing the CVSSv2 vulnerability scoring system on which CRSS is based with CVSSv3. To address the above questions, they performed a comparative study on CRSS, RSMA (Risk Scoring Methodology for Automotive systems), and RSS-CVSSv3 for multiple use cases such as a CGW (Central Gateway) and a drone in order to examine the efficiency and usefulness of the presented methods. For this comparative purpose, they devised an approach for the refinement of RSMA to the obstacles in comparing CRSS with RSMA.

In the article "Security Requirements Engineering in Safety-Critical Railway Signalling Networks", the authors report on their experience in developing security architecture for railway signalling systems, starting from the bare safety-critical system that requires protection. They used a threat-based approach to determine security risk acceptance criteria and derive security requirements and developed a security architecture based on the security requirements. The architecture is based on a hardware platform that provides the resources required for safety as well as security applications and is able to run these mixed-criticality applications (safety-critical applications and other applications run on the same device). To achieve this, the MILS approach is applied and discussed in detail in relation to the security requirements.

With respect to security validation of (safety-critical) systems, there is an article entitled "Multidevice False Data Injection Attack Models of ADS-B Multilateration Systems". The authors assume that attackers equipped with multiple devices can manipulate the ADS-B (Automatic Dependent Surveillance Broadcast) messages in distributed receivers without any mutual interference and can thus efficiently construct attack vectors to change the results of multilateration. The feasibility of a multidevice false data injection attack is demonstrated experimentally and countermeasures for such attacks are discussed.

Last but not least, three contributions deal with concrete security mechanisms/approaches for the context of cyberphysical systems of systems.

A secure SDN-based protocol is presented in "SSPSoC: A Secure SDN-Based Protocol over MPSoC". Following the SDN concept, the authors propose a new protocol in order to secure the communication and efficiently manage the routing within the CoC (Cloud of Chips). The SSPSoC includes a private key derivation phase, a Group Key Agreement (GKA) phase, and a data exchange phase to ensure that basic security primitives are preserved and provide secure communication. Furthermore, a network of 1-30 nodes is used to validate the proposed protocol and measure the network performance and memory consumption of the proposed protocol.

Next, there is an article focusing on memory protection, "SoftME: A Software-based Memory Protection Approach for TEE System to Resist Physical Attacks". The approach utilizes the on-chip memory space to provide a trusted execution environment for sensitive applications. It uses data encryption to protect the confidentiality of data on the off-chip memory and to provide integrity protection for the data. In addition, task scheduling in the encryption process is implemented. The prototype system of the approach was implemented on a development board supporting TrustZone and the overhead of the approach was tested. The experimental results show that the approach improves the security of the system and that there is no significant increase in system overhead.

In their article "Single-Round Pattern Matching Key Generation Using Physically Unclonable Function", the authors discuss that this not only enables defeating manipulation attacks but also makes it possible to prove security theoretically. In addition to its simple construction, the utilized scheme can use a weak PUF like the SRAM-PUF as a building block if the system is properly implemented, so that the PUF is directly inaccessible from the outside. It is therefore suitable for tiny devices in IoT systems. The article discusses the scheme's security and demonstrates its feasibility by means of simulations and experiments.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

We thank the authors for their contributions and the reviewers for their valuable comments, which made this special issue possible.

Daniel Schneider
Jens Braband
Erwin Schoitsch
Sascha Uhrig
Stefan Katzenbeisser