Guest Editors' Introduction

CYBER-PHYSICAL systems (CPSs) tightly couple cyber components (used for computation and communication) with physical components for sensing and actuating. These systems are extremely heterogeneous and require novel and holistic design methods to completely capture the requirements and the constraints.

CPS exhibit many of functional and nonfunctional requirements that are typical in other systems. Low power and energy consumption and real-time capabilities are, for instance, needed to reliably interact with the physical world. Nevertheless, there are additional, and very important security requirements that arise from the CPS interaction with the environment. For example, the sensitivity to the captured data from sensors, and their ability to actuate in the world, creates a serious threat for the system itself and its environment including people around it.

CPS face the same security challenges of embedded systems, such as the need of robustness against physical attacks and the need to migrate toward quantum resistant cryptography. However, standard design techniques used for securing embedded systems are not suitable for CPS, due to the often limited availability of computation and communication. Furthermore, current research efforts mainly focus on securing only the cyber-part of CPS, ignoring security threats caused by the physical-part. Therefore, there is a need for novel research to address the cross-domain and cross-layer security problems in CPS.

A promising approach to address these issues is to consider security from the beginning of the design flow. This allows for a holistic approach to jointly address the cyber and physical components of the whole system. Additionally, novel modeling strategies and methods to measure and evaluate the security of CPSs must be devised, developed, and formalized.

In this special issue, the problem of security in CPS is framed within the development of novel design methodologies suitable for the design of CPSs. Security requirements are often conflicting with other requirements, such as reliability and performance. The problem of novel design methodologies for CPS, including security aspects, is currently being investigated worldwide by a number of projects and initiatives of government and standardization bodies. Among them, it is worth mentioning, in the U.S., the DARPA programs (CASE and HACMS), the National science foundation CPS program, the CPSs security initiatives of the Department of Homeland Security, and, in Europe, the H2020 projects Platforms4CPS, CERBERO, CPSwarm, Bonseyes, and DEIS.

Security of CPS is a multifaceted problem, which is tackled by under different point of views. This aspect is also reflected by the contributions in this special issue. The first paper, by S. K. Ghosh, S. Dey, and D. Mukhopadhyay, focuses on vulnerabilities of cyber physical control software and proposes a methodology for implementing secure cyber-physical control systems. The proposed secure implementation requires a strong physically unclonable function (PUF) with a large challenge space. The second paper addresses the problem of long-term security and of the transition to quantum resistant cryptographic primitives. The work proposes an implementation of a quantum resistant datagram transport layer security (DTLS) for establishing secure communications suitable for being deployed in CPSs. The key transportation uses the NTRU post-quantum algorithm. The third paper, by F. Asplund, J. McDermid, R. Oates, and J. Roberts, proposes a framework for assessing the cyber risk. The framework is based on openly available taxonomies taken from the domains of safety and security that are combined into a single framework for CPS risk analysis. The work of M. Gay, B. Karp, O. Keren, and I. Polian presents the design of an error-correcting architecture suitable for cryptographic circuits susceptible to fault attacks. The architecture is based on a new class of error-detecting and correcting codes, that is validated using mathematical analysis and experiments on a real field programmable gate array platform.

We believe that the contributions of this special issue reflect some of the main challenges related with CPS security and provide an insightful look into the problems that are yet to be solved in the field.

FRANCESCO REGAZZONI
ALaRI – USI
6900 Lugano, Switzerland

ARQUIMEDES CANEDO
Corporate Technology
Siemens Corporation
Princeton, NJ 08540 USA

MOHAMMAD ABDULLAH AL FARUQUE
Department of Electrical Engineering and Computer Science
University of California at Irvine
Irvine, CA 92697 USA

Digital Object Identifier 10.1109/LES.2019.2910027