Information and Software Technology 83 (2017) 116–135

Contents lists available at ScienceDirect

Information and Software Technology

journal homepage: www.elsevier.com/locate/infsof

Model-based security engineering for cyber-physical systems: A systematic mapping study

Phu H. Nguyen[a,*], Shaukat Ali[a], Tao Yue[a,b]

[a] Simula Research Laboratory, Martin Linges vei 25, 1364 Fornebu, Norway
[b] Department of Informatics, University of Oslo, Norway

ARTICLE INFO

Article history:
Received 22 June 2016
Revised 19 October 2016
Accepted 8 November 2016
Available online 12 November 2016

Keywords:
Cyber-physical systems
Security
Model-based engineering
Security engineering
Systematic mapping
Snowballing
Survey

ABSTRACT

Context: Cyber-physical systems (CPSs) have emerged to be the next generation of engineered systems driving the so-called fourth industrial revolution. CPSs are becoming more complex, open and more prone to security threats, which urges security to be engineered systematically into CPSs. Model-Based Security Engineering (MBSE) could be a key means to tackle this challenge via security by design, abstraction, and automation.

Objective: We aim at providing an initial assessment of the state of the art in MBSE for CPSs (MBSE4CPS). Specifically, this work focuses on finding out 1) the publication statistics of MBSE4CPS studies; 2) the characteristics of MBSE4CPS studies; and 3) the open issues of MBSE4CPS research.

Method: We conducted a systematic mapping study (SMS) following a rigorous protocol that was developed based on the state-of-the-art SMS and systematic review guidelines. From thousands of relevant publications, we systematically identified 48 primary MBSE4CPS studies for data extraction and synthesis to answer predefined research questions.

Results: SMS results show that for three recent years (2014–2016) the number of primary MBSE4CPS studies has increased significantly. Within the primary studies, the popularity of using Domain-Specific Languages (DSLs) is comparable with the use of the standardised UML modelling notation. Most primary studies do not explicitly address specific security concerns (e.g., confidentiality, integrity) but rather focus on security analyses in general on threats, attacks or vulnerabilities. Few primary studies propose to engineer security solutions for CPSs. Many focus on the early stages of development lifecycle such as security requirement engineering or analysis.

Conclusion: The SMS does not only provide the state of the art in MBSE4CPS, but also points out several open issues that would deserve more investigation, e.g., the lack of engineering security solutions for CPSs, limited tool support, too few industrial case studies, and the challenge of bridging DSLs in engineering secure CPSs.

1. Introduction

Nowadays, Cyber-Physical Systems (CPSs) could be considered as the game changer in a wide range of industries (e.g., manufacturing, energy, healthcare and automotive industry), infrastructures (e.g., transportation, water management, oil and gas pipelines, wind farms), facilities (e.g., airports, space stations and buildings), and military (e.g., drones and unmanned aerial vehicles). As stated in [68], "*cyber-physical systems (CPSs) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core*". An example of CPSs is seen in modern power grid systems. In such a smart grid system, information and communication technology (ICT) is increasingly integrated throughout the grid to support novel communication and control functions among physical resources such as wind farm, solar farm, smart meters and information and control systems. Data (e.g., meter readings) collected from the sensors of physical resources (e.g., smart meters) are transmitted to information and control systems for live monitor and control (e.g., remote disconnect of smart meters). Computations based on these two-way communications allow the most efficient utilisation of renewable resources, and the great customisation of smart grid services. CPS technology would be expected to transform the way people

* Corresponding author.
E-mail addresses: phu@simula.no, nguyenhongphu@gmail.com (P.H. Nguyen).

http://dx.doi.org/10.1016/j.infsof.2016.11.004
0950-5849/

interact with engineered systems like the Internet has transformed the way people interact with information [60].

The more human beings surrounded by CPSs, the more important that these CPSs must be secure. A single security issue in smart grid could lead to city blackout or even country blackout. Large scale attacks on the software side of highly specialised industrial control systems were supposed to be very unlikely. However, the Stuxnet worm attack in the summer of 2010 was a wake-up call on the security of industrial CPSs [35]. By interfering the software that controls physical devices in a nuclear power plant, Stuxnet worm could destroy those physical devices or even the power plant. Stuxnet proved that even isolated industrial CPSs could be compromised, causing them to have unexpected (physical) operations, e.g., self-destruction. Moreover, many modern CPSs would unavoidably need to connect to the Internet that could bring much more security challenges. The security of CPSs is of paramount importance also because in many cases security could mean the physical safety of human beings around these systems. Put aside industrial systems, one of the biggest cybersecurity threats in 2016 was predicted to come from hacked medical devices [25]. By hijacking insulin pumps and pacemakers that are part of CPSs in the healthcare domain, hackers could hold patient's life ransom as warned in [25]. Again, this kind of threat urges the security of CPSs to be taken into account very early, seriously, and systematically. An important lesson should be learned from the way information systems had been engineered in the past is that security often came as an afterthought [18]. If security is not taken into account very early in the development lifecycle, it is nearly impossible to engineer security requirements properly into any complex system. One of the main reasons is that security requirements are often scattered and tangled throughout system functional requirements. Therefore, the security of CPSs should be engineered "by design" early in the CPSs' development.

However, CPSs are in many cases highly complex and making sure of their security is very challenging. Besides the cyber security challenges of CPSs, the security of the physical parts of CPSs, which are controlled by software-defined controllers based on computational algorithms, is indeed a new critical challenge. For example, physical devices like smart meters are deployed on the "client side", where hackers could have better chance to tamper them and intrude into smart grid. The software is the soul of CPSs. Therefore, innovative, sound software security engineering methodologies are sought to address the security challenges of CPSs. Some researchers consider Model-Based Engineering (MBE) or Model-Driven Engineering (MDE) as one of the key solutions to the handling of complex systems [8], including CPSs [5]. One of the main ideas of MBE/MDE is the engineering at the model level, a higher level of abstraction than the code level. This would allow better engineering security together with the system as well as providing the foundations for (semi-) automated (formal) verification or validation of the security of complex systems. Indeed, MDE methods have been actively developed for engineering the security of complex software systems very early and throughout the development life cycle as surveyed in [57]. In a recent study that assessed the state of the art and the state of the practice in the verification and validation of CPSs, the authors suggest that "*model-based approaches are gaining momentum, and it seems inevitable that model-based approaches will emerge that can be applied to general purpose CPSs*" [96]. By engineering systems via computer-readable models, model-based security engineering (MBSE) techniques could provide solutions to address the challenges for the security of CPSs. We call the MBSE approaches that are specifically developed or adopted for CPSs as MBSE4CPS. However, it remains a big question on how extensively the MBSE4CPS approaches have been developed. This paper aims to give an answer to this question.

After conducting a trial survey on the topic of MBSE4CPS, we found that this is an emerging interdisciplinary research area among several research fields such as software (system) engineering, (software) security engineering, and electrical/system engineering. Therefore, a systematic mapping study (SMS) would be useful to provide a picture of the MBSE4CPS research so far, in the interests of researchers and practitioners in the research fields mentioned above. We followed the latest guidelines in [66] to conduct a SMS on the existing primary MBSE4CPS studies. Thousands of relevant papers have been systematically filtered from four main online publication databases, and from an extensive snowballing process [89] to finally obtain a set of 48 primary MBSE4CPS studies. We extracted and synthesised data from the primary MBSE4CPS studies to answer our research questions. In the end, the key contributions of this work are our answers to the following research questions (and their sub-questions in Section 5):

- RQ1: What are the publication statistics of the existing primary MBSE4CPS studies in the literature?
- RQ2: What are the existing primary MBSE4CPS studies & their characteristics?
- RQ3: What are the open issues of MBSE4CPS research?

Besides, it is important to note that in complex systems such as CPSs, uncertainty is very likely to happen and must be handled [95]. From security's point of view, uncertainty in CPSs could lead to serious security issues. For example, some uncertainties in the functionalities of CPSs might lead to vulnerabilities that could be exploited by an adversary, either attacker or malicious user. Vice versa, any uncertainty in the specification, implementation, and evolution of security mechanisms might cause other uncertainties in the functionalities of CPSs, e.g., incorrect access control can disable some physical processes, especially whose real-time requirement is critical. On the other hand, security attacks could also cause uncertainties in the functionalities of CPSs. Therefore, while conducing this SMS we did keep in mind to check if any primary MBSE4CPS study explicitly deals with uncertainty.

The remainder of this paper is structured as follows. Section 2 provides some background concepts that are used in this paper. Then, we present in Section 3 our approach to conducting this SMS. Section 4 contains our classification schemes for the primary MBSE4CPS studies and other criteria for supporting the data extraction and comparison among these primary studies. Key results are described in Section 5 followed by threats to validity in Section 6. Related work is presented in Section 7. Finally, Section 8 concludes the paper with the major findings and some directions for future work.

2. Background

In this section, we provide some background concepts that are used throughout this paper. First, we recall in Section 2.1 the definition of SMS in relation to other types of secondary study such as Systematic Literature Review. In Section 2.2, the scope in which an approach can be considered as an MBSE approach is discussed in comparison with related concepts such as Model-Driven Security (MDS). Then, in Section 2.3 we define the scope in which a system can be considered as a CPS, and some fundamental security concepts in the context of CPSs.

2.1. Systematic mapping study vs. systematic literature review

According to [38], there are three different kinds of secondary study that would complement each other: Systematic Literature Review (SLR), SMS, and Tertiary Review (TR).