Chapter 9

A Self-Adaptive Software System for Increasing the Reliability and Security of Cyber-Physical Systems

Johannes Iber
Graz University of Technology, Austria

Tobias Rauter
Graz University of Technology, Austria

Christian Kreiner
Graz University of Technology, Austria

ABSTRACT

The advancement and interlinking of cyber-physical systems offer vast new opportunities for industry. The fundamental threat to this progress is the inherent increase of complexity through heterogeneous systems, software, and hardware that leads to fragility and unreliability. Systems cannot only become more unreliable, modern industrial control systems also have to face hostile security attacks that take advantage of unintended vulnerabilities overseen during development and deployment. Self-adaptive software systems offer means of dealing with complexity by observing systems externally. In this chapter the authors present their ongoing research on an approach that applies a self-adaptive software system in order to increase the reliability and security of control devices for hydro-power plant units. The applicability of the approach is demonstrated by two use cases. Further, the chapter gives an introduction to the field of self-adaptive software systems and raises research challenges in the context of cyber-physical systems.

INTRODUCTION

Cyber-physical systems (CPS) are the next-generation of systems that integrate computational and physical components. In contrary to the embedded devices of the last decades, they offer high performance, are interconnected and, with a good chance, somehow connected with the internet. Following DOI: 10.4018/978-1-5225-2845-6.ch009
this trend, control devices typically found in industry are going to manage more and more functionality with the help of sophisticated software. According to a National Institute of Standards and Technology workshop report (NIST, 2013) the key challenges of CPS development include what is needed to cost-effectively and rapidly build in and assure the safety, reliability, availability, security and performance of next-generation CPS. Industry is using more and more commercial off-the-shelf hardware platforms, which are inexpensive and offer a high performance. The downside of these platforms is that they typically only sparsely offer safety and fault tolerance features (Alhakeem et al., 2015). Further, industrial cyber-physical systems are becoming increasingly targets of security attacks (Miller & Rowe, 2012).

The inherent problem of CPS is complexity. This issue is going to escalate as CPS become large-scale distributed systems. They have to deal with uncertainty, change during operation, be scalable and tolerant to threats (Muccini, Sharaf, & Weyns, 2016). Self-adaptive software systems are systems that target to deal with complexity. Typically, self-adaptive software systems externally observe their managed systems, detect problems and adapt the managed systems in order to repair or circumvent inconsistencies. In the case of security, a self-adaptive software system can detect security attacks and isolate the infected devices or block the attackers. In the case of hardware faults, a self-adaptive software system can detect permanent hardware faults and move the application logic running on a managed system to an alternative hardware. Such problems would be complicated for a managed system itself to circumvent, but through an external overlooking system this becomes possible and the lurking complexity of CPS may become manageable.

Because of the increased performance and connectivity of modern and future hardware, self-adaptive software systems can be deployed to former restricted devices found in industry. In this chapter, ongoing research of an approach is presented that provides a novel application of a self-adaptive software system in an industrial setting, namely control devices for hydro-power plant units which is also the context of our research project. The goal of the presented approach is to increase the reliability and security of systems through anomaly detection and adaption. Simply put, we want to extend the time of control systems as long as possible so that they can carry out undisturbed their intended purposes.

The following Sections are structured as follows: First we give a detailed overview of the underlying principles of self-adaptive software systems. After that we extensive present our approach named Scari (Secure and reliable infrastructure); including an overview of our industrial setting (hydro-power plants), the vision of Scari, the detailed approach and two use cases. In the subsequent Section, we present a number of research challenges that we derive from our self-adaptive software system. Last, we conclude this Chapter.

BACKGROUND

Self-adaptive software modifies its own behavior in response to changes in its operating environment. By operating environment, we mean anything observable by the software system, such as end-user input, external hardware devices and sensors, or program instrumentation. (Oreizy et al., 1999)

Historically, the intention of building self-adaptive software systems has been around some time. Though not being the first talking and writing about self-adaptive software systems but making significant investments, IBM introduced in 2001 the Autonomic Computing Initiative in response to their observation that the main obstacle to further progress in the IT industry is a looming software complexity crisis (Kephart