Chapter 32
Secure Interoperability in Cyber-Physical Systems

Cristina Alcaraz
University of Malaga, Spain

Javier Lopez
University of Malaga, Spain

ABSTRACT

Transparency in control transactions under a secure network architecture is a key topic that must be discussed when aspects related to interconnection between heterogeneous cyber-physical systems (CPSs) arise. The interconnection of these systems can be addressed through an enforcement policy system responsible for managing access control according to the contextual conditions. However, this architecture is not always adequate to ensure a rapid interoperability in extreme crisis situations, and can require an interconnection strategy that permits the timely authorized access from anywhere at any time. To do this, a set of interconnection strategies through the Internet must be studied to explore the ability of control entities to connect to the remote CPSs and expedite their operations, taking into account the context conditions. This research constitutes the contribution of this chapter, where a set of control requirements and interoperability properties are identified to discern the most suitable interconnection strategies.

INTRODUCTION

In the last few years, we have witnessed how the advent of new technologies, such as the Internet and wireless communication infrastructures, has radicalized the current control systems, the infrastructures of which are becoming smarter with a strong dependence on heterogeneous cyber-physical systems (CPSs). CPSs are collaborative systems comprising autonomous and intelligent control devices (e.g., smart meters, gateways, servers working as front-ends, remote terminal units (RTUs), sensors, smart industrial engineering devices, mobile robots, smart-phones, and many other cyber-physical control elements) capable of managing data flows and operations, and monitoring physical entities integrated as part of critical infrastructures (CIs). A Smart Grid system is a clear example of the composition of these

DOI: 10.4018/978-1-7998-2466-4.ch032

systems based on complex communication infrastructures (Yan et al., 2012). Their technologies, from diverse vendors or manufactures, manage a set of fundamental services according to the real demand, facilitating effective energy production, the management and notification of electricity pricing, as well as the provision of customizable services to end-users.

However, the composition of diverse types of networks requires addressing aspects related to the interoperability, so as to ensure control from anywhere and at any time. Cyber-physical devices located at different locations should be managed irrespective of the types of devices and protocols, and they must allow control entities to assist in a situation when needed. To address this heterogeneity, it is necessary to include a set of fundamental requirements linked to the underlying interconnection system, among them: authentication, authorization and policy management because:

1. Any unauthorized access to restricted devices may become a threat, and
2. Authorized access under different policies may hamper the monitoring tasks.

Intermediary policy enforcement systems with support for dynamic access could be an easy way of ensuring interoperable communication between different CPSs. If, in addition, the context has to consider dynamic access, the resulting system is a decision-making system with the capability to adapt the access to the type of context. These fundamental conditions are primarily related to the connectivity phase in which control entities may require the absolute connection with the desired destination node; and this connection is strongly linked to the privileges assigned to the control entities (human operators, processes), the intentions of these entities in the field and the contextual conditions.

However, the construction of specific interoperability architectures may lead to certain questions related to:

1. Whether these architectures may directly connect with the end cyber-physical devices instead of going through the main interfaces (gateways or front-ends) that generally comprise the current control systems; or
2. To directly connect with the control devices (e.g., RTUs, sensors, actuators).

To do this, it is necessary to analyze the existing interconnection strategies of CPSs to the Internet to determine which approach is the most suitable for maintaining the interoperability in restricted control contexts, assessing the connection level and timely access in extreme situations. The result of all this research constitutes the main contribution of this chapter, which is organized as follows. First we contribute with a generic interconnection architecture based on decision points, so as to provide the architectonic basis required for subsequent research. In the third section we identify the control requirements that all CPSs and their devices have to comply with, and present the different interconnection strategies to substations (where the CPSs are deployed). Lastly, we evaluate and discuss the properties of the CPSs in the fourth section according to the present constraints of the control systems, and provide the conclusions and future work.

Secure Interoperability: Diversity, Interaction, and Collaboration

As mentioned, in the majority of CIs and their physical systems all activity must be supervised, either locally or remotely, by complex and decentralized monitoring systems comprising large and small com-