Computer Networks 134 (2018) 46–54

Contents lists available at ScienceDirect

Computer Networks

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

Access control for cyber-physical systems interconnected to the cloud

Javier Lopez, Juan E. Rubio*

Department of Computer Science, University of Malaga, Campus de Teatinos s/n, Malaga 29071, Spain

ARTICLE INFO

Article history:
Received 30 July 2017
Revised 7 December 2017
Accepted 18 January 2018

Keywords:
Cyber
Physical
Systems
Cloud
Security
Access
Control

ABSTRACT

The continuous advance in manufacturing and information analytics has improved the connectivity between computational and physical elements within the industry, hence increasing the effectiveness and reliability of Cyber-Physical Systems (CPS). This progress has been further enhanced by Cloud computing technologies, by externalizing services and interconnecting different industrial networks. As a consequence, there has been an increase of cyber-security threats in the industrial sector in recent years. Among other security measures, it is of paramount importance to introduce flexible access control mechanisms to avoid unauthorized access to the heterogeneous systems that coexist in this context. In this paper, we identify the requirements for such techniques, and propose a novel industrial architecture where multiple access control models are assessed when cloud technologies are integrated. In particular, we emphasize their adaptability to new heterogeneous scenarios through diverse indicators, achieving a trade-off between security and efficiency.

1. Introduction

A Cyber-Physical System (CPS) refers to a mechanical mechanism that is controlled by computational entities which work collaboratively: namely, sensors and actuators that capture data from the procedure and regulate its parameters according to a set of defined rules, hence achieving an interaction between the physical and computational components [1]. These systems have been deeply integrated in critical infrastructures (i.e., energy sector, transport) and generally in all industrial control systems for years. The initial goal of achieving intelligent, resilient and self-adaptable machines in this context has been eased in recent years by the increasing affordability of sensors and the rapid development of new communication networks and protocols. This has resulted in the continuous generation of high volumes of data and the integration with information technologies (IT). The most evident case is Cloud Computing. It is of key importance to understand the evolution of the industry towards a model where the product is flexibly manufactured by a network of suppliers accessible via the cloud along the whole production chain, with an extensive integration between customers and business partners.

The counterpart of the modernization of industrial technologies (which we will refer to as “operational technologies”, OT) and the interconnection of CPSs with external networks like the Internet brings with it the appearance of new cyber-security threats. Some of them are inherited from the IT paradigm and others arise from the growing integration between IT and OT assets. As a result, there has been an increase of vulnerabilities in the industrial sector in recent years, as some reports show [2,3]. We are talking about attack vectors such as denial of service, presence of malware, exploitation of vulnerabilities in communication protocols to intercept traffic, phishing and social engineering, etc. In terms of authorization and access control, which are the main focus of this work, they imply the misuse of resources and the misappropriation of the identity of nodes, that can even influence the overall behavior of the system. Altogether, these issues make security the main concern for the adoption of these technologies in such a critical scenario.

In this complex environment, where any element could potentially interact and cooperate with any other element, access control is essential to manage permissions of users, peripheral devices or programs when they request to use certain resources within the infrastructure. The integration of IT technologies and especially the cloud hinders the application of conventional access control models in industrial systems, for several reasons. These can be summarized in the sharing of information among heterogeneous entities with different degrees of sensitivity, performance and regulations. Therefore, it becomes mandatory to analyze the full range of requirements that access control presents in the upcoming scenario, in order to accurately tailor the available models and propose new approaches that meet these conditions. In particular, it is useful to consider how these security techniques can affect the physical world by introducing an extra overhead in the control and monitoring procedures.

* Corresponding author.
E-mail addresses: jlm@lcc.uma.es (J. Lopez), rubio@lcc.uma.es (J.E. Rubio).

https://doi.org/10.1016/j.comnet.2018.01.037
1389-1286/

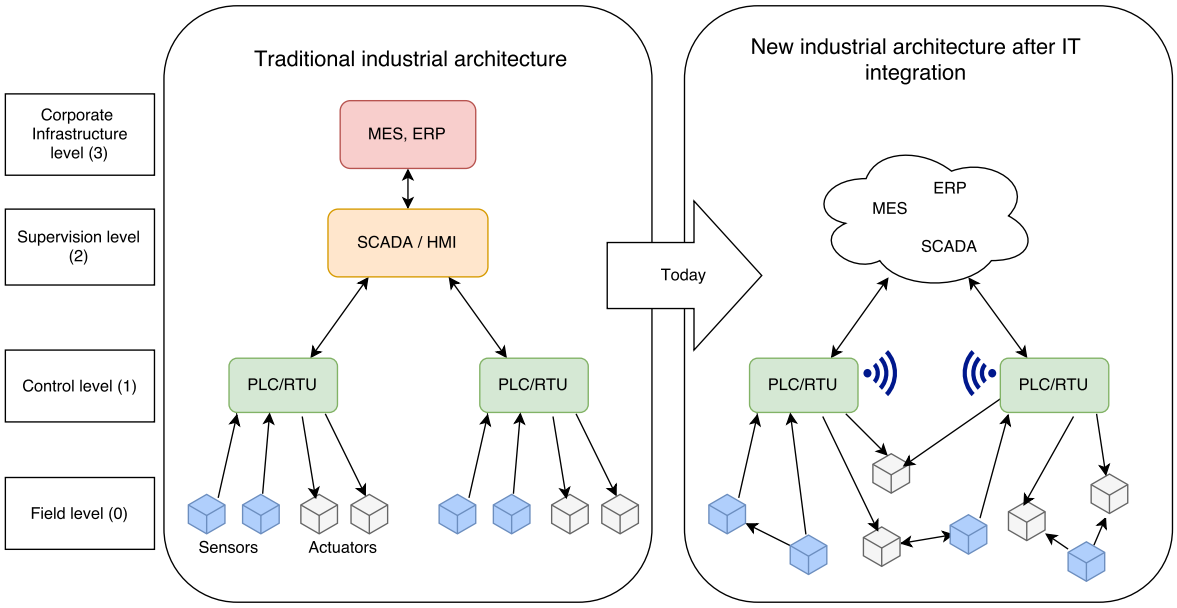

Fig. 1. Evolution of the traditional industry architecture.

In this paper, we identify the set of requirements that access control mechanisms must have in the industry as a consequence of the CPS and cloud interconnection, assessing the adaption of particular models. The paper is organized as follows: Section 2 exposes the requirements that access control solutions must match, taking the new architecture into consideration. Section 3 presents traditional approaches, whereas Section 4 describes new mechanisms in the literature. They are ultimately analyzed according to the aforementioned requirements in Section 5. Finally, conclusions and future work are presented in Section 6.

2. Access control requirements

In order to identify the requirements of access control in the CPS infrastructure, it is mandatory to firstly review how industrial networks are affected by the integration of IT technologies. A traditional control network follows the architecture described in the ISA-95 standard [4]. In this way, the productive process itself constitutes the base of the pyramid (level 0), whereas devices that interact with it (i.e., PLCs, RTUs) are set in level 1. Level 2 represents those devices that control the production process (i.e., SCADAs, HMIs), and those that control the workflow (i.e., MES systems) are located in level 3. Lastly, the highest level contains the infrastructure of logistics, inventory, ERP or planning.

The implementation of cyber-physical systems within this context means the introduction of advanced connectivity technologies and computational capabilities to ensure a real-time data acquisition from the physical world and an intelligent data management. The goal is to gather information from every connected machine and run specific analytics to extract additional insights, providing feedback from cyber space back to the physical space. In practice, this evolution is fostered by the implementation of several communication protocols due to the standardization of software and hardware: ranging from field bus protocols (i.e., HART; wirelessHART, etherCAP, IO-Link) to protocols working with Ethernet and TCP/IP, such as Ethernet/IP, Ethernet POWERLINK, CANopen, PROFINET, Modbus/TCP or HART/IP. The case of standards devised for the interoperable management of all types of industrial equipment, like CIP, OPC UA and MTConnect are especially interesting. On the whole, this results in the evolution of the traditional architecture towards a distributed and decentralized model, as Fig. 1 shows.

According to the new architecture model, devices located in the lower levels of the architecture interoperate with each other to interconnect all the components of the infrastructure, ranging from machines to operators or the product itself, in order to gather data. On the other hand, the cloud is leveraged to provide supervision as a service and interconnect different substations easily. By this means, a collaborative environment can be created by diverse companies whose applications and constraints may differ, making it difficult to reach a global agreement or the adoption of any common specification.

In this complex scenario, access control mechanisms deployed (either in field devices, PLCs or cloud resources) aim to restrict what each entity should be able to access and the connections that can be accepted, having the ability to deal with a diversity of devices [5]. Actual solutions are still in their infancy, due to the need for a dynamic and fine-grained mechanism that deals with several users and constrained resources. We can thereby define the following set of specific requirements, based on an extensive review of the literature with the aim to study which features the models need for this particular context:

- *Dynamicity:* services in modern CPSs are accessed remotely by a large number of technologies and protocols, which are also added or removed on demand. Due to cloud computing, several applications could be integrated in the product life cycle, ranging from monitoring procedures (e.g., inventory, real-time performance) to dynamic manufacturing processes defined on the go, which could change their parameters dynamically. Virtualization elements of cloud computing also offer scalability in terms of resource allocation, which in turns introduces a challenge for access control systems with the control of multiple user accounts.
- *Scalability:* access control must accept the definition of new users and complex policies, while not introducing operational costs. It should be extensible with respect to the number of users and resources controlled, including the adaptation to new technologies (e.g., communication protocols, operating systems) through well defined interfaces. It is important that the access control system has a situational awareness of all factors involved in the authorization decisions at all times: this involves parameters such as the number of connected devices, and their available resources.