Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 50-1 (2017) 5837–5842

Using a Virtual Plant to Support the Development of Intelligent Gateway for Sensors/Actuators Security

Thomas Toublanc, Sébastien Guillet, Florent de Lamotte, Pascal Berruet, Vianney Lapotre

Univ. Bretagne-Sud, UMR CNRS 6285, Lab-STICC, 56100 Lorient, Fr.

(e-mail: firstname.lastname@univ-ubs.fr)

Abstract: Our industries are facing a new revolution, about Connectivity, Information and Network. Nowadays, the threats on industrial cyber physical systems are not just theoretical. They can do major damage to our real world through cyberspace. In this paper, a demonstrator for security on Sensor/Actuator network in industrial applications is proposed. It consists of an operational part simulator SimSED and automation emulator Straton Runtime, linked together by TCP/IP. This demonstrator is dedicated to evaluate a secure gateway for security in Network Control System (NCS). Two support bricks of the gateway are introduced. The first one is a filter for demonstrator protocol. The second one an auto-generated input/output model which represents the protected system. The intelligent gateway will support safety, reliability and resilience objectives for security of NCS.

Keywords: Discrete events modeling and simulation, Networked embedded control systems, Cyber-Physical Systems, Control over networks.

1. INTRODUCTION

Cyber Physical System (CPS) interfaces cyber and physical worlds through modern Intelligent Control Systems (ICS). CPS are found in many domains (i.e. power distribution, process industries, transport and services) and more of those are widespread logically and physically. This leads to more security threats. Therefore their needs in security is a primary concern, as their failure or malfunction induce major damage on humans, environment, economy and society. CPS is composed of several parts summarized in Fig.1. The first one is office Information Technology (IT): network between computers, servers, intranet and Internet environment (i.e. cloud, mail and other services). This high-level network can be supervised by a Security Operational Center (SOC). By direct access to office IT networks through the Internet or intranet, it catches all logs from servers, firewalls and computers. The goal is to respond to cyber-attacks dynamically and they cover a large area of expertise to detect, respond and treat CPS high levels (i.e. Corporate network (CN) and Process Supervision (PS)). The second one is an interface between the two others normally secured by DeMilitarized Zone (DMZ). The most largely deployed solution is named Supervisory Control and Data Acquisition (SCADA). It permits remote control of operational subsystems, distribution of process data across ICS or the Internet for several office IT applications and Network Control System (NCS). Several researches and warnings about SCADA systems are presented by Miller and Rowe (2012). Although interfaces between SCADA and SOC exist, the main targeted threats are related to data security. The last part: the NCS, which links across several and occasionally different Industrial Locals Networks (ILN) Process Intelligence (PI) (i.e. automation or controllers), Process Actor (PA) (i.e. Sensor/Actuator (S/A), smart S/A or robots). They are Distributed (DNCS), centralized or hierarchical and widespread.

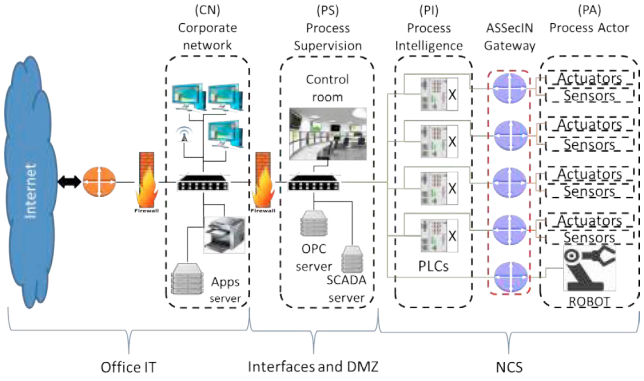

Fig. 1. CPS Description

The firewalls used in office IT and DMZ, do not protect low levels (i.e. PI and PA). Some precondition like direct or proximate access to PI or PA components through USB, radio frequency, network plug and Internet facing are becoming threats. Denial of services, man in the middle or hijacking are possible attacks leading to a major impact on the real world. The solution presented in this paper is a secure gateway at NCS level as illustrated in Fig.1. The gateway goal is to detect, identify, and react to threats from PI or PA, by checking information integrity and consistency within the system. This paper presents a

10.1016/j.ifacol.2017.08.541

software demonstrator to test relevance of the solution.
In the following, Section 2 gives an overview of CPS platforms, their security and a positioning. Section 3 presents secure gateway concept. Section 4 describes the demonstrator. Section 5 presents the experimental setup.

2. CPS SECURITY: STATE OF THE ART

CPS are built to be durable, some of them are already over 20 years old and even with technical updates they are vulnerable. Their lifespan is relative to those of their weakest parts. Industries are vulnerable to attacks, Dzung et al. (2005) proved it and they detailed security characteristic of ICS. CPS is highly networked, Cheminod et al. (2013) reviewed security issues about it. NCS is exposed to both old threats (i.e. technical issues, human negligence and wear of a system) and new ones (i.e. cyber-attacks).
During last decades, many researches on control over the network and embedded control have emerged. For instance, Tipsuwan and Chow (2003) studied control methodology to reduce delay in NCS. Research trends with challenges for NCS is given by Gupta and Chow (2010).

2.1 CPS platforms

Many projects about CPSs platforms were started in Europe, Asia or USA. Leitão et al. (2015) present an overview of four European projects and compare them.

(1) SOCRADES: Colombo et al. (2010)
(2) GRACE: Castellini et al. (2011)
(3) IMC-AESOP: Colombo et al. (2014)
(4) ARUM: Marin et al. (2013)

(1) introduces service-oriented architecture paradigm for automation. Peculiar automation services implementation for distributed smart embedded devices, components of industrial Internet of things. (2) introduces multi-agent systems which integrate quality and process control. Also it presents an implementation of high-level solutions for manufacturing execution system. (3) is about service-oriented process, monitoring and control. It introduces the next-generation of SCADA and DNCS. (4) presents adaptive production management. The goal is to introduce a high-level solution of scheduling tools to respond to unexpected events. Lerner (2015) gives five Trust Requirements (TR) to design trustworthy components of CPS.
TR1: The source code is analyzed. TR2: The component uses private hardware resources. TR3: All external communication is through hardware-implemented, bounded, and isolated queues. TR4: The component cannot be bypassed or disabled. TR5: Critical functionalities cannot be updated without secure or physical access.
The platform reviewed do not integrate security at low level specifically at NCS level.

2.2 Security in CPS review

CPS are migrating. In the future distributed network with embedded cyber physical control systems will be standard. Research on embedded system security warns us. For instance, Papp et al. (2015) present different ways the attackers can pike to achieve their goal. The security is a general term relying on four objectives safety, reliability, resilience, and security. Lu et al. (2015) reviewed these objectives and present a CPS security architecture.

At design time Nowadays, with new design method like formal checking Kwiatkowska et al. (2011), which guarantee the knowledge of the system behavior, at every time. Controllers synthesizing Pnueli et al. (1998) permit synthesis of the appropriate controller for specific set of controllable variables and constraints. Guillet et al. (2013), used it in another domain, but security is the main objective and the method can be transposed to industrial equipment. These solutions lead to robust systems which answer resilience objectives. The choice of equipment and maintenance policy answer to reliability and safety objectives. Another way to secure industrial systems is by adding flexible organization to the system, Berruet (2007) presents at design time, simulations to determine models of organization and solution issues at run time.

At run time The Reconfigurable Manufacturing System (RMS) problematic: faulty subsystems in CPS are not threats, because they can be detected, the global system continues to fulfill the process needs. It has several solutions through plurality (i.e. redundancy), flexibility, and knowledge of other functional organizations, like presented by Lamotte et al. (2007), which answers resilience objectives. But RMS solution needs fault diagnosis to trigger reconfiguration process. Gao et al. (2015) reviewed two different approaches to fault diagnosis for industrial control systems. Another kind of reconfiguration can be done, through networks like presented by García et al. (2004). Industrial systems are time dependent or relative, that is why Saddem and Philippot (2014) introduce causal temporal signature. It permits to intricate time and value in a model and permits fault detection.
Security in NCS can be achieved at runtime or design time. For newer it is better to do it at design time. For older by interfacing new technologies or by updates. The proposed gateway is relative to the second option.

2.3 Related Work & Positioning

Franklin et al. (2014) investigates hardware security gateway with trustworthy autonomic interface guardian architecture. Their philosophy: *"the most trusted layer of a system should validate request from the less ones."* is interesting but in our context is incomplete. Even S/A have malfunctions, so resilience and reliability are linked. Sunindyo et al. (2011) present a method to enforce runtime safety objectives with knowledge of users or stakeholder initial needs. The safety is an objective for our secure gateway. Zerkane et al. (2016) introduce the first software defined network reactive firewall. This principle is interesting specially in DNCS with real time constraints. Sentryo (2000) presents another way to deal with security in ICS. Probes are deployed on network equipment (i.e. switch, gateways, hub), the aim is to secure high-level network office IT. The probes are connected to a center which has the intelligence to detect attacks. We draw on these principles to perform the same kind of detection but at low level. The demonstrator presented in this work permits to simulate a controlled system with a gateway integrating different principles and evaluate it.