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.

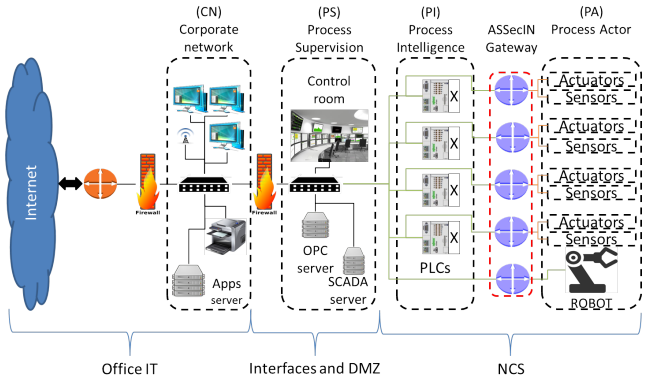

Fig. 1. CPS Description

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

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.

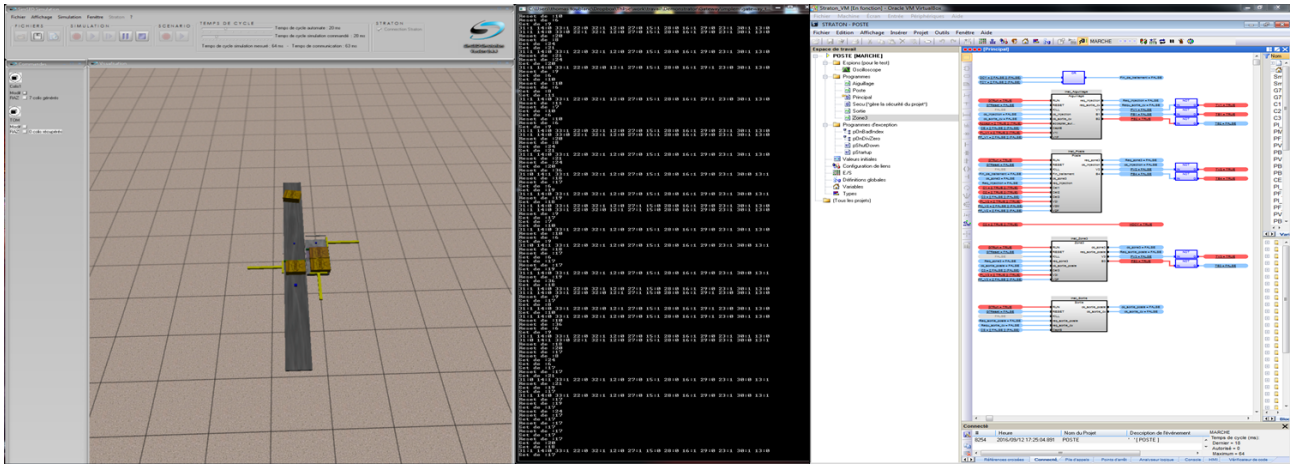

Fig. 2. Demonstrator presentation

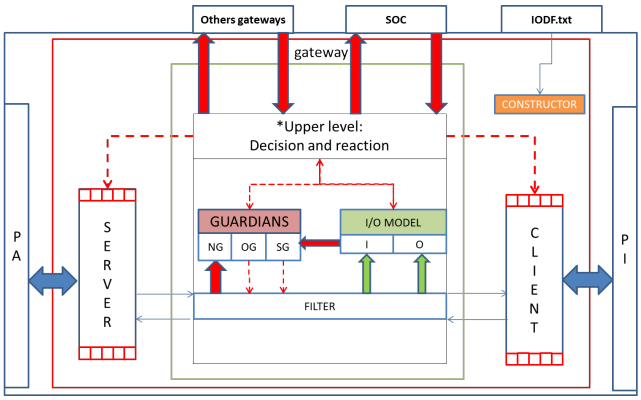

Fig. 3. Secure gateway representation

3. SECURED GATEWAY CONCEPT

Fig.3 details the concept of the secure gateway. The gateway uses man in the middle principles on ILN. The frames are received by the server or client and passed through a passive filter presented in 4.3.2. At the initial phase I/O model detailed in 4.3.1 is constructed. I/O model is a real-time image of the system reconstructed from the filtered communication. When frames have proper characteristics, filter updates the I/O data in the model. The guardians: Operational Guardian (OG), Safety Guardian (SG), Network Guardian (NG) have to satisfy security objectives and they act like agents.
The NG monitors traffic, the filter provides it logs for every frame (i.e time, size, type, source, recipient). NG analyzes filter logs and detects if the network is under attack. The SG is a reflex module which triggers the filter. It checks update of the I/O model and if the safety of the system is not overstepped it allows the frame passage. The aim is to assure the safety of the system and human at every time. The OG monitors the system using action reaction principle (e.g. Causal Temporal Signature) and profiling. It uses I/O model and is time relative. The goal is to detect malfunctioning of the system. The three guardians are interfaced with an upper level which supervise them and communicate with SOC or other gateways on the system. The Upper level implements decision and reaction mechanism but it acts in a delayed time unlike SG which is in real time.
To test the proposed concept, a demonstrator has been setup and is described in the next section. Moreover the implementation of the support bricks for the secure gateways relative to the demonstrator is presented.

4. DEMONSTRATOR SETUP

We propose a software Demonstrator designed to simulate a DNCS, which integrates a secure gateway implemented with several hypotheses:

Hypothesis 1. At very-low level in the system, closer to the physical world, better detection and reaction is possible.

Hypothesis 2. Mix safety, reliability and resilience.

Hypothesis 3. Secure gateway knows the system.

Hypothesis 4. The gateway does not induce latency on NCS.

The demonstrator, shown in Figure 2, makes use of the SimSED simulator as shown *on the left*, the secure gateway is *in the center*. Finally, the Straton virtual machine is shown *on the right*. these different parts are described in the following sections.

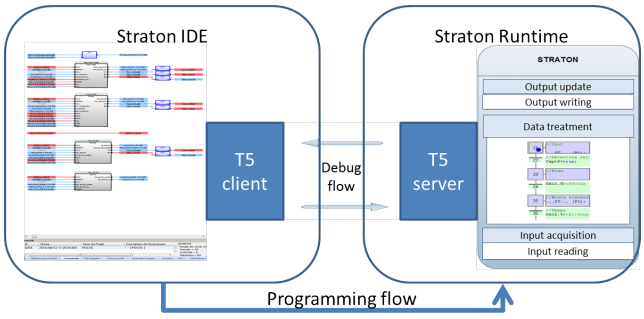

Fig. 4. Straton tool presentation

4.1 Straton

Straton is a toolkit to design and run automation programs. Fig.4 details its use. It consists of an IDE, a Runtime and features a proprietary protocol for communications namely T5.

Straton IDE (Integrated Development Environment) permits to write software compatible with IEC 61131-3 standards. At run phase, it permits to observe I/O and running state of the program through TCP/IP.

Straton Runtime executes automation code and has a TCP server for communication. In this work it is used to simulate control program execution, with real programs used on physical platform.

T5 is the proprietary network protocol of Straton, it is used both for programming/debug and communication between runtime and SimSED or gateway. It is a TCP/IP client-server base.

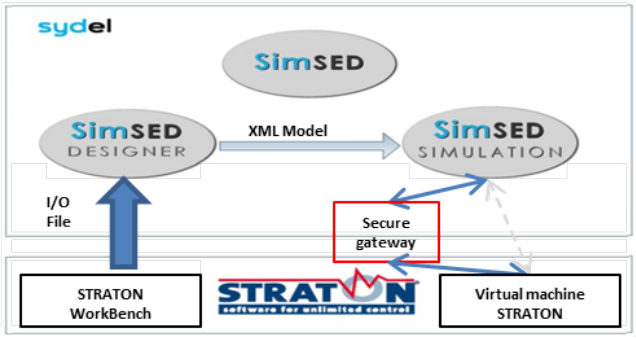

Fig. 5. SimSED tool presentation and gateway positioning

4.2 SimSED

SimSED is an operational part designer and a simulator presented in Bévan et al. (2012). A presentation of the development and simulation flow is given in figure 5. It shows the location of the secure gateway between the Straton runtime and SimSED satisfying hypothesis.1.

SimSED designer is a development environment that uses a component based-approach to model the system. A physical system is modeled and seen as an assembling of Process Components (PC) (i.e. process action on the product). Every PC is composed of one Contextual Effective Component (CEC). Relying on Basic Enriched Component (BEC) composed of Basic Component (BC), and Support Component (SuC). But some BC or SuC are interfaces between CEC and our primary concerns. The designer takes I/O Device File (IODF) from Straton to link to Sensor & actuators of CEC.

SimSED simulator is a physical simulator engine as close to reality as possible. It integrates a physical engine called OpenDynamic Engine (Smith et al. (2005)) and a hazard generator. It was designed to detect critical points of the system. The hazard generator is used to create scenarios with any component (set, reset, parameter changes), relative to the time, the number of products or at random. In this work it is used to test the capacity of the gateway to detect physical attacks or malfunctions on the system.
The simulator is a client of the Straton Runtime through T5 protocol as described in sec 4.1 and runs a step-by-step simulation. It uses continuous simulation, which respects Straton runtime cycle and manages the synchronization.

4.3 Secure gateway implementation

The support bricks of the gateway as presented in section 3 are implemented to be integrated in the demonstrator.

I/O model generation: The aim is about gateway knowledge of the system and to interface SG and OG. Also it facilitates adaptability of the gateway for other systems. At initialization phase of the secure gateway, a reading of the I/O description file from Straton permits the construction of I/O Description Structure (IODS). These structures contain critical data for I/O variable (VAR) (i.e. VAR_{name}, $VAR_{addresse}$, VAR_{type}, $VAR_{initial-state}$, $VAR_{current-state}$, ...).

Filter: The goal of the filter is not about blocking frames but to acquire critical data with security requirements to update I/O model and satisfy the hypotheses (2) and (4). A study during the run phase, without the secure gateway has been done. It determines that only 13% of the frames are useful for security concern. This study had characterized T5 frame filter with two parameters the size and $frame_{index}$.

(1) $Input-Frames$ of 13 Bytes which writes sensor data from SimSED for Straton.
(2) $Output-Frames$ which writes actuators data from Straton for SimSED. Those frames have a static size. $size = 10B + Nb_{output} \times 5B$.

$Output-Frames$ are cyclic and send at every step. Only output changes are interesting to update I/O model. A second level had been implemented, to filter (2).

$$Frame_{Index} = \sum_{i=1}^{n} \begin{cases} Var^{i}_{Adresse} + 2^{i} & \text{if } Var^{i}_{State} = 1 \\ 0 & \text{if } Var^{i}_{State} = 0 \end{cases} \quad (1)$$

Algorithm 1. T5 protocol frames filtering for security requirements

Require: x is a new frame captured of size y, u is a memorized frame index, z is number of Straton output link to SimSED t data length in frame

```
1:  function COMPARE(x, u)
2:      δ ← x ⊕ y                    ▷ ⊕: 2nd level filter equation 1
3:      if δ ≠ u then
4:          δ ← u
5:          return TRUE
6:      else
7:          return FALSE
8:  while x = TRUE do
9:      if y = 13 then
10:         Let pass the frame
11:         Transmit for analysis
12:     else if y = z then
13:         σ ← COMPARE(x, u)
14:         if σ = TRUE then
15:             Let pass the frame
16:             Transmit for analysis
17:         else
18:             Let pass the frame
19:     else
20:         Let pass the frame
```

A description of the filter algorithm is given in algorithm 1, which permits to induce minimum latency. Not all frames will be used to update I/O model, but information about all frames are provided to NG.
Now that the demonstrator has been introduced. A presentation of an experimental setup to test it is given.

5. EXPERIMENTAL SETUP

The use case for the demonstrator is modeled from a real system in our laboratory.

5.1 SimSED use case

Figure 6 is representing the global system, five stations around a supplier ring. This is a discrete and distributed system. The gateways have to secure each subsystem (i.e. stations, supplier ring) and automation.

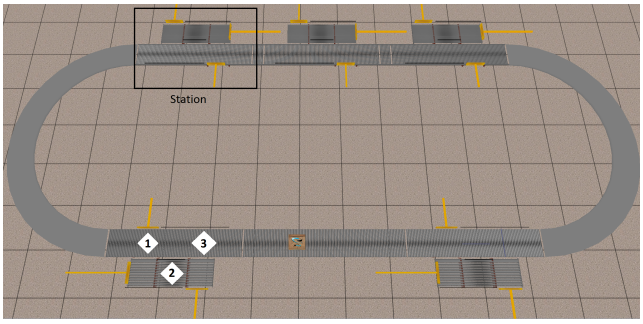

Fig. 6. Use case simulate by SimSED

Figure 7 describes one station and all components. The station is composed of three jacks V1, V2, V3 four stops B1, B2, B3, B3 and two conveyors one for supplier ring and another for the station. V1 intercepts parcels/products on supplier ring. V2 moves products across the station during treatment. V3 ejects the product after treatment on supplier ring.

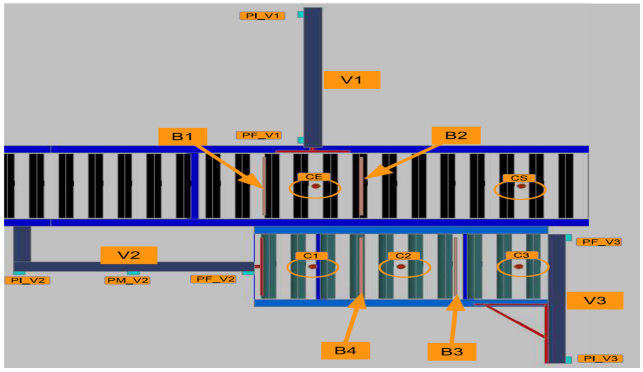

Fig. 7. Subsystem representation

Figure 8 gives a structural decomposition of the system as modeled in SimSED. A representation of the links between IODS and SimSED component is provided. Several IODS are linked together in BEC or SuC, for BC only one IODS is linked. Also some SuC or BC are common to several CEC.

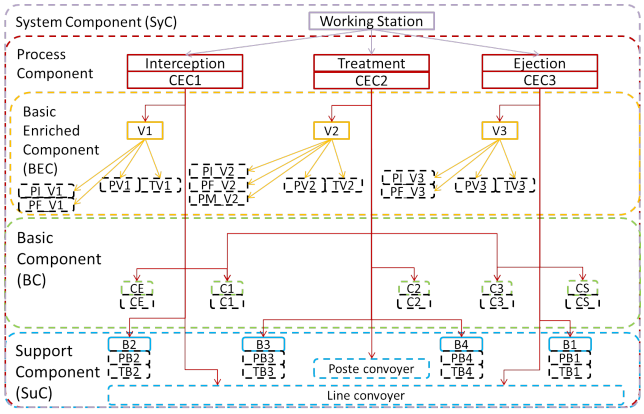

Fig. 8. SimSED model representation

5.2 Control Program

The control program has three tasks: Interception, Treatment, Ejection. It was implemented with three process zones shown in figure 6: switch (♢1), treatment (♢2) and eject (♢3). When a product is detected by (CE) and accepted by the station, the interception task request zone (♢2) and move the product when free. When a product had been treated ejection task request zone (♢3) and move the product when available. Another control program has been developed for the corrupted Straton attack scenario. It implements a commanded mechanism to activate all output at a certain time or amount of product. The SimSED simulator let us use five runtimes with the same program for our five stations.

5.3 Execution of the simulation

An experiment has been executed on our demonstrator with only one station. During the experiment SimSED measured 57ms for communication time without gateway and 59ms with it. So the gateway induces on average 2ms of latency. The runtime has 18ms cycle time and simulator measured 60ms of simulation time. The latency induced by the gateway does not interfere with the simulation.
The demonstrator parts, uses physical network interface, which permits a monitoring through a network analyzer. Also it provides weakness similar to those of NCS and exploited by our scenarios.
Three attack scenarios can be carried out on the platform, the first one uses hazard generator of SimSED to test OG and detect malfunctions or physical attacks. The second one uses a malicious client in parallel of SimSED which sends frames to test NG and detect DoS attacks. The third one use corrupted Straton sending malicious orders to test the protection of the system by SG.

6. CONCLUSION

In this Paper a demonstrator has been introduced. It is composed of three parts: an operational part simulator SimSED, a Straton tool-chain IDE and Runtime, and the first draft of a secure gateway.
The demonstrator can simulate the physical use case and monitor all communications. Secure gateway can filter T5 frames to keep only desired ones for security objectives. Also it can generate a first model of the system which will

be the interface for security requirement implementation at the second step. The monitoring combined with filtering and model permitting to observe in the console at runtime the set or reset of sensors from SimSED and output change from Straton.

Now that the demonstrator is set up, security functions (i.e. guardians) of the gateway can be implemented. The second perspective is about communication between gateways and with SOC to take a decision about the reaction at a global system level. This reaction are about process preservation. The third one is about knowledge of the system by the gateway, which could be augmented by analyzing the component model of the system provided by SimSED. The last one is about physical deployment: The experiment with the secure gateways on the demonstrator is not sufficient to prove transparency of the gateway, but it can be deployed and connected to the real system to validate this problematic.

ACKNOWLEDGEMENTS

This work is founded by Brittany Region, Morbihan department and sponsored by Syleps, which supplies SimSED simulator. The authors thanks Syleps team and Romain Bévan for their time and fruitful discussion.

REFERENCES

Berruet, P. (2007). Simulation of reconfigurable systems: from control code simulation to reflective simulation. In *European Conference on Modelling and Simulation (ECMS)*, 290–294. Prague, Czech Republic.

Bévan, R., Berruet, P., de Lamotte, F., Adam, M., Cardin, O., and Castagna, P. (2012). Generation of multiplatform control for transitic systems using a component-based approach. ETFA '12, 1–8.

Castellini, P., Cristalli, C., Foehr, M., Leitão, P., Paone, N., Schjolberg, I., Tjnns, J., Turrin, C., and Wagner, T. (2011). Towards the integration of process and quality control using multi-agent technology. In *Industrial Electronics Society (IECON)*, 421–426.

Cheminod, M., Durante, L., and Valenzano, A. (2013). Review of security issues in industrial network. *IEEE TII*.

Colombo, A.W., Karnouskos, S., and Mendes, J.M. (2010). *Factory of the Future: A Service-oriented System of Modular, Dynamic Reconfigurable and Collaborative Systems*, 459–481. Springer London, London.

Colombo, A., Bangemann, T., Karnouskos, S., Delsing, J., Stluka, P., Harrison, R., Jammes, F., and Lastra, J.L. (2014). *Industrial Cloud-Based Cyber-Physical Systems: The IMC-AESOP Approach*. Springer Publishing Company, Incorporated.

Dzung, D., Naedele, M., Von Hoff, T.P., and Mario, C. (2005). Security for industrial communication systems. In *Analysis, Design, and Evaluation of Human-Machine Systems (HMS)*, 1152–1177. Kyoto, Japan.

Franklin, Z.R., Patterson, C.D., Lerner, L.W., and Prado, R.J. (2014). Isolating trust in an industrial control system-on-chip architecture. In *Resilient Control Systems (ISRCS)*, 1–6.

Gao, Z., Cecati, C., and Ding, S.X. (2015). A survey of fault diagnosis and fault-tolerant technique–part1:fault diagnosis with model-based and signal-based approaches. *IEEE TIE*.

García, J., Palamo, F.R., Luque, A., Aracil, C., Quero, J.M., Carrión, D., Gámiz, F., Revilla, P., Prez-tinao, J., Moreno, M., Robles, P., and Franquelo, L.G. (2004). Reconfigurable distributed network control system for industrial plant automation. *IEEE TIE*.

Guillet, S., Bouchard, B., and Bouzouane, A. (2013). Correct by construction security approach to design fault tolerant smart homes for disabled people. *Procedia Computer Science*, 21, 257–264.

Gupta, R.A. and Chow, M.Y. (2010). Network control system: overview and research trend. *IEEE TIE*.

Kwiatkowska, M., Norman, G., and Parker, D. (2011). *PRISM 4.0: Verification of Probabilistic Real-Time Systems*, 585–591. Springer Berlin Heidelberg, Berlin, Heidelberg.

Lamotte, F., Berruet, P., and Philippe, J.L. (2007). Using model engineering for the criticality analysis of reconfigurable manufacturing systems architectures. *International Journal of Manufacturing Technology and Management (IJMTM)*, 11.

Leitão, P., Colombo, A.W., and Karnouskos, S. (2015). Industrial automation based on cyber phisical systems technologies: Prototype, implementation and challenges. *Comput. industry*.

Lerner, L.W. (2015). *Trustworthy embedded computing for cyber-physical control*. Ph.D. thesis, Virginia Polytechnic institute and state university.

Lu, T., Lin, J., Zhao, L., Li, Y., and Peng, Y. (2015). A security architecture in cyber-physical systems: Security, analysis, simulation and application. *International journal os security an its application*.

Marin, C.A., Monch, L., Leitão, P., Vrba, P., Kazanskaia, D., Chepegin, V., Liu, L., and Mehandjiev, N. (2013). A conceptual architecture based on intelligent services for manufacturing support systems. In *Systems, Man, and Cybernetics*, 4749–4754.

Miller, B. and Rowe, D. (2012). A survey scada of and critical infrastructure incidents. RIIT '12, 51–56. ACM, New York, NY, USA.

Papp, D., Ma, Z., and Buttyan, L. (2015). Embedded systems security: threats vulnerability, and attack taxonomy. *Privacy, Security and Trust*.

Pnueli, A., Asarin, E., Maler, O., and Sifakis, J. (1998). Controller synthesis for timed automata. In *Proc. System Structure and Control. Elsevier*. Citeseer.

Saddem, R. and Philippot, A. (2014). Causal temporal signature from diagnoser model for online diagnosis of discrete event systems. In *Control, Decision and Information Technologies (CoDIT)*, 551–556.

Sentryo (2000). Solution for cyber security for industrial internet. `https://www.sentryo.net/fr/`.

Smith, R. et al. (2005). Open dynamics engine.

Sunindyo, W., Melik-Merkumians, M., Moser, T., and Biffl, S. (2011). Enforcing safety requirements for industrial automation systems at runtime position paper. In *Requirements@Run.Time (RE@RunTime)*, 37–42.

Tipsuwan, Y. and Chow, M.Y. (2003). Control methodologies in network control systems. *Control Engineering Practice 11*.

Zerkane, S., Espes, D., Le Parc, P., and Cuppens, F. (2016). *Software Defined Networking Reactive Stateful Firewall*, 119–132. Springer International Publishing, Cham.