Une plateforme pour l'évaluation de la cybersécurité des systèmes de contrôle industriels et IOT

Mohamad Kaouk, Francois-Xavier Morgand, Jean-Marie Flaus

UNE PLATEFORME POUR L'ÉVALUATION DE LA CYBERSÉCURITÉ DES SYSTÈMES DE CONTRÔLE INDUSTRIELS ET IOT

A TESTBED FOR CYBERSECURITY ASSESSMENT OF INDUSTRIAL AND IOT-BASED CONTROL SYSTEMS

Mohamad KAOUK, Francois-Xavier MORGAND et Jean-Marie FLAUS
Univ. Grenoble Alpes, CNRS, Grenoble INP*, G-SCOP, 38000 Grenoble, France
* Institute of Engineering Univ. Grenoble Alpes

Résumé

L'introduction de l'Internet des Objets (IoT) dans les systèmes de contrôle industriel (ICS) les a exposés à de nouvelles menaces. Face à ces menaces, les méthodes de simulation et les plateformes de test sont utilisées pour modéliser le comportement des ICS et pour la recherche et le développement de la cyber-sécurité. Cependant, la plupart des solutions existantes ont été développées comme des systèmes isolés qui n'interagissent pas avec le monde extérieur, et donc, ne sont plus adaptées pour l'évaluation des nouveaux ICS. Dans cette étude, nous présentons une nouvelle plateforme pour les ICS dans un environnement IoT. La plateforme peut être facilement configurée par simulation ou du matériel réel en fonction des besoins. Nous montrons aussi l'utilité et l'efficacité de notre solution à travers plusieurs études de cas.

Summary

The introduction of Internet of Things (IoT) technologies in Industrial Control Systems (ICS) has exposed them to new threats. To cope with these threats, simulation and testbeds tools are used to model the ICS behavior and to provide support for cybersecurity research and development. However, most existing solutions were developed as isolated systems, which do not interact with the external world. Therefore, these solutions are not suitable for the assessment of new ICSs architecture. In this study, we introduce a novel testbed architecture for an ICS in an IoT environment. The testbed can be easily configured with simulation or real hardware depending on the experiments' needs. The applicability of the developed testbed is demonstrated through various case studies in order to present how it can be efficiently used.

1. Introduction

Due to the increasing demands on production quality, system performance and economic requirements, industrial manufactures always require being monitored and controlled to ensure their reliability and safety. Therefore, Industrial Control Systems are often found in the industrial sectors and critical infrastructures to monitor and control industrial processes. Industrial Control System (ICS) encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC).

Recent years have observed various successful demonstrations of the emerging Internet of Things (IoT) technologies and its related domains, such as wireless networks (WSN), big data, and cloud computing. In the industrial area, the Industrial Internet of Things (IIoT) gives rise to what is predicted to be a sweeping change that will fundamentally reconfigure industry. It is being called the 4th Industrial Revolution or 'Industry 4.0'.

In the era of Industry 4.0, IoT technologies are being applied to various critical infrastructure to create what we call Cyber-Physical Systems (CPS). CPS is the integration of computation with physical processes in which embedded computers and networks monitor and control the physical processes through a feedback loop in a networked environment. This integration allows machines to simultaneously optimize their efforts in response to conditions, predict their own failures, gather data about their performance, broadcast alerts and adjust their operations accordingly. In particular, in the field of ICS, the introduction of IoT and WSN technologies has led to several enhancements in term of remote monitoring and control (Sajid *et al.,* 2016). This has resulted in increasing system efficiency, scalability, and reducing cost.

The benefits of using IoT technologies in industrial infrastructure are thus clear. However, this also brought new challenges. Security and interoperability are considered the two biggest challenges facing the implementation of in the industry. Interoperability in the Industrial IoT concerns the convergence between old Operational Technologies (OT) and new Information Technologies (IT), which use different protocols and have different architectures. On the other hand, ICSs that were previously operated as standalone are becoming today connected with the external world (Abdo et al., 2018). In fact, classical SCADA systems are already lacking with security problems, and with the increased interconnectivity to the Internet, they are now exposed to new types of threats and cyber-attacks (Sajid *et al.,* 2016).

Therefore, various security technologies are being researched and developed to cope with cyber vulnerabilities and threats (Nazir *et al.,* 2016). However, it is risky to apply novel security technologies that are not verified as secure, to control systems, the availability of which must be guaranteed all time. Such situation calls for the need of an experimental setup equivalent or quite close to the real scenario where experiments for cybersecurity can be performed safely.

To better understand how to protect ICS, universities, governments, and industry-based researchers have begun to develop testbed solutions that model industrial control systems to support cybersecurity research and development in this domain. These solutions have been used to provide accurate assessments of the effects that cyber-attacks may have on the critical infrastructure. On the other hand, testbeds provide an ideal environment where security solutions can be tested and evaluated.

In this paper, we present our testbed solution: GSCOP-testbed. Our solution provides a tangible source of data and an experimentation platform that other researchers and industrials may use to study and validate cybersecurity in

their systems. The key benefit of our solution is that it provides a set of experimental capabilities that are missing from other approaches, e.g.:

1. A novel architecture for an ICS that combines old industrial protocols with new IoT protocols.
2. Flexibility to use different physical processes.
3. Flexibility to configure testbed components with simulation or real hardware depending on needs.

The remainder of the paper is organized as follows. Section II enumerates previous testbed development. Section III explains the main problems with existing testbed. Section IV provide a detailed description of the proposed solution. Section V demonstrates the utility of the testbed by presenting various case studies. The paper concludes in section VI.

2. Related work

Many efforts have been made by various universities and national research laboratories to develop testbeds that simulate the behavior of Industrial Control Systems. The most commonly mentioned objectives in developed testbeds were vulnerability analysis, education, and tests of defense mechanisms. These objectives highlight the fact that most testbeds focus on cybersecurity rather than performance and analysis.

A testbed that use real components is the National SCADA Testbed (NSTB) which represents a national lab collaborative project (Idaho National Laboratory, 2007). This environment implements actual physical grid components and helps to discover and addresses critical security vulnerabilities and threats in the energy sector. The testbed has contributed to the production of a SCADA-specific security assessment methodologies. In another work, (Fovino et al., 2010) have also proposed an approach that uses only real components to develop a testbed environment that reproduces the physical dynamics of a power plant with height fidelity to study the cyber vulnerabilities of power plant control systems. Therefore, the authors have developed a platform consisting of pipes, valves, sensors, pumps used to physically emulate the different states and thermo-dynamical processes of a real power plant. The system is directly connected, through a field network and a process network, to the SCADA server typically used to control the power plant. The testbed was used to demonstrate the vulnerabilities of electric power systems against cyber-attacks and to study the effects that could have these attacks on the system. These testbeds would provide reliable experimental data, since everything is real, however, they are counterbalanced with the high cost and complexity of deployment and maintenance of real physical processes.

Other researchers focused on simulating both SCADA and physical processes. For example, (Chabukswar et al., 2010) used the Command and Control WindTunnel simulation model environment to simulate DDOS attacks on a plant and its control system, while they have chosen OMNeT++ modules to simulate the network and MATLAB/Simulink to build and run the physical process model. Another solution that uses simulation is the Testbed for Analyzing Security of SCADA Control Systems (TASSCS) that has been developed to support the experimentation and evaluation of cyber-attack detection and recovery techniques for SCADA based control systems (Mallouhi et al., 2011). The testbed uses the OPNET tool to simulate computer networks and Power-World simulation to provide a simulated electric grid. The control part was simulated using Modbus RSsim software which provides the control functionalities of a PLC.

In their solution, (Farooqui et al., 2014) have developed a SCADA testbed using the TrueTime framework, which is a MATLAB/Simulink based tool, to simulate the process of a typical Turbo-Gas Power Plant. The platform developed was used to study the effects of ICT attacks against SCADA systems through several case studies. Recently (Singh et al., 2015) have proposed a testbed in which the physical process consisting of a power system was simulated with the PSAT (Power System Analysis Toolbox) software package for MATLAB. The authors have chosen also to simulate the SCADA system and its component. The developed testbed was used to study the impact of different attack scenarios and to test new security solutions for power grid systems.

In other approaches, researchers have developed testbed solutions that use both simulation tools and real components. An example of these testbeds is the testbed proposed by (Chunlei et al., 2010) that uses real components for a networked Industrial Control System. In this approach, the only simulated component is the enterprise network; all the other components (servers, PLCs, etc.) are real. Because almost every component is real, such a testbed can provide reliable experimental data, but it cannot support tests on large infrastructures such as chemical plants and gas pipelines. In another work, the SCADASim testbed has been developed by (Queiroz et al., 2011) at Royal Melbourne Institute of Technology (RMIT) University to provide an evaluation of network performance under cyber- attack. The SCADASim uses a simulation model to recreate the physical process and focuses on developing an emulated communication infrastructure that can be used to interconnect physical devices using common SCADA protocols. Another testbed solution was presented by (Siaterlis, et al., 2013) who implemented an emulation-based testbed termed EPIC. The testbed is able to recreate the cyber-part of interconnected critical infrastructures on real devices and makes use of multiple software simulators to represent physical components. The testbed demonstrated effective results under cyber-security experimentation.

In another work, (Hahn et al., 2013) introduced a cyber-physical testbed for a power system that they called the PowerCyber testbed. The testbed utilizes real, emulated, and simulated components to provide a realistic cyber and physical environment. The physical part of the testbed deploys two different tools for performing power system simulation, the DIgSILENT PowerFactory software and a real-time digital simulator, while the cyber part uses simulation and real components. The testbed was used to discover the impact of different attacks on the physical (the power system) and the cyber (communication) parts of the system. Later, (Candell et al., 2014) proposed a new testbed to measure the performance of an ICS with cyber-security protections. Multiples physical processors can be integrated in the platform. In this work, the authors have used simulation models to simulate the physical processes and real components to create the cyber layer.

In a recent work, a testbed for power generation system was proposed by (Korkmaz et al., 2016). The physical process for a power station was emulated using real hardware. They proposed to collect data from system to be used in the analysis of different type of attacks that could impact the system. Finally, (Lee et al., 2017) designed a cybersecurity testbed for a simulated power control system. The testbed was used to evaluate their proposed solution for an IDS that could be used to secure industrial IoT systems. However,

they did not provide an explanation on how IoT technologies will be integrated in their testbed.

3. Statement of the problem

The classification of physical process implementations of the previous solution shows that most testbeds are designed to study one specific industrial infrastructure. The restriction to one physical process poses a problem when researchers need to verify and validate the applicability of their solutions to multiple sectors of ICS. An architecture that enables the use of different physical processes is more interesting when demonstrating the effectiveness and the stability of a security solution.

A further inspection shows that the approaches found in the literature for the development of testbeds vary considerably in the use of simulators and real components. Simulation-based testbeds offer a low-cost environment to model industrial control systems. In addition, simulation provides abstraction interfaces that hide the complexity found in the deployment and configuration of real hardware. Also, the simulators allow scientists to isolate different factors to focus on specific parameters when conducting their experiments. Moreover, simulation enables the collection of all exploitable data and results that can be used for analysis and education purposes. However, they lack the ability to completely model the interactions of control system components. For example, a study conducted by (Chertov et al., 2008), revealed key differences between the use of simulators and real components in cyber security experiments. The study showed that simulators abstract a number of systems attributes and do not model key components such as drivers, CPUs and buses. The same study showed that TCP-based DoS attacks are effective only when real routers and PCs are used, and seems ineffective when simulators are used. On the other hand, real components are used to ensure high fidelity and increase the realism of the simulated process. Testbeds that integrate real components provide ideal environments to perform and evaluate industrial systems with high degree of accuracy. Using real component increase the realism of the simulated industrial process and provide access to the hardware features that are not available in software-only simulations. The problem with the previous solutions is that they restraint their users with their specific choices of components. In fact, they does not offer them the choice to select the method that is most suitable for their experiment needs. Therefore, the flexibility to choose between simulation and real components should be considered as an important factor in the development of testbed solutions.

Finally, a major concern with the previous approaches is that they were developed as isolated systems that do not have contact points with the external world. In fact, today, legacy ICS that were previously operated as standalone have been changed to the open architecture with the introduction of new ICT technologies such as IoT. For example, (Lojka et al., 2014) proposed a new architecture for an ICS where the SCADA will be hosted in the cloud and uses IoT protocols to monitor and control the physical process through the Internet. This shift from strictly isolated to highly interconnected systems has led to several enhancements in term of improved efficiency and cost reduction, however, it brought new vulnerabilities and cyber threats. On the other hand, the convergence between Operation Technologies (OT) and Information Technologies (IT) is considered also as a major problem. In fact, OT technologies have been intentionally separated from IT. This separation originally generated from the different technologies involved in each domain. OT systems were never designed for remote accessibility and, as a result, the introduction of new IoT protocols with the old OT protocols pose is a challenging problem. Therefore, previous solutions are not suitable for the assessment of new ICS architecture. Therefore, we need a new architecture for testbeds that incorporates IoT and legacy ICS.

To overcome these problems, we have proposed a novel architecture that provide an ideal environment where the security of new Industrial and IoT-based Control Systems could be tested and evaluated.

4. Proposed solution

We developed our solution based on the advantages of the previously mentioned methods. For the physical part, instead of using real components, we have used simulation. This provides an efficient, safe and low-cost approach with fast and accurate analysis capabilities. For the cyber part, the components can be flexibly configured with simulation or real hardware depending on needs. The testbed includes also an IoT gateway that enables the communication with the ICS components from the outside. Our approach should be able to overcome all the major difficulties that raised with previous solutions.

4.1. Architecture and components

SCADA systems collect information from industrial filed devices for real-time monitoring and control and have been used widely in the industrial sector and critical infrastructure. Therefore, we have implemented a SCADA system in our testbed to perform the monitoring and control actions. A typical architecture of a SCADA is shown in Figure 1.

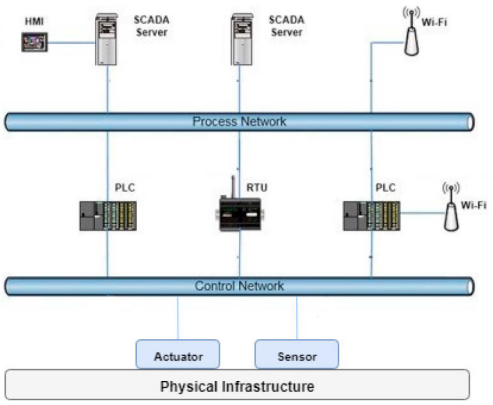

Figure 1. A simplified architecture for SCADA system

The US National Institute of Standard and Technology (NIST) has recommended that a SCADA testbed for security assessment should consider four general areas (Stouffer et al., 2011): the control center, the communication architecture, the field devices and the physical process itself. Modeling and implementing SCADA as a system of different areas has its own benefits. First of all, by implementing each area separately, we can reduce the dependency between each area. As a result, this will give us the flexibility to configure the components of our testbed to use simulation or real hardware regardless of the material or the configuration used in other areas. In the second place, modeling SCADA as architecture is important when we are identifying the source the threats and cyber-attacks based on each area. This section describes how components in our testbed are implemented in every area.

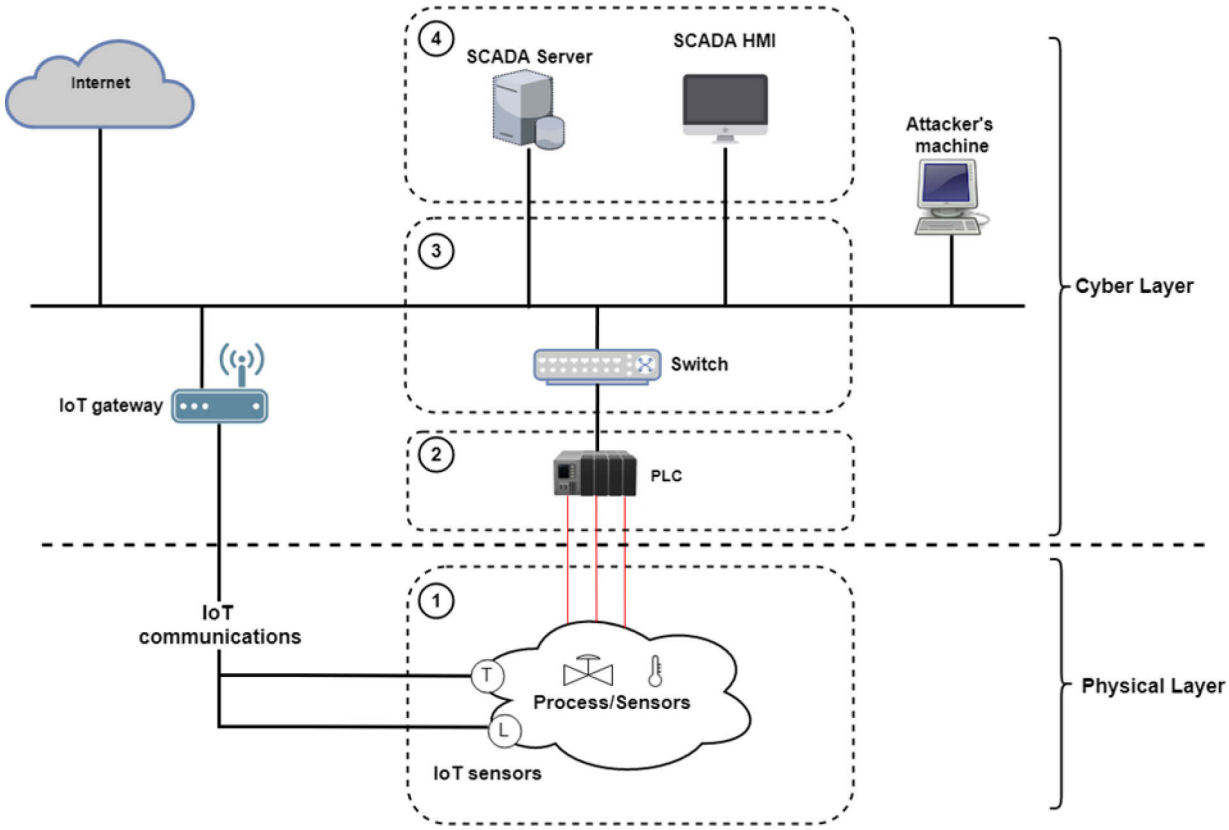

Figure 2. General architecture of the GSCOP-Testbed

4.1.1. The Physical Process

The physical process concerns the physical reality that an ICS observes and controls. For the physical layer, GSCOP-testbed uses simulation with a virtual mockup. As we saw before, most of the developed solutions use simulation for the physical part. This is due to multiple reasons. First of all, the simulation offers significant cost saving. Secondly, simulation models are easy to deploy and provide an accurate representation of the system behaviour. Finally, the simulation approach guarantee the security and the safety in the operational conditions where experiments for cybersecurity that aim to disrupt the functionality of a system can be performed safely (especially for critical infrastructures). Therefore, we have chosen the simulation approach for the physical process in our testbed. Also, this will make our testbed more flexible to use multiple physical processes by just switching between different simulation models. On the other hand, we could use real components for the physical part to increase the fidelity of our experiments if it is needed. An example where it is interesting to use real hardware would be with IoT sensors, as these components are cheap, easy to deploy and used widely today in different industrial sectors such as in smart traffic lights systems for example.

The virtual mockup in our testbed provides the capability to perform real-time industrial system simulation and allows physical layer integration with the cyber layer. The virtual mockup is built with a Raspberry Pi and an Arduino Uno device. The Raspberry Pi performs all the calculations and represents the core of the physical process, the sensors and the actuators. Simulation models will be implemented in the Raspberry Pi.

The testbed consists of two distinct environments: the physical environment and the cyber environment. In order to integrate these environments, the Arduino device is used to translate the information between the simulated physical world and the cyber world. It is in charge of the communications between the controller (Field Devices) and the process using analog communications.
GSCOP-testbed provides the ability to use different physical processes. Normally, a simulation model takes several variables as inputs and outputs several variables or states related to the simulated process. So, we can change the simulated physical process on our platform just by configuring the simulation program to send and receive the right inputs and outputs to/from the Arduino device.

4.1.2. The Field Devices

The Field Devices layer concerns the components that link the physical world to the digital. A programmable logic controller (PLC) is often used in this layer to perform the control of the process. The PLC receives data from the physical layer, elaborates a local actuation strategy, and sends commands to the actuators. It often uses a predefined program or a regulator (PID) to calculate the appropriate outputs or new states. The PLC also sends data received from the physical layer to the SCADA system and executes the commands that it receives. Our testbed includes a real hardware PLC. However, we can use a simulated one as well. The component selected is the Schneider Modicon M221C PLC, which has 16 Input/output ports and it is compatible with the communication protocol Modbus TCP/IP.

4.1.3. The Communication Architecture

The Communication Architecture involves components that realize communication between the different devices of the ICS. It includes both the network architecture and network protocols.

In the past, SCADA systems run on the dedicated networks with proprietary protocols and use vendor-specific hardware and software, which are isolated from the public network (Chunlei et al., 2010). However, with the advances in the Information and Communication Technologies (ICS), open protocols are widely used in SCADA systems in recent years to improve the efficiency and facilitate the exchange of information. This has exposed ICS to new kinds of security threats mainly due to the large number of new vulnerabilities and architectural weaknesses introduced by the extensive use of ICT and networking technologies into such complex systems (Fovino et al., 2010).

In fact, the networking protocols used for industrial systems (such as Modbus, DNP3, IEC 60870-5-101 and IEC 60870-5-104 …) use simple plain-text messages to exchange messages between the different components of the system and present a large number of vulnerabilities and weaknesses (Nazir *et al.,* 2016). These lack security and encryption, as these were designed for isolated systems. Therefore the security of communication protocols for SCADA systems has gained much attention in the previously mentioned testbeds.

In our solution, the GSCOP-testbed deploys a realistic wired Ethernet network to connect the different components of the ICS. Deploying a real network in our platform results in network flaws (packet loss, delay…) that are important to ensure the fidelity of the system. However, if needed, we can use a simulation tool as well. The SCADA controller and the PLC exchange data via MODBUS/TCP protocol. The local network is also used to make our testbed more flexible to connect new devices. For example, we have connected a PC to our testbed in order to launch attacks on the system from the internal network.

4.1.4. The Control Center

The control centre concerns the servers and operator stations that are used to remotely observe and control field devices. The functions of control in our testbed are supported with a SCADA system that is used to monitor and control the simulated processes. The SCADA control system is simulated using the software myScada. It has tools for supervising and managing the physical processes with multiple levels of action. It mainly displays information about the ongoing process, and sends commands to the PLC.

4.2. The IoT Gateway

Due to the tremendous number of different communications standards and technologies available for IoT, the implementation of IoT in the industrial sector has faced many challenges. Therefore, the Industrial Internet Consortium (IIC) proposed the Industrial Internet of Things Reference Architecture (IIRA). The IIRA provides guidance for the development of interoperable IIoT systems, solution and application architectures. It provides a standard-based framework and common terminology that identifies and highlights important architectural concerns, concepts and patterns that can be applied for IIoT.

The IIRA introduces the gateway-mediated edge connectivity and management architecture pattern. This pattern provides local connectivity solution for the edge of an IIoT system, with a gateway that bridges the local network of an industrial system to an external network as shown in Figure. 3. The gateway is used to mediate communication between the factory LAN with the outside network. It allows for protocol bridging between this two different network that normally has different architecture and could use different communication protocols.

In order to meet the requirements of increased connectivity in the new generation of ICS, and to provide an effective way to integrate IoT with the legacy ICS systems, we have applied the edge connectivity pattern to our testbed. Therefore, we extended our ICS system by connecting it to an IoT gateway. The IoT gateway bridges the gap between industrial legacy systems and new IoT technologies. It plays a key role in the convergence of IT and OT technologies. Thus, the physical process can be monitored and controlled from outside through the gateway using IoT protocols.
The IoT gateway is implemented using the Kura framework on a Raspberry Pi device. Eclipse Kura is an Eclipse IoT project that provides a platform for building IoT gateways. It

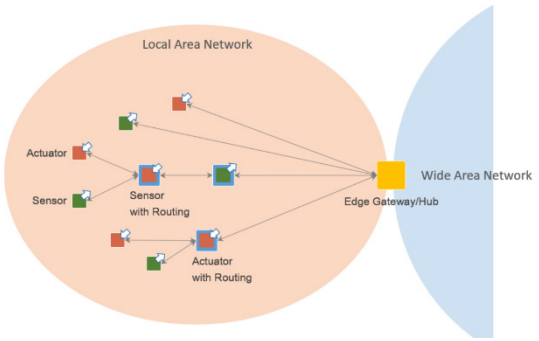

Figure 3. Gateway-Mediated Edge Connectivity and Management Pattern

is a smart application container that enables remote management of such gateways and provides a wide range of services and Application programming Interfaces (APIs) to write and deploy IoT application. Kura framework in our solution comes from that it supports a variaty of field protocols such as modbus, OPC-UA, S7 and other options to communicate with field devices. It supports also the request/response and publish/subscribe architectures for the IoT communication.

In order to connect the gateway to our testbed, we have been able to communicate with the PLC using the Modbus protocol. The Kura framework maintains a table that contains the addresses of each register in the PLC and provides an API to read and write from the registers. In addition, the user can easily choose the field protocol by just installing its appropriate driver. On the other side, we choose the MQTT protocol for communication with the Internet and the IoT-based sensors and actuators in our testbed. The MQTT protocol is a lightweight messaging protocol based on the IoT world, especially remote monitoring and communication with small sensors in high-latency or unreliable networks. The Kura framework provides a library for an MQTT client to send and receive data and a broker to store MQTT packets.

The IoT gateway translates the MQTT messages that it receives to Modbus messages and sends them to the PLC. It does the same thing on the other side, it translates the Modbus messages into MQTT messages and sends them to the broker. IoT protocol, which is the main objective of our proposed solution.

5. Case studies

In this section, we start by briefly presenting how our platform can support the use of different types of industrial processes. The physical processes simulated and implemented in our platform involve a printed circuit board assembly line (discrete process) and a chemical reactor (continuous process). Also, we show through two other

case studies how our testbed can be used to provide valuable insights into the disruptive effect of cyber attacks on the chemical reactor process. We show that the proposed framework can be applied also to explore new threats that come with the increased connectivity in ICS. In the first case study, we explore the effect of Distributed Denial of Service attack (DDoS) on the chemical reactor, while in the second case study we launch a cyber-attack targeting the IoT sensors in the chemical reactor.

5.1. Physical processes

As the platform simulates industrial processes. Those processes can be divided into two groups, the continuous ones and the discrete ones, each one having its own way of being handled. Continuous processes are characterized by having continuous variables that change over time. However, even their predictability is high, they generally need a permanent control in order to make the process works as is supposed to. Those processes are generally handled with a Process control loop. On the other hand, discrete manufacturing is often characterized by individual or separate unit production. The processes deployed in discrete manufacturing are not continuous in nature. Each process can be individually started or stopped and can be run at varying production rates. The products are typically manufactured following a cycle of steps in individually defined lots. In this section, we demonstrate through two case studies how our platform can support the use of discrete and contenuous industrial processes.

5.1.1. Discrete process: boards assembly line

production or not. Figure 5 shows the different steps in the PCB assembly line.

The typical model for computers communicating on a network is request/response. In the request-response model, a client computer or software requests data or services, and a server computer or software responds to the request by providing the data or service. However, this type of communication is not suitable for this case as the communication between the inspection machines and the software is an event-based communication: when a defect is detected the results should be sent instantly to the software that can be installed locally inside the factory or hosted over the internet. A different way for devices to communicate on a network is with the publish/subscribe architecture. In the publish/subscribe systems, publishers post messages to an intermediary message broker, and subscribers register subscriptions with that broker. The broker normally performs a store and forward function to route messages from publishers to subscribers. This communication pattern is gaining much attention in the industrial sector for asynchronous communication and sensor-based control systems.

In order to demonstrate how our testbed can support discrete processes controlled with IoT, we have simulated the assembly line and implemented it in our testbed. We have used MQTT as the communication protocol. The Kura IoT-gateway in our platform provides an MQTT broker to store and forward MQTT packets. The simulation of the PCB assembly line was done using JavaScript. The main objective of this architecture is to evaluate communications

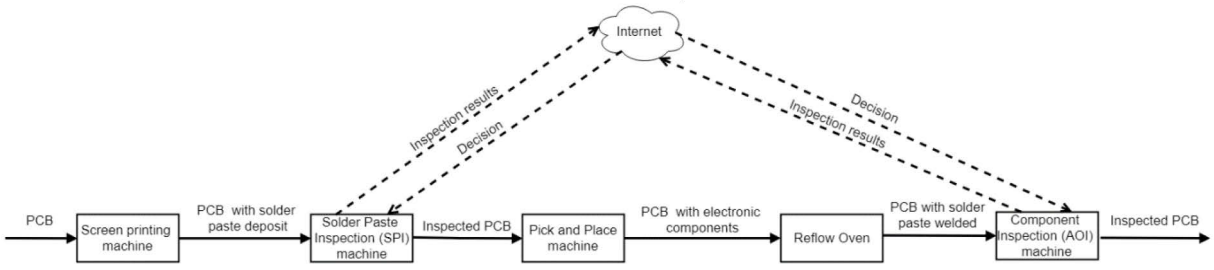

Figure 5. Printed circuit board assembly line

Surface-mount technology (SMT) is a method for producing electronic circuits in which the components are mounted or placed directly onto the surface of printed circuit boards (PCBs). The SMT process starts with the screen printing process which applies solder paste using a stencil and squeegees to the appropriate pads on the PCB. Then the PCB pass through the Solder Paste Inspection (SPI) machine to check the solder paste deposit. Once the printed PCB has been confirmed to have the correct amount of solder paste, it moves into the next step of the manufacturing process which is the component placement. In this step, each component is picked from its packaging using either a vacuum and placed in the programmed location on the PCB. Once all component have been placed on the PCB, it will move to the reflow oven machine where all the electrical solder connections are formed between the components and PCB by heating the assembly to a sufficient temperature. Finally, the PCB passes through the Automated Optical Inspection (AOI). In the two steps of the quality control on SPI and AOI machines, when a defect is detected, the inspection results are sent to a software that is responsible of analysing the results and taking the corresponding decision. According to the decision taken by the software the PCB can be sent to the next step of

between different components with the MQTT protocol. The simulation has showed that using a publish/subscribe architecture has resulted in enhanced response time, high performance and low latency.

5.1.2. Continuous process: Chemical reactor

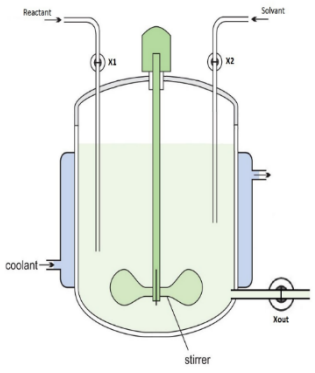

Figure 4. Simulated chemical reactor

A chemical reactor (Figure 4) is simulated using a script of python with a set of mathematical expressions. The process simulates a chemical reaction, which rises the temperature inside the reactor and needs then to be cooled to maintain the reaction in a controlled state. The process takes as input the states of the valves (X1, X2, Xout) and the rate of the cooling liquid (Qc):

- X1 (reactant)
- X2 (solvent)
- Xout (Exit)
- Qc (cooling liquid)

Then gives as Output:

- T: the temperature inside the reactor
- V: The volume of liquid inside the reactor

The process is regulated through a PID, which takes as input the current Temperature, and a setpoint. The regulator's goal is to change a variable (here Qc) in order to make the temperature stabilized at the setpoint (generally slightly oscillating around the setpoint).

5.2. Attack scenarios

5.2.1. Distributed Denial of Service attacks

The aim of this study is to evaluate if an Intrusion Detection (IDS) solution deployed on our testbed could be effective to detect DoS and DDoS attacks. A DoS attack is a cyber-attack in which the attacker seeks to make a machine or network resource unavailable. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. The Modbus protocol is particularly susceptible to this type of attack because the messages in the Modbus protocol do not include any authentication mechanisms that will allow the detection and rejection of injected false packets.

In order to conduct a successful DoS attack on the PLC to disrupt its communication with the SCADA system, the attacker simply sends a large volume of packets to the target by increasing the payload size of the Modbus message with unnecessary data to consume resources on PLC. In another way, the attacker can launch a DDoS attack by flooding the targeted machine or resource with superfluous requests from many different sources in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

As our platform provides an effective way to develop and evaluate security solution. We implemented a solution based on the Snort IDS to test its effectiveness against DoS and DDoS attacks. Snort is an open source signature-based network IDS. It was installed and configured on a PC and connected to the switch in the testbed. Then using the port mirroring property on the switch, we can duplicate all traffic passing it and send it to the IDS.

In order to enable Snort to detect DoS attacks, we used two specific rules. The first rule works on the length of the payload when the other works on the rate of packets exchanged over the network. These properties can give sign on DoS attacks as DoS attack is generally accompanied by a change in the statistical properties of these parameters. Hence, to detect such change in these parameters we defined a threshold value for each one of them. We supposed that we can detect abnormal traffic if the value measured for the observed parameter exceeds the threshold value. For example, the IDS will raise an alarm if it finds that a device is sending packets at a rate greater than the threshold defined or if the size of a packet passes the value of the size's threshold. Figure 6 shows the implemented rules.

In the next step, we tried to define the threshold for each parameter mentioned above. To do this, we captured normal traffic from the SCADA system to the PLC on the port 502. We observed that the maximal size between the captured packets was 60 bytes and the value for the maximal rate of transferred packets in one second was 25 packets per second. Therefore, we defined our thresholds based on these values. These values are specific to the scenario, and will need to be changed to suit the other environments.
To test and evaluate our solution, we studied two scenarios. In the first scenario, we assume that the attacker has access to the internal network of the testbed. Also, we supposed that the ICS is isolated and not connected to the Internet. In the second scenario, the attacker has not a direct access to the internal network, but he could communicate with the system from outside through the gateway. He can send requests to read variables from the PLC in order to monitor the temperature of the chemical reactor from outside. In the two scenarios, we used the Low Orbit Ion Cannon (LOIC) software to launch our attacks.

In the first scenario, the IDS was able to detect DoS attacks. In fact, we tried to send packets with large size of payload at first time, and in the second one we have sent a large volume of licit packets to try if we can avoid detection. However, the IDS was able to detect the attacks and raised alarms in the two times.

In the second scenario, when the ICS is connected to the Internet, we started by simulating a group of user that sends read request using MQTT protocol to get the temperature in the reactor. We noticed that the IDS generated a lot of false positive alarms. This could be easily explained as the IoT-gateway serves as the single entry point to the system and an aggregator for all received requests. As a result, the rate of packets sent from the gateway will exceed the defined threshold definitely. Defining another threshold in this case in a complex task, as we do not know how many users are communicating with the system from outside and when they decide to send their requests. Therefore, we decided to omit the rule related to the rate from the rules implemented in the IDS, then we proceed to the attack. However, this time, we launched a DDoS attack as we supposed that the attacker on the Internet could obtain the sufficient resources to launch such type of attacks. To detect if the attacker has succeeded, we measured the time of response of the PLC to a ping request before and after launching the attack. Figure 7 shows the results of our measures.

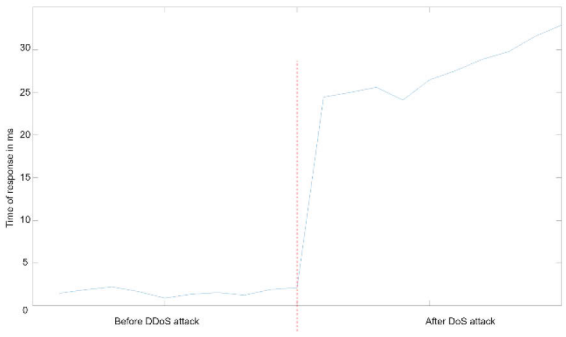

Figure 7. Ping Response Time from PLC before and after launching DDoS attack

In this experiment, we showed that the implemented security solution in a closed ICS was effective in detecting DoS attacks. However, when our ICS becomes connected to the Internet, we see that the solution is unable to detect DDoS attacks and raised several problems. Thus, the legacy ICS that is considered as secure when it is isolated becomes more vulnerable to cyber-attacks when it is connected to the Internet. This highlight the need of new security mechanisms to cope with the new threats in the new architecture of ICS.

5.2.2. Man in The Middle Attack

In this study case, we supposed that the system is fully controlled using IoT technologies. For this purpose, we modified the simulation model so that now the temperature sensor, the valves and the pumps support IoT communication. In addition, we developed an application that control the reactor form the Internet using MQTT protocol. The IoT sensor measures the temperature then publishes the measured value message on the broker. The broker then sends the published message to the application over the Internet. To constrol the system, the application sends the right commands to the valves and the pumps to maintain the reactor in a safe state. In addition, we simulated the functionalities of a Safety instrumented system (SIS) with our physical process. SISs are set of hardware and software used to ensure the safety of critical process systems. The simulated SIS in our platform monitors the state of the reactor. When the reactor is in critical state, the SIS is programmed to turn off the system to prevent the reactor from being exploded.

In this case study, we intend to show how an attacker can use a simple man-in-the-middle attack to capture and modify packets that are transmitted from the temperature sensor through a WiFi network. Due to the lack of resources (memory, energy, CPU performance), the traffic generated from the wireless node is not encrypted. This makes the task of attacker much easier as the data is sent in plain text. On the other hand, the attacker must not be necessarily connected directly to the testbed network to conduct his attack. He just needs to be in the range of the wifi network to perform his attack successfully.

Using the airbaise-ng tool the attacker was able to intercept the packets sent from the temperature sensor. Then using a technique known as ARP spoofing or ARP poisoning, he tricks the sensor to send the data to its machine instead of sending it to the broker. After he received the message from the sensor, the attacker uses the airbaise-ng tool to modify the message and send it back to the broker. This causes the temperature to rise to a critical level as the controller does not receive the real value of the temperature. In fact, the attacker has sent him a value of temperature much smaller than the real value, thus he was not able to execute the right commands to maintain the process in a safe state. This will cause the process state to reach a critical level after 11 minutes. In this case, the SIS intervened and shut down the reactor before it explodes. This case study shows the impact of a MiTM attack that caused the failure of the physical process. The attacker was able to take advantage of vulnerabilities presented in wireless sensors to launch his attack and cause the stop of the reactor. Figure 8 shows the impact of the attack on the reactor temperature.

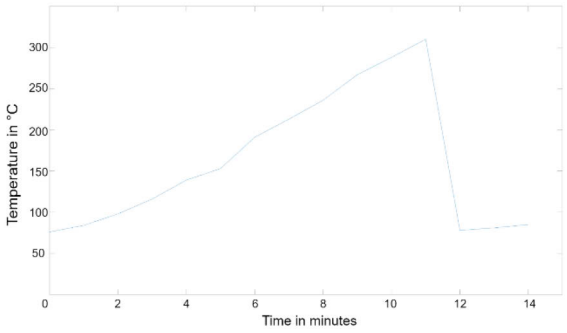

Figure 8. Impact of MiTM attack on the operation of the chemical process

6. Conclusion

The industrial sector is being impacted by the Internet of Things. The introduction of IoT technologies in the industrial systems has led to several enhancements in terms of more efficiency and cost reduction, however, this also brought new challenges. Therefore, it is important to study and exploit the potential effects of integrating such technologies in industrial infrastructures without compromising their reliability and availability. In this work, we presented the GSCOP-testbed, a novel infrastructure specifically designed for the security assessment of industrial control systems exposed to IoT environments. The components of our testbed could be configured with simulation and real hardware depending on experiment needs. We showed that the shift of legacy ICS systems from isolated to open systems has exposed them to new threats. We demonstrated through multiple case studies the applicability and the utility of our solution as an effective tool to discover the effects that could have cyber-attacks on our system and to evaluate and verify security solutions.

In the future, we intend to incorporate other communication protocols in our testbed. In addition, we would like to use the testbed for testing more sophisticated attacks and to propose solutions that can be used to ensure the security system against these attacks.

7. Acknowledgement

The authors gratefully thank the minister of industry in France for supporting this research under the project ‘Vision’.

8. Références

Abdo, H., Kaouk, M., Flaus, J. M., & Masse, F. (2018). A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. Computers & Security, 72, 175-195.

Candell, R., Stouffer, K., & Anand, D. (2014, October). A cybersecurity testbed for industrial control systems. In Process Control and Safety Symposium, International Society of Automation, Houston, TX.

Chabukswar, R., Sinopoli, B., Karsai, G., Giani, A., Neema, H., & Davis, A. (2010, April). Simulation of network attacks on SCADA systems. In First Workshop on Secure Control Systems.

Chertov, R., Fahmy, S., & Shroff, N. B. (2008). Fidelity of network simulation and emulation: A case study of tcp-targeted denial of service attacks. ACM Transactions on Modeling and Computer Simulation (TOMACS), 19(1), 4.

Chunlei W, Lan F, Yiqi D. A simulation environment for SCADA security analysis and assessment. In: Proc. of the 2010 International Conference on Measuring Technology and Mechatronics Automation. 2010, p. 342–7.

Farooqui, A. A., Zaidi, S. S. H., Memon, A. Y., & Qazi, S. (2014, October). Cyber security backdrop: A scada testbed. In Computing, Communications and IT Applications Conference (ComComAp), 2014 IEEE (pp. 98-103). IEEE.

Fovino, I. N., Masera, M., Guidi, L., & Carpi, G. (2010, May). An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants. In Human System Interactions (HSI), 2010 3rd Conference on (pp. 679-686). IEEE.

Hahn, A., Ashok, A., Sridhar, S., & Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. IEEE Transactions on Smart Grid, 4(2), 847-855.

Idaho National Laboratory, "National SCADA Test Bed: Fact Sheet", 2007.

Korkmaz, E., Dolgikh, A., Davis, M., & Skormin, V. (2016, June). Industrial control systems security testbed. In 11th Annual Symposium on Information Assurance.

Lee, S., Lee, S., Yoo, H., Kwon, S., & Shon, T. (2017). Design and implementation of cybersecurity testbed for industrial IoT systems. The Journal of Supercomputing, 1-15.

Liu, R., Vellaithurai, C., Biswas, S. S., Gamage, T. T., & Srivastava, A. K. (2015). Analyzing the cyber-physical impact of cyber events on the power grid. IEEE Transactions on Smart Grid, 6(5), 2444-2453.

Lojka, T., & Zolotová, I. (2014, September). Improvement of human-plant interactivity via industrial cloud-based supervisory control and data acquisition system. In IFIP International Conference on Advances in Production Management Systems (pp. 83-90). Springer, Berlin, Heidelberg.

Mallouhi, M., Al-Nashif, Y., Cox, D., Chadaga, T., & Hariri, S. (2011, January). A testbed for analyzing security of SCADA control systems (TASSCS). In Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES (pp. 1-7). IEEE.

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. Computers & Security, 70, 436-454.

Queiroz, C., Mahmood, A., & Tari, Z. (2011). SCADASim—A framework for building SCADA simulations. IEEE Transactions on Smart Grid, 2(4), 589-597.

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges. IEEE Access, 4, 1375-1384.

Siaterlis, C., Genge, B., & Hohenadel, M. (2013). EPIC: a testbed for scientifically rigorous cyber-physical security experimentation. IEEE Transactions on Emerging Topics in Computing, 1(2), 319-330.

Singh, P., Garg, S., Kumar, V., & Saquib, Z. (2015, August). A testbed for SCADA cyber security and intrusion detection. In Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on (pp. 1-6). IEEE.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST special publication.