OmniaScience

Journal of Industrial Engineering and Management
JIEM, 2018 – 11(2): 318-333 – Online ISSN: 2013-0953 – Print ISSN: 2013-8423
https://doi.org/10.3926/jiem.2534

Software Defined Networking Firewall for Industry 4.0 Manufacturing Systems

Akihiro Tsuchiya[1], Francisco Fraile[2], Ichiro Koshijima[1], Angel Órtiz[2], Raúl Poler[2]

[1]*Nagoya Institute of Technology, Graduate School of Engineering Systems Management (Japan)*

[2]*Universitat Politècnica de València (Spain)*

a.tsuchiya.054@nitech.jp, ffraile@upvnet.upv.es, koshijima.ichiro@nitech.ac.jp, aortiz@cigip.upv.es, rpoler@cigip.upv.es

Received: November 2017
Accepted: December 2017

Abstract:

Purpose: In order to leverage automation control data, Industry 4.0 manufacturing systems require industrial devices to be connected to the network. Potentially, this can increase the risk of cyberattacks, which can compromise connected industrial devices to acquire production data or gain control over the production process. Search engines such as Sentient Hyper-Optimized Data Access Network (SHODAN) can be perverted by attackers to acquire network information that can be later used for intrusion. To prevent this, cybersecurity standards propose network architectures divided into several networks segments based on system functionalities. In this architecture, Firewalls limit the exposure of industrial control devices in order to minimize security risks. This paper presents a novel Software Defined Networking (SDN) Firewall that automatically applies this standard architecture without compromising network flexibility.

Design/methodology/approach: The proposed SDN Firewall changes filtering rules in order to implement the different network segments according to application level access control policies. The Firewall applies two filtering techniques described in this paper: temporal filtering and spatial filtering, so that only applications in a white list can connect to industrial control devices. Network administrators need only to configure this application-oriented white lists to comply with security standards for ICS. This simplifies to a great extent network management tasks. Authors have developed a prototype implementation based on the OPC UA Standard and conducted security tests in order to test the viability of the proposal.

Findings: Network segmentation and segregation are effective counter-measures against network scanning attacks. The proposed SDN Firewall effectively configures a flat network into virtual LAN segments according to security standard guidelines.

Research limitations/implications: The prototype implementation still needs to implement several features to exploit the full potential of the proposal. Next steps for development are discussed in a separate section.

Practical implications: The proposed SDN Firewall has similar security features to commercially available application Firewalls, but SDN Firewalls offer additional security features. First, SDN technology provides improved performance, since SDN low-level processing functions are much more efficient. Second, with SDN, security functions are rooted in the network instead of being centralized in particular network elements. Finally, SDN provides a more flexible and dynamic, zero configuration framework for secure manufacturing systems by automating the rollout of security standard-based network architectures.

Social implications: SDN Firewalls can facilitate the deployment of secure Industry 4.0 manufacturing systems, since they provide ICS networks with many of the needed security capabilities without compromising flexibility.

Originality/value: The paper proposes a novel SDN Firewall specifically designed to secure ICS networks. A prototype implementation of the proposed SDN Firewall has been tested in laboratory conditions. The prototype implementation complements the security features of the OPC UA communication standard to provide a holistic security framework for ICS networks.

Keywords: cyber security, CPS, MES, SDN, OPC UA

1. Introduction

The concept of Cyber-Physical System (CPS) (Baheti, 2015) is rapidly reshaping the manufacturing sector. CPSs interconnects (cyber) computational assets with physical assets through devices with computational and communication capabilities. These devices turn physical objects into smart components conforming distributed and autonomous ecosystems that can sense and interact with the physical word, as well as with other software systems. Thus, CPSs are feedback systems that fuse the real world and the cyber world, providing new knowledge from connected devices. Because of the endless possibilities and expandability of CPSs, their applications have been explored in various research fields, including manufacturing (Lee, Bagheri & Kao, 2015). Indeed, the implementation of CPSs in manufacturing factories provides many advantages, from advanced fault detection for maintenance operations to work and waste reductions for lean manufacturing operations. For this reason, CPS is regarded as one of the core elements of the next generation paradigm for the manufacturing industry, Industry 4.0 (Kagermann, Wahlster & Helbig, 2013).

CPSs are a core element for industrial companies to implement vertical integration and networked manufacturing systems, where the different hierarchical levels (from the operational level to the corporate planning level) are able to share information in real time far beyond any traditional Manufacturing Execution Systems (MES). MES are intermediate systems between Industrial Control Systems (ICS) and enterprise applications (Kletti, 2006) and are crucial systems to materialize vertical integration.

However, enhancing IT system interconnectivity can expose process control devices like Program Logic Controllers (PLC) to cyber-attacks. Attackers may compromise devices to disturb production (Smith, 2015), but also, as highlighted in the report from the Repository of Industrial Security Incidents (RISI, 2017), to conform botnets and direct massive distributed attacks to other systems. Clearly, if a cyberattack shutdowns manufacturing operations, companies can lose large amounts of money, but most importantly, cyberattacks targeting systems that require safety operations represent a serious hazard to the safety of operators. Therefore, CPSs require thorough design and implementation of IT Security measures.

Moreover, towards the realization of secured vertical integration, IT network configuration rules need to be defined in a flexible manner, depending on the status of the manufacturing process (Kagermann et al., 2013), in order to minimize security threads. Software Defined Network (SDN) is likely a key technology in this regard (Nunes, Mendonca, Nguyen, Obraczka & Turletti, 2014), since it allows to control the network architecture programmatically, making it possible to modify network access on demand and minimize the exposure of ICS networks to attackers.

Software Defined Networking Firewalls have been introduced in the literature (Satasiya, 2016). In this paper, a protective network structure with a novel SDN Firewall specifically designed for industrial networks is proposed. The authors propose the concept of protective network structure for manufacturing systems and an access control mechanism implemented with a specialized SDN Firewall based on the Open Networking Foundation OpenFlow specification (2017).

Thus, the research is focused on protecting the network against attacks based on Network Scanning/Probing, since it is one of the major causes of security incidents in industry, according to research by the National Cybersecurity and Communications Integration Center (ICS-CERT, n.d.). SHODAN (Shodan, SHODAN Industrial Control Systems, 2017) or other network scanning tools can be used to conduct this kind of network scanning attacks (Bodenheim, Butts, Dunlap & Mullins, 2014). As a countermeasure, network segmentation with appropriate access rules can reduce the risk of unauthorized computer access. In this paper, in order to improve security in manufacturing systems, the following three objectives are established.

- Objective 1: Create segments without reconfiguring existing networks. Industrial devices are required to keep running constantly for safety operations. On the other hand, the ICS network should be separated with a defense-in-depth strategy -a common strategy that uses layers of firewalls to protect ICS- in order to check cyberattacks at an upper layer network. Therefore, DMZ is recommended to implement vertical integration without compromising security. However, changing the existing network may result in loss of availability of automation equipment. Authors propose a mechanism which enables networks to be changed into ideal networks without reconfiguration in order to implement a defense-in depth-strategy.
- Objective 2: Develop unidirectional access mechanisms. In order to protect industrial control systems, it is necessary to establish mechanisms that allow access to servers only when clients require the connection. This technique is known as unidirectional access mechanisms. Since lower networks, such as separate Control LANs, need to be interconnected, unidirectional communication is highly recommended (Agence Nationale de la Sécurité de Systems d'Information (ANSSI), 2014).
- Objective 3: Reduce loopholes in access rules. Machine-to-Machine (M2M) standards like OPC UA (Mahnke, Leitner & Damm 2009) enable communications with control devices and implement several security policies like authentication. However, security under transport layer is not covered by the OPC UA security specifications. Conversely, firewalls comprehend security for lower level communication layers. Therefore, firewall access rules and OPC UA security are complementary security measures for vertical integration of enterprise and industrial systems. However, the control of access rules between enterprise network and the industrial network is complex due to the different business functionality of each zone. For instance, devices are frequently introduced or exchanged in enterprise zone while they are more or less static in the manufacturing zone. This may lead to loopholes in firewall access rules.

In order to present the proposed solution, the rest of the paper is organized as follows: First, Section 2 includes a literature review of key existing systems and technologies for vertical integration in manufacturing systems. The literature review also covers the main cyberattack threats against industrial networks and the main countermeasures and technologies for cybersecurity. Section 3 presents the proposed network structure and the proposed SDN Firewall to mitigate security risks. Discussions are presented in Section 4, including the prototype implementation and the results of the security scanning tests. Finally, Section 5 includes some final remarks.

2. Literature Review

2.1. Industrial Control Systems and Networks

Industrial Control Systems (ICS) is a comprehensive term to describe the many applications and uses of facility control and automation systems in industry. ISA-99/IEC 62443 (International Electrotecnical Commission (IEC), 2009) is using the term Industrial Automation and Control Systems with following definition: "collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process".

Traditional ICSs architectures were closed systems. Industrial control systems started to incorporate networking at different levels to enable the connection between different manufacturing assets in order to improve the monitoring and control functions of the system. According to the National Institute of Standards and Technology (NIST, 2006), Industrial Network components can be classified into the following categories:

- Programmable Logic Controllers (PLCs): PLC are specialised devices that control industrial equipment and processes through digital and/or analogue input and output interfaces. PLCs have reliable, real-time runtimes to execute closed-loop control programs and are the core of every industrial control system.
- Supervisory Control and Data acquisition (SCADA): SCADA systems are software systems used to monitor and control geographically dispersed manufacturing assets.
- Distributed Control Systems (DCS): DCSs are integrated control architectures containing a supervisory level of control overseeing multiple, integrated subsystems that are responsible for controlling the details of localized processes. The main difference between SCAD2.4A and DCSs systems and that functionalities of DCSs are limited to display the current status of manufacturing assets, whereas SCADA systems implement event-driven control mechanisms.

Additionally, Human Machine Interfaces (HMI) are Graphical User Interfaces implementing human interactions with industrial network components.

Communications between these components occur at two different network levels (Sauter, 2010), the Local Area Network (LAN) and the Field Area Networks. Although there are several fieldbus technologies that can still be found in factories, both networks are rapidly migrating towards Ethernet-based networks, in some cases incorporating wireless access. Switched Ethernet networks lead to simpler physical network configurations and the technology is becoming very cost-efficient, due to the large economies of scale. End-to-end Ethernet networks favour system interoperability, since all corporate systems can be interconnected in the same physical network. In this context, communications between industrial network components are supported by IP industrial Machine to Machine (M2M) as described in the following section.

2.2. Industrial Machine to Machine (M2M) Protocols

Industrial Machine to Machine (M2M) communication protocols provide support for networking and data transfer in industrial control networks. The proliferation of Ethernet-based field buses and networks has fostered the appearance of different M2M protocols. Due to the strict timing requirements of industrial control applications, many manufacturers have developed communication protocols optimized for their industrial control equipment. This is the case of the Automation Device Specification (ADS) Protocol from Beckoff. Some of these proprietary protocols, originally developed by private companies, were later adopted by standard organizations and achieved larger market presence and vendor independence. This is the case of the CANOpen (Bosch), DeviceNet (Rockwell), or Profinet (Siemens) communication protocols. Similarly, the OLE for Process Control (OPC) was developed from Microsoft Windows Application Programming Interfaces (APIs) to allow the development of Microsoft applications interconnecting Industrial control components. The OPC protocol later evolved into the OPC Unified Architecture (OPC UA) protocol, providing support to the development of platform independent OPC UA based applications, enabling the development of industrial control applications in platforms like Linux or Android. OPC UA is becoming the de-facto standard for M2M communications in industrial environments. MTConnect is another protocol which, like OPC UA, has been designed to promote interoperability to exchange data between industrial network components. On the other hand, TCP Modbus is another open standard to exchange industrial control data which is widely used in industry.

As corporate applications migrate to cloud platforms or hybrid private-cloud platforms, industrial M2M need to provide support to Internet communications. This Internet capable M2M protocols are an important cornerstone of the Industry 4.0 and Industrial Internet of Things (IIoT) concepts. In this sense, the OPC UA protocol provides two different protocol stacks, a tcp-based protocol stack designed to work in private networks and an HTTPS protocol stack that can be used over the Internet. The Message Queue Telemetry Transport (MQTT) is a publish-subscribe messaging protocol that is optimized to reduce communications overhead and consume as little bandwidth as possible. MQTT is widely used in both IoT and IIoT applications. The Constrained Application Protocol (CoAP) and the Lightweight Machine to Machine (LWM2M) protocols are alternatives to MQTT also backed by strong standardization bodies. Finally, the WebThings protocol is a M2M protocol specifically designed to bridge the gap between devices and web applications, by using web compatible technologies like websockets.

Finally, Table 1 summarizes the different protocols presented in this section.

M2M Protocol	Private Network Applications	IIOT Applications
ADS	Yes	No
CANOpen	Yes	No
DeviceNet	Yes	No
Profinet	Yes	No
OPC	Yes	No
Modbus	Yes	No
OPC UA	Yes	Yes
MTConnect	Yes	No
MQTT	Yes	Yes
CoAP	Yes	Yes
LWM2M	Yes	Yes
WebThings	Yes	Yes

Table 1. Industrial M2M machine protocols

M2M Protocols play an important role in vertical integration, since they enable interoperability between industrial network components and other systems in the corporate level. Manufacturing Execution Systems (MES) play an important role in this integration and for this reason they are described in the following section.

2.3. Manufacturing Execution Systems (MES)

Manufacturing Execution System (MES) are intermediate systems between ICSs and corporate applications like the Enterprise Resource Planning (ERP). A detailed description of MES functions can be found in the ISA 95 standard (American National Standard, 2005), which is based on a three-level structure: Corporate Management, Manufacturing Operation System (MOS) MES/MOM and Process Control level. ISA 95 part 3 (American National Standard, 2005) defines the interfaces to interact with the process control level to integrate corporate management systems and process control systems in the following activities: process execution, definition management, data collection, dispatching, analysis, resource management, detailed scheduling and tracking.

Through this integration, the MES model provides significant advantages in comparison with the classical manufacturing model. First, MES/MOM improves the transparency of the manufacturing data. Sensor data can be used to calculate production Key Performance Indicators (KPIs) in real time or to monitor the status of the machines and the quality of the manufacturing process. The integration with enterprise data gives sense to this information, relating it to specific products and assets, providing the ability to map the value stream of the company in real time. This information improves the responsiveness of the organization to detect problems and unplanned events, becoming able to correct errors and adapt to the demand more rapidly. This vertical integration fosters networking between the tactical level and the operational level, encouraging inter-company cooperation and enabling a faster and more effective exchange of information between levels. According to Kletti (2016), MES systems can be regarded as decision support systems developed from classic disciplines such as production data acquisition, operator work time logging, or quality assurance.

Moreover, the Manufacturing Execution Solution Association (MESA, n.d.) defines twelve function groups which are required for an effective decision support of production management: (1) detailed planning, (2) resource management (3) registration and display of the current status of resources, (4) document management, (5) material management, (6) performance analysis, (7) order management, (8) maintenance management, (9) process management, (10) quality management, (11) data collection and acquisition and (12) product tracking and genealogy. MESA has also established the terms Collaborative MES (C-MES) and Advanced Collaborative MES (ACMES) to refer to redesigned and modified functions for supply networks.

A more detailed definition of the functions of MES systems can be found in ISA 95 standard (American National Standard, 2005). ISA 95 is based on a three-level structure: corporate management, Manufacturing Operation System (MOS)/MES and process control level. ISA 95 part 3 (American National Standard, 2005) defines the interfaces between enterprise activities and control activities. In the document, a generic activity model of production operations management shows several activities which interact with the process control level: (1) execution, (2) definition management, (3) data collection, (4) dispatching, (5) analysis, (6) re-source management, (7) detailed scheduling and (8) tracking. Equipment and process specific production rules are applied to process control level with product definition management. The rules are downloaded to the equipment such as PLC in order to change process. Operational commands and responses are interacted with production execution. Operational commands are information to command production steps to personnel or equipment which belong to process control level. And, operational responses are obtained from them to managers who execute production execution for next decision. Equipment and process data which is in-formation about the equipment performing and the production functions is acquired from process control level for production data collection. As to a boundary between MES and corporate management level, the model is classified into four types depending on operation mode, which are maintenance, production, quality and inventory.

2.4. Security in ICS and Manufacturing Systems

2.4.1. The challenges of Network Probing Attacks

Attackers compromise devices to disturb production by exploiting different system vulnerabilities. According to ICS CERT (ICS), attackers commonly follow three steps to compromise devices running in industrial control networks. The first step is to gain access to the control system LAN. After that, attackers try to understand the communication mechanisms implemented in the system to perform specific attacks to the devices. Finally, they compromise a device. The main objectives of cyberattacks are to gain control over the process, to hack the Human Machine Interface (HMI), to change the database, or to perform other attacks with Man-in-the-Middle.

In order to intrude a control system LAN, Sentient Hyper-Optimized Data Access Network (SHODAN) (Shodan, 2017), which is a search engine for Internet connected devices, can be perverted by attackers. SHODAN provides users with IP addresses, Hostnames, domain information, positional information, service ports, Operating System (OS), banner (device-specific) information, and the date of registration. The banner is especially sensitive since it includes information such as default password, which can be used to compromise a device. (Bodenheim et al. 2014) shows the impact of SHODAN attacks in industrial networks. Figure 1 contains the flow chart of SHODAN device scans. As shown in the figure, SHODAN generates a random IP address and service port to carry out a Synchronize (SYN) scan. If the SYN/Acknowledge (ACK) flag is received from an opponent, the SYN scan is regarded as success. Then, SHODAN starts to grab opponent's information (banner). After that, SHODAN stores this information in the database and repeats this scan for all IP addresses in the provided range.

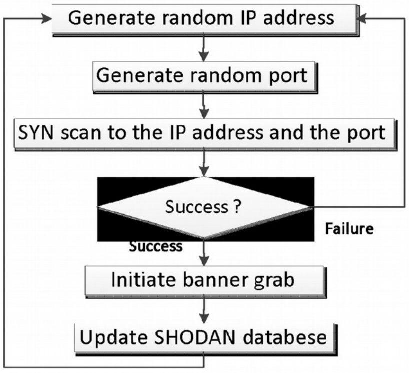


Figure 1. SHODAN scanning flow chart

This paper presents a security solution to mitigate the risk of network probing attacks. The proposed solution is encompassed in standard cybersecurity frameworks and architectures for industrial control networks which are described in the following sections.

2.4.2. Cybersecurity Framework in Manufacturing Systems

Cybersecurity models for manufacturing systems should regard different aspects beyond technical security requirements and functionalities. In this sense, The US Department of Homeland Security (DHS) (2016a) developed a specialized framework for critical industrial systems. The DHS framework presents a comprehensive set of functions that provide a strategic overview of the different activities in the cybersecurity lifecycle:

- Identify: Lay the foundation for effective use of the framework. Cybersecurity practices in the Identify Function include systems, assets, data, capabilities, and other foundational elements that are critical to the organization.
- Protect: Develop and identify appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect: Identify and implement the tools to identify the occurrence of a cybersecurity incident.
- Respond: Use the tools and activities to support the containment of a cybersecurity event.
- Recover: Bolster resilience and restore any capabilities or services impaired by the cybersecurity event.

The National Institute of Standards and Technology (NIST) guide to ICS Security (Stouffer et al. 2014) on the other hand groups activities in two main phases: risk management and assessment and ICS Security Program development and deployment. Furthermore, according to the Agence Nationale de la Sécurité de Systems d'Information (ANSSI), industrial control systems can be categorized into three types depending on the risks and impact of attacks (ANSSI 2014).

The ISA-99/IEC 62443 (IEC, 2009) Industrial Network and System Security standards, which are under development at the time of writing this report, builds upon these standards and proposes four different categories to group standardization activities:

- General: Definition of main concepts and models, security lifecycle and use cases and conformance metrics.
- Policies and procedures: Requirements and guidance for security management systems, patch management and requirements for solution providers.
- System: Technologies, system security requirements, security level and security risk assessment and security system design.
- Component: Product development and technical security requirement for industrial control network components

The Virtual Factory Operating System (vf-OS) project develops a security model which complies with these standards and that it is based on security architectures for industrial control networks which are further described in the next subsection.

2.4.3. Secure Architecture for Industrial Control Networks

In order to minimise the risk of cyberattacks against industrial control network components, the different standard organizations presented in the previous sections recommend network segmentation and segregation in order to minimize the access from one segment to other segments. This technique minimises the risk of exposing sensitive information of industrial network composes to network probing attacks. Indeed, from a security point of view, the ideal situation would be to keep the industrial control network completely isolated, but, as discussed in the introduction, this would limit system interconnectivity and limit the functionalities and scope of CPS and MES systems. In order to enable interconnectivity, standards propose the use of specialised network architectures for industrial control networks (Stouffer, Pillitteri, Lightman, Abrams & Hahn, 2014; ANSSI, 2014; IEC, 2009) based on the Defence in-Depth strategy (DHS, 2016b; Barnum, Gegick & Michael, 2005). With this strategy, security systems are not concentrated in a single network point, but scattered across the network, so that potential attackers meet several burdens before they can compromise the industrial control network. The main security system recommended in all standards to implement this security strategy is Firewalls, which control the network traffic in and out every network segment. The DHS secure ICS network architecture divides the network into two zones (and five subnetworks depending on business functions. The different subnetworks are interconnected through Firewalls which prevent untrusted traffic in every subnetwork and implement the access rules to enable interoperability between the different business functions within each zone. The ISA/IEC 62443 secure ICS network architecture, illustrated in Figure 2, uses the same approach and defines different levels for the industrial (ie manufacturing) zone, the operation, the control and the field level. This approach is adopted in state-of-the-art interoperability platforms such as vf-OS.

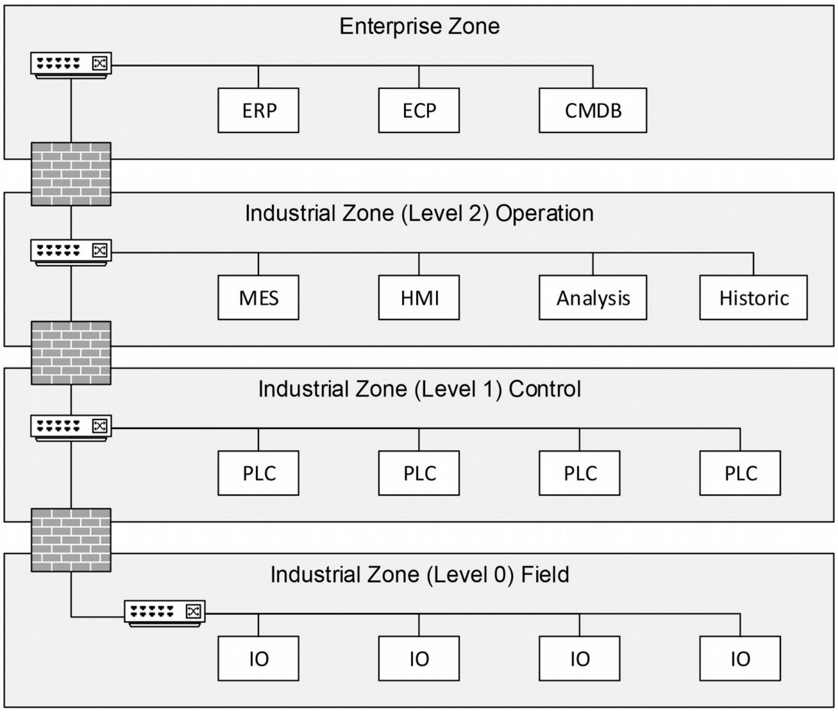

Enterprise Zone
ERP
ECP
CMDB
Industrial Zone (Level 2) Operation
MES
HMI
Analysis
Historic
Industrial Zone (Level 1) Control
PLC
PLC
PLC
PLC
Industrial Zone (Level 0) Field
IO
IO
IO
IO

Figure 2. Zone segmentation of Enterprise & ICS (ISA/IEC 62443)

Thus, an attacker pretending to intrude the control network, needs to generate traffic that meets the security filtering rules programmed into each Firewall in the different security levels. In this sense, (Byres, Karsch & Carter, 2005) categorizes a firewall into several types depending on the type of filtering rules that can be applied. Most advanced Firewalls implement in-depth packet inspection, allowing to deploy application layer filtering rules, so that only traffic matching specific application level rules can access the network. This makes it possible to integrate network security rules with application layer security mechanisms. Next section describes the application level security mechanisms provided by the OPC UA standard, since is the technology used in the prototype implementation of the proposed solution.

2.4.4. OPC UA Security

The OPC UA security specifications are described in (OPC Foundation, 2015; Amstrong & Hunkar, 2010). Figure 3 shows the OPC UA security architecture. The figure highlights how the security addresses three layers of the OSI Model (Boait, Neville, Norris, Pickman, Tolhurst & Walmsley, 1988) above the network layer: The application layer, the communication layer and the transport layer. At the Application layer, Authentication and Authorization are required to allow access only to trusted clients. OPC UA applications have Application Instance Certificates to implement certificate based application layer security. At the communication layer, data encryption provides confidentiality to prevent eavesdropping. Finally, other mechanisms achieve data integrity and transport layer security to prevent data loss.

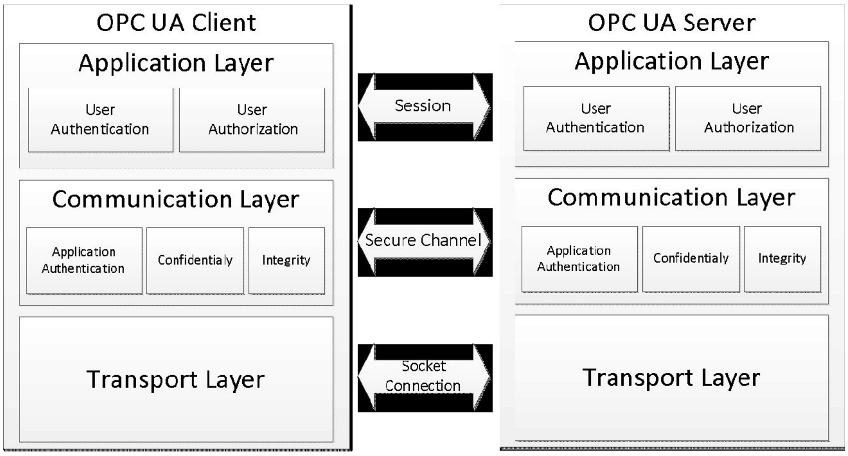


Figure 3. OPC UA security architecture (UA Part2)

3. Sample and Methods

3.1. MES Network with Transparent Firewall

Figure 4 shows the MES system network architecture with the transparent SDN Firewall proposed in this paper. The SDN Firewall has two main functions: First, to filter packets based on access rules and second, to act as a bridge between network interfaces. With packet filtering – based on application layer rules, IP rules or Medium Access Control (MAC) layer rules – industrial devices can be grouped into the appropriate network segment automatically. On the other hand, bridging allows to implement the firewall without changing the existing network configuration. It can be noted that the proposal is still compatible with the aforementioned standards and recommendations, except that security functions are not implemented at the boundaries of the different levels. Instead, each system boundary faces other system boundaries through a SDN Firewall, programming the security functions in the network, thus taking the defence in-depth strategy to a new level.

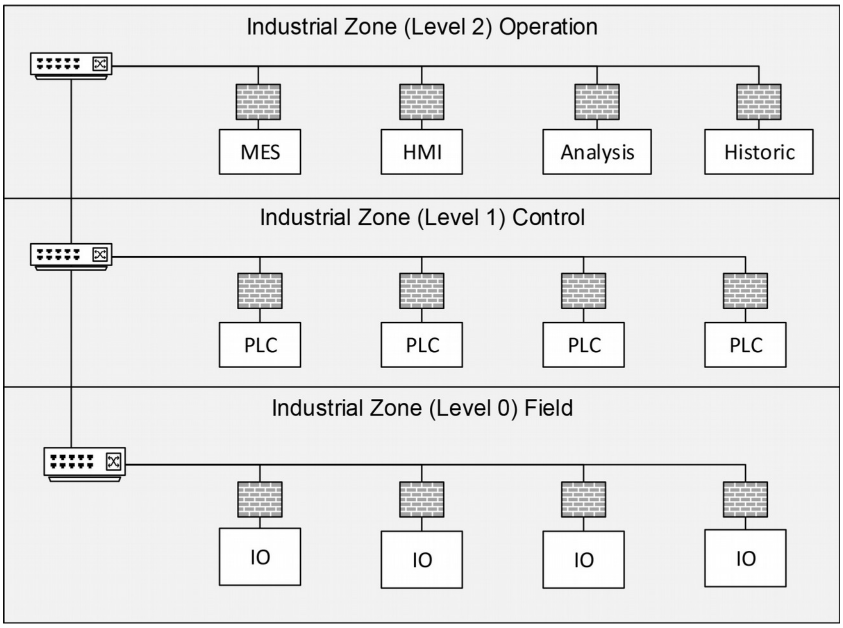

Industrial Zone (Level 2) Operation
MES
HMI
Analysis
Historic
Industrial Zone (Level 1) Control
PLC
PLC
PLC
PLC
Industrial Zone (Level 0) Field
IO
IO
IO
IO

Figure 4. Secure manufacturing system architecture with SDN Firewalls

Figure 4 shows the different functional levels of manufacturing systems and industrial control networks with the proposed SDN Firewall. The SDN Firewall limits access to PLCs or any other Safety Instrumented Systems (SIS) by applying the different rules and only allowing access to well-known services (eg MES systems or CPS components). The following sections describe two different filtering techniques that can be used to implement SDN Firewalls.

3.2. Temporal Filtering

The access rules in the proposed SDN Firewall are only enabled when a connection is required. This feature, known as temporal filtering, is implemented with OpenFlow. The SDN Firewall consists of two components, the actual Firewall operating in the data plane of every system boundary (hereafter Transparent Firewall) and the control plane (hereafter Firewall Controller) controlling the behaviour of the Transparent Firewall. This way, The Transparent Firewall enforces access rules, allowing clients to connect to servers when packets match all the rules that have been defined and dropping packets that do not match access rules. The firewall controller keeps the configuration of the manufacturing system network and enables/disables access rules in the Transparent Firewall accordingly.

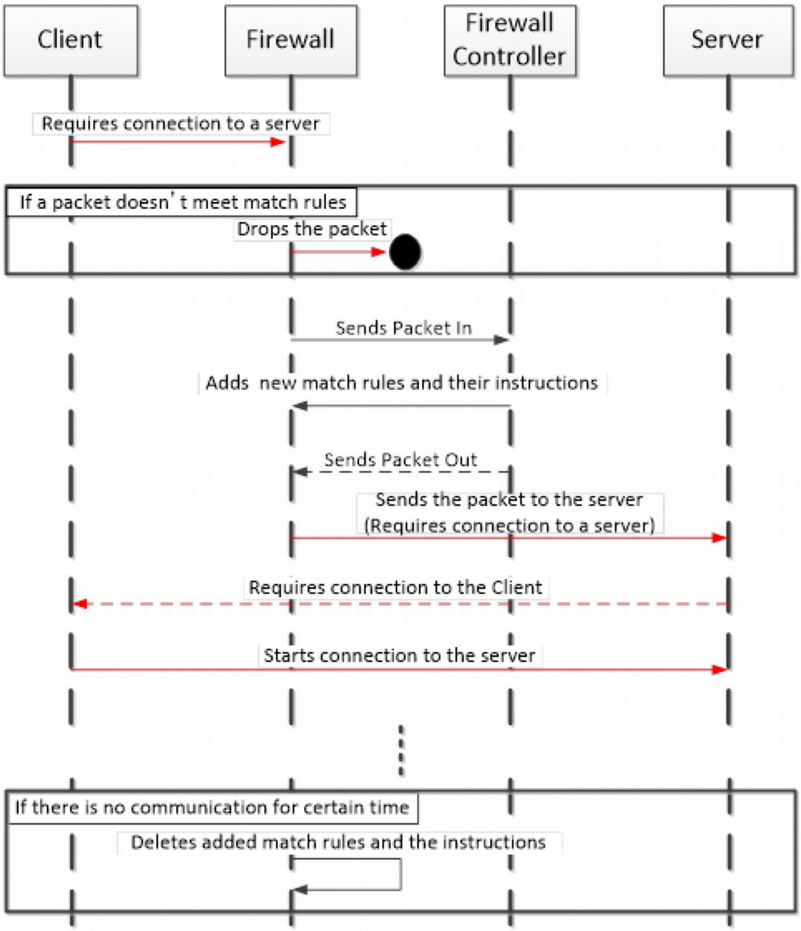

Client
Firewall
Firewall Controller
Server
Requires connection to a server
If a packet doesn't meet match rules
Drops the packet
Sends Packet In
Adds new match rules and their instructions
Sends Packet Out
Sends the packet to the server (Requires connection to a server)
Requires connection to the Client
Starts connection to the server
If there is no communication for certain time
Deletes added match rules and the instructions

Figure 5. Communication sequence of packet filtering

The communication sequence of temporal filtering is depicted in Figure 5. When a client requires connection to a server, the Transparent Firewall intercepts the packet and inspects the packet headers. The packet is dropped if it does not match the rules set by the Firewall Controller. Otherwise, the packet is kept on the Transparent Firewall and a message is sent the Firewall Controller in order to request instructions on how to deal with the packet. When the Firewall Controller receives the message, the Firewall controller checks the information against the overall security rules and adds new match rules if the packet is allowed to pass through the Transparent Firewall, Then, the Firewall Controller sends a Packet Out message with the corresponding instructions so that the Firewall forwards the withheld packet to the server. The red arrows depicted in Figure 5 represent the Three-way handshaking that establishes TCP/IP communications. If there is no communication for a certain time, the Firewall deletes the added match rules and the instructions. Therefore, the Firewall controller only allows connections to servers when specific clients in a whitelist try to establish a connection. The rest of the time, all communications are virtually closed.

3.3. Spatial Filtering

In addition to temporal filtering, the Transparent Firewall implements an Access Control system based on the OPC UA standard. Since the Transparent Firewall virtually separates networks based on access rules programed in the Firewall Controller, it is possible to automatically rewrite the access rules based on OPC UA application level authorization. This novel mechanism is referred to as spatial filtering. An illustrative structure of spatial filtering is depicted in Figure 6. The steps for setting access rules are described as follows:

1. The OPC UA Access Control Server (ACS) requests OPC UA Applications information about their trust list and network interfaces. The Firewall Controller must allow the ACS to pass through the Firewall in advance.
2. OPC UA applications send trust lists and network interfaces to the ACS.
3. The ACS generates the access control list with this information.
4. The Firewall Controller configuration is updated. The access control list must be downloaded with encrypted communication to protect the system information from external attackers.
5. The Firewall applies temporal filtering according to the access control list implemented in the Firewall Controller.

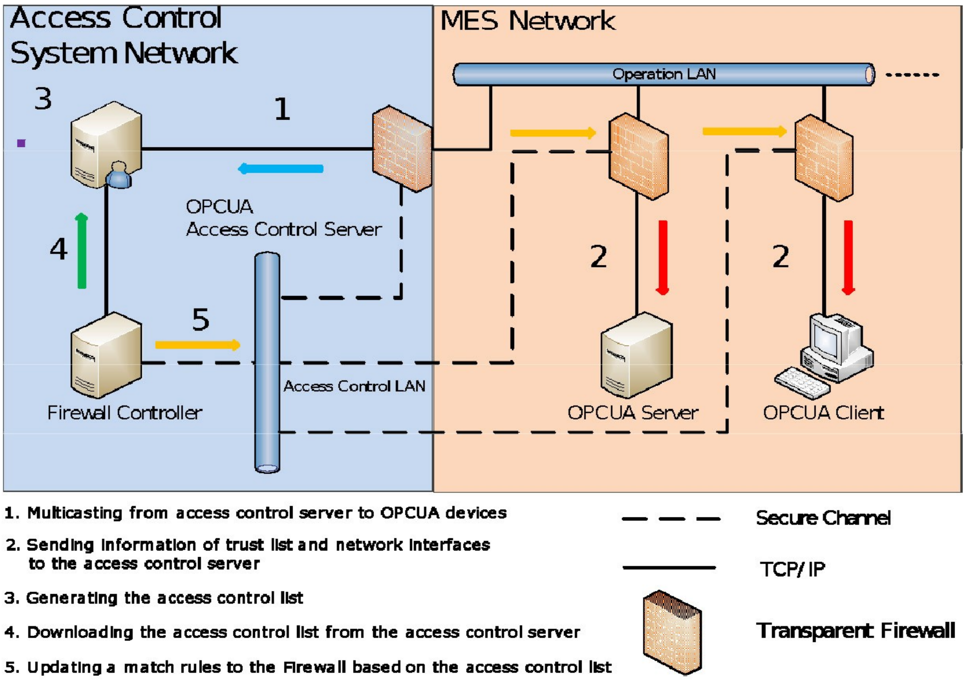

Access Control System Network
MES Network
Operation LAN
3
1
4
5
2
2
OPCUA Access Control Server
Access Control LAN
Firewall Controller
OPCUA Server
OPCUA Client
1. Multicasting from access control server to OPCUA devices
2. Sending information of trust list and network interfaces to the access control server
3. Generating the access control list
4. Downloading the access control list from the access control server
5. Updating a match rules to the Firewall based on the access control list
Secure Channel
TCP/IP
Transparent Firewall

Figure 6. Structure of spatial filtering mechanism

This way, the Transparent Firewall flexibly filters packets depending on trusted applications and enabled network interfaces in OPC UA applications.

4. Discussion

4.1. Prototype implementation

Authors have developed a prototype SDN Firewall implementation as described in this paper. A system structure of the prototype implementation is shown in Figure 7. An OPC UA server application (KEP Server EX, 2017) and tOPC UA client application (UaExpert, 2017) are installed on Windows based virtual machines (Guest machine1 and Guest machine 2) in order to test the solution. The Transparent Firewall has been implemented with OpenVSSwitch (Openvswitch, 2017) and the Firewall Controller with Trema (Trema, 2017) and run on virtual Linux machines (Guest machine 3). The Access Control Server is developed on a Linux virtual based (Guest machine 4). The virtual network consists of three LAN segments simulating the presented secure industrial control network architecture. The Firewall and the Firewall Controller internally communicate with Local Loopback. The Firewall Controller download a file containing the access rules from the Access Control Server. They use shared key to communicate each other by using the Secure Shell (SSH) connection. Firewall Controller downloads a set of match rules. In this version, the rules are based on service, IP and MAC level information. The Firewall Controller provides logs to describe information of the status of the Firewall and filtering results. Figure 8 shows the console interface of the Firewall Controller.

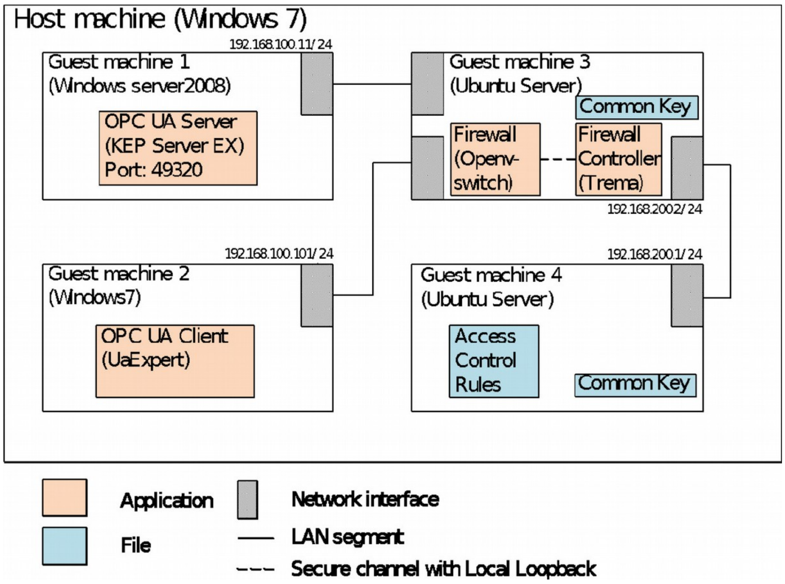
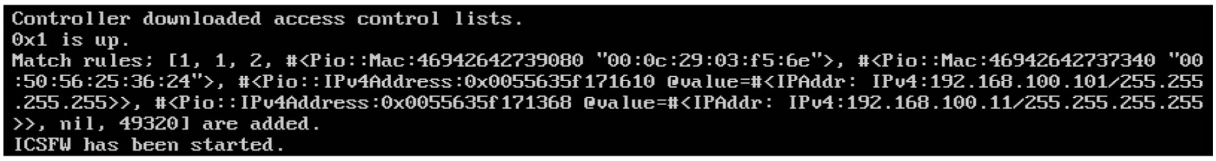


Figure 7. Prototype implementation structure



```
Controller downloaded access control lists.
0x1 is up.
Match rules; [1, 1, 2, #<Pio::Mac:46942642739080 "00:0c:29:03:f5:6e">, #<Pio::Mac:46942642737340 "00
:50:56:25:36:24">, #<Pio::IPv4Address:0x0055635f171610 @value=#<IPAddr: IPv4:192.168.100.101/255.255
.255.255>>, #<Pio::IPv4Address:0x0055635f171368 @value=#<IPAddr: IPv4:192.168.100.11/255.255.255.255
>>, nil, 49320] are added.
ICSFW has been started.
```

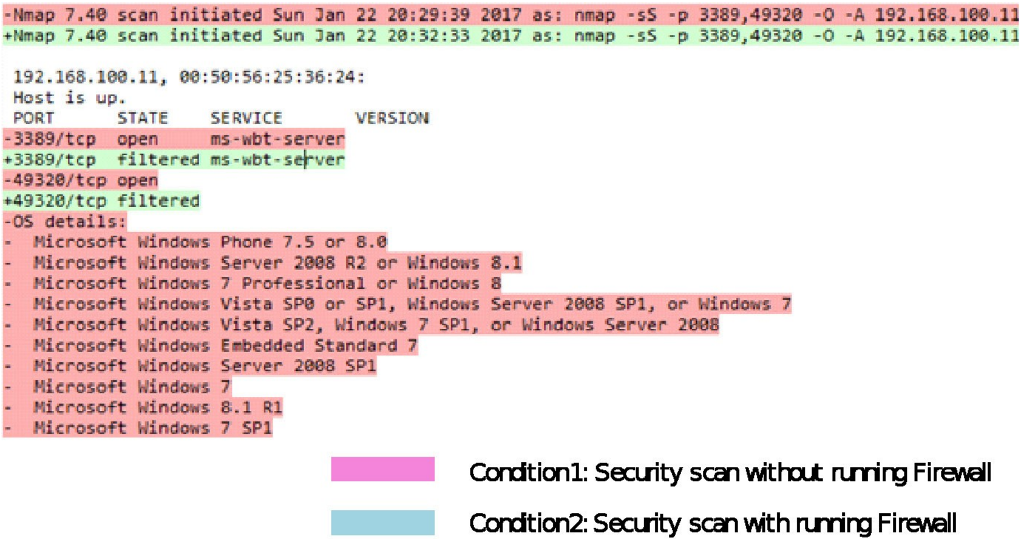
Figure 8. Firewall Controller's console

4.2. Security Test

Authors tested how the Firewall works against network scans. Two conditions were conducted on the prototype system. One is security scan with the SDN Firewall disabled, ie the Firewall runs as a legacy Ethernet switch. The second part of the test, the scan is performed with the SDN Firewall applying the filtering rules. The Nmap (2017) scanning tool was shown in the tests, scanning information of port status and OS from the Guest machine 2.

Then, service ports for Remote Desktop Protocol (RDP) (port number 3389) and the OPC UA Server application (port number 49320) are opened in the Guest machine 1.

The results are illustrated in Figure 9. When the firewall is disabled, the ports were opened and several expected OS versions are shown. On the other hand, when the SDN Firewall is enabled the application ports were closed and no details of OS were displayed. As a consequence, the SDN Firewall did not expose Guest machine 1 port status or OS details regardless of its access rules. Therefore, the Firewall can be regarded as a secure measure against network scanning.



```
-Nmap 7.40 scan initiated Sun Jan 22 20:29:39 2017 as: nmap -sS -p 3389,49320 -O -A 192.168.100.11
+Nmap 7.40 scan initiated Sun Jan 22 20:32:33 2017 as: nmap -sS -p 3389,49320 -O -A 192.168.100.11

 192.168.100.11, 00:50:56:25:36:24:
 Host is up.
 PORT      STATE    SERVICE       VERSION
-3389/tcp  open     ms-wbt-server
+3389/tcp  filtered ms-wbt-server
-49320/tcp open
+49320/tcp filtered
-OS details:
-  Microsoft Windows Phone 7.5 or 8.0
-  Microsoft Windows Server 2008 R2 or Windows 8.1
-  Microsoft Windows 7 Professional or Windows 8
-  Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
-  Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
-  Microsoft Windows Embedded Standard 7
-  Microsoft Windows Server 2008 SP1
-  Microsoft Windows 7
-  Microsoft Windows 8.1 R1
-  Microsoft Windows 7 SP1
```

🟪 Condition1: Security scan without running Firewall

🟦 Condition2: Security scan with running Firewall

Figure 9. Comparison of results

4.3. Next Steps

The prototype implementation is an early implementation that works as a Stateful Firewall. Currently, the configuration is performed manually. In the next steps, authors need to focus on two main tasks. The first task is to develop more automatic spatial filtering mechanisms. With this purpose, authors need to continue to develop the Access Control Server based on the OPC UA standard. Authors need also tackling the development of an algorithm for automatically generate access rules. The second task is to develop more sophisticated packet inspection mechanisms to secure even more OPC UA communications.

5. Conclusions

Cybersecurity is a critical aspect of MES systems and other CPS systems for Manufacturing. Most common attacks are based on Network Scanning/Probing. Defence-in-depth is an effective counter-measure against scanning attacks. This paper has presented a manufacturing system network architecture based on this security strategy. The network architecture implements a novel SDN Firewall that features temporal filtering (packets are only allowed from authorised clients when they need communications) and spatial filtering (access control list is integrated with OPC UA Application level authorization). This way, the ICS network is virtually closed for Network Scanning or Probing. Additionally, the SDN Firewall is able to separate a flat network into the proposed manufacturing system network architecture without loss of network availability.

An implementation prototype has been developed and tested in a virtual network. The prototype firewall has been tested together with OPC-UA client and OPC UA server applications exchanging machine data. Access from the OPC UA client to the OPC UA server is only allowed by temporal filtering firewall. Test results showed that the firewall could prevent security scanners from acquiring the application port and other Operating System level details of the OPC UA server. The prototype implementation implemented Transport layer filters, although authors plan to develop a more sophisticated SDN Firewall implementing deep packet inspection for OPC UA. This could potentially improve security and performance. Regarding spatial filtering, authors regarded using the standard OPC

Discovery Service, but this service lacked Discovery information for client applications, so further research needs to be conducted in order to automatically generate access lists.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

This research has been partially funded by the European Commission, under Grant Agreement 723710.

References

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) (2014). *Cybersecurity for Industrial Control Systems - Classification Method and Key Measures*. ANSSI

American National Standard (2005). *ANSI/ISA-95 Enterprise - Control System Integration Part 3: Activity Models of Manufacturing Operations Management*. ISA.

Armstrong, R., & Hunkar, P. (2010). *The OPC UA Security Model For Administrators.*

Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The impact of control technology,* (12), 161-166.

Barnum, S., Gegick, M., & Michael, C.C. (2005, September). *US CERT Defense in depth.*

Bodenheim, R., Butts, J., Dunlap, S., & Mullins, B. (2014). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection*, 7(2), 114-123. https://doi.org/10.1016/j.ijcip.2014.03.001

Boait, P., Neville, G., Norris, R., Pickman, M., Tolhurst, M., & Walmsley, J. (1988). *The OSI Model. In Open Systems Interconnection*, 26-46. Macmillan Education UK. https://doi.org/10.1007/978-1-349-10306-5_3

Byres, E., Karsch, J., & Carter, J. (2005). *Firewall Deployment for SCADA and Process Control Networks Good Practice Guide*.

Department of Homeland Security (DSH) (2016a). *Critical Manufacturing Sector Cybersecurity Frame-work Implementation Guidance*. Available at: https://www.dhs.gov/critical-manufacturing-sector-resources (Accessed: October 2017).

Department of Homeland Security (DSH) (2016b). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. DHS.

International Electrotecnical Commission (IEC) (2009). *IEC/TS62443-1-1Technical Specification: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*. GVA: IEC.

Kagermann, H., Wahlster, H., & Helbig, J. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*. Available at: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf (Accessed: October 2017).

KEP Server EX (2017). Available at: https://www.kepware.com/en-us/products/kepserverex/ (Accessed: October 2017).

Kletti J (2006). *Manufacturing Execution Systems-MES*. BER: Springer. https://doi.org/10.1007/3-540-28011-1

Lee, J., Bagheri, B., & Kao, H.A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3, 18-23. https://doi.org/10.1016/j.mfglet.2014.12.001

Mahnke, W., Leitner, S.H., & Damm, M. (2009). *OPC unified architecture.* BER: Springer Science & Business Media. https://doi.org/10.1007/978-3-540-68899-0

MESA International (n.d). Available at: http://www.mesa.org/en/modelstrategicinitiatives/MESAModel.asp (Accessed: October 2017).

National Cybersecurity and Communications Integration Center (ICS-CERT) (n.d.). Available at: https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities#under (Accessed: October 2017).

National Institute of Standards and Technology (NIST) (2006). *SP800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*.

Nmap (2017). Available at: https://nmap.org/ (Accessed: October 2017).

Nunes, B.A.A., Mendonca, M., Nguyen, X.N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. I*EEE Communications Surveys & Tutorials*, 16(3), 1617-1634. https://doi.org/10.1109/SURV.2014.012214.00180

OPC Foundation (2015). *OPC Unified Architecture Specification Part 2: Security Model*. OPC Foundation.

Open Networking Foundation (2017). Available at: https://www.opennetworking.org/software-defined-standards/specifications/ (Accessed: October 2017).

Openvswitch (2016). Available at: http://openvswitch.org/ (Accessed: October 2017).

Repository of Industrial Security Incidents (RISI) (2017). Available at: http://www.risidata.com/Database (Accessed: October 2017).

Satasiya, D. (2016). Analysis of Software Defined Network firewall (SDF). In *Wireless Com-munications, Signal Processing and Networking (WiSPNET). International Conference* (228-231). IEEE. https://doi.org/10.1109/w.2016.7566125

Sauter, T. (2010). The three generations of field-level networks-Evolution and compatibility issues. *IEEE Transactions on Industrial Electronics*, 57(11), 3585-3595. https://doi.org/10.1109/TIE.2010.2062473

Shodan (2017). Available at: https://www.shodan.io (Accessed: October 2017).

SHODAN Industrial Control Systems (2017). Available at: https://www.shodan.io/explore/category/industrial-control-systems (Accessed: October 2017).

Smith, S. (2015). *Cybercrime will cost business over 2 Trillion*. Available at: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion (Accessed: October 2017).

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. NIST. https://doi.org/10.6028/NIST.SP.800-82r2

Trema (2017). Available at: https://trema.github.io/trema/ (Accessed: October 2017).

UaExpert (2017). Available at: https://www.unified-automation.com/products/development-tools/uaexpert.html (Accessed: October 2017).

Journal of Industrial Engineering and Management, 2018 (www.jiem.org)