Software-Defined Networking to Improve Cybersecurity in Manufacturing Oriented Interoperability Ecosystems

Francisco Fraile, José Luis Flores, Raúl Poler and Eduardo Saiz

Abstract Industry 4.0 is reshaping the manufacturing industry. Through Industrial Internet of Things (IIoT) and cloud computing, manufacturing orientated interoperability ecosystems allow companies to reinvent the use of manufacturing data in value creation. Cybersecurity is a critical aspect in the design of these interoperability platforms to ensure safety in manufacturing operations. Software-Defined Networking (SDN) allows to control the network architecture and behavior in a programmatic way, thus enabling innovative cybersecurity concepts that can be applied to manufacturing orientated interoperability ecosystems. The Virtual Factory Open Operating System (vf-OS) is an innovative multi-sided platform designed to enable collaboration between manufacturing companies. The vf-OS Holistic Security and Privacy Concept incorporates the latest standards and technologies to enable interoperability with industrial control systems (ICS) in the vf-OS ecosystem. This paper uses this state-of-the-art security concept to describe the role of SDN in securing manufacturing oriented interoperability ecosystems and presents an innovative proposal to further improve cybersecurity using SDN technology.

Keywords Privacy and security in enterprise interoperability · Platforms and infrastructures for enterprise interoperability · Interoperability in industry 4.0

1 Introduction

After the three industrial revolutions brought by steam engines, electricity, and automation, the concepts and technologies of the fourth revolution, coined Industry 4.0, are helping manufacturing companies to reinvent themselves, increasing productivity or shifting to new business models in order to remain competitive [1]. Among these concepts and technologies that are reshaping the manufacturing

F. Fraile (✉) · R. Poler
Universitat Politècnica de València, 46023 Valencia, ES, Spain
e-mail: ffraile@cigip.upv.es

J. L. Flores · E. Saiz
IK4-Ikerlan Technology Research Centre, 20500 Guipuzkoa, Spain

K. Popplewell et al. (eds.), *Enterprise Interoperability VIII*, Proceedings of the I-ESA Conferences 9, https://doi.org/10.1007/978-3-030-13693-2_3

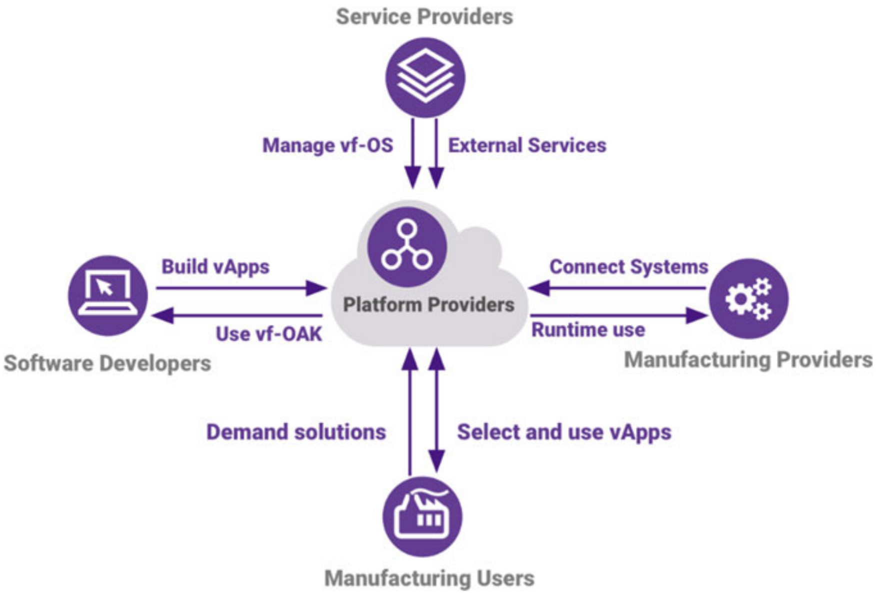

Fig. 1 vf-OS Platform concept

industry, Industrial Internet of Things (IIoT) [1] and cloud computing allow manufacturing companies to leverage the potential of production data far beyond the possibilities of any traditional manufacturing execution system (MES) [2]. These technologies enable the creation of data streams along the entire production process and among supply chains that can be used to monitor manufacturing assets and/or value streams in real time. In combination with data analytics, machine learning, and artificial intelligence, they provide the basis for gaining predictive insights into any supply chain process [1], from customer relationship management, through manufacturing flow management, to returns management. Moreover, bringing together these cybernetic systems and the physical world through actuators, cobots, and other smart devices that can sense and interact with the physical world—comprising what is known as cyber-physical systems [3]—provides endless possibilities for manufacturing. Some of the applications of these technologies are advanced fault detection for maintenance operations, waste reductions for lean manufacturing operations or support to collaborative manufacturing.

The Virtual Factory Open Operating System (vf-OS) Platform [4] is a multi-sided platform orientated to manufacturing and logistics companies that exploit these technologies through a range of services to integrate better manufacturing and logistics processes within organizations and among supply networks. These services are instantiated by applications (vApps) developed by independent software developers and available within a given vf-OS Platform installation, which can be hosted in the cloud. The vf-OS Platform concept is shown in Fig. 1.

The value proposition for the different customer groups of the multi-sided platform is clear:

- Manufacturing users can select and use vApps from the marketplace to integrate manufacturing and logistics processes, enabling collaboration in the value chain. If they do not find any applications suitable for their needs they can demand the development of new solutions to software developers.
- Software developers gain access to a new and high-growth potential market of applications for Industry 4.0 and the Factories of the Future.
- Manufacturing providers delivering products and services to manufacturing users have new ways to collaborate and interact with their customers and provide added value.
- Service providers can provide new services (hosting, storage, cloud services, etc.) to realize the vf-OS ecosystem.

Within the vf-OS system architecture, there are certain components designed to interact with all kinds of manufacturing assets, both physical devices (e.g., PLCs or sensors) and business software applications (e.g., ERPs or CRMs). These components, known as Input–Output (IO) Components, confirm the Virtual Factory I/O (vf-IO) and implement interoperability mechanisms specifically oriented to manufacturing processes.

In order to materialize this, it is necessary to implement holistic cybersecurity and privacy concept covering all the interactions in the multi-sided platform shown in Fig. 1. Securing the use of vApps that interact with industrial control systems (ICS) is a particularly sensitive issue, given the criticality of industrial control in manufacturing processes. This paper describes the specific security standards, specifications, and technologies used in the design of the vf-OS holistic cybersecurity concept to enable secure interoperability with manufacturing assets. Later, it describes a series of security solutions based on Software-Defined Networking (SDN) [5] that can be used to implement and enhance the proposed network layer security mechanisms. Furthermore, SDN technology allows to control the behavior and the topology of the network in a programmatic way and represents a new paradigm in networking that can bring many benefits to manufacturing oriented interoperability ecosystems such as vf-OS.

2 vf-OS Holistic Security and Privacy Concept

2.1 Thread Model and Response

vf-OS provides a flexible infrastructure to develop and deploy applications that act as interoperability mechanisms between manufacturing assets within organizations and among supply networks. Flexibility is achieved thanks to the microservices [6] architecture of the vf-OS Platform: vApps are built on top of a series of heterogeneous, potentially distributed, components that provide well-defined web services.

Protecting and preserving this infrastructure is a significant challenge since it concentrates all classical security requirements (confidentiality, integrity, and availability) in a challenging environment with a multi-fold threat model:

- Public Services: The vf-OS marketplace is a public web service on the Internet providing applications, components, identities, and services. Every web service on the Internet is subjected to any kind of threat, and the attack surface comprises a significant list of elements (information gathering, configuration management, data in transit, authentication, etc.). Moreover, attackers have the target permanently available to test different attack techniques. In order to address this threat, the main reference for vf-OS is the Open Web Application Security Project (OWASP) [7] initiative security guidelines and recommendations to secure web services, which are the core of vf-OS technology.
- The vf-OS internal microservices need to be deployed in factories, implementing interoperability mechanisms with industrial control systems (ICS) as well as with other services. This represents a very critical environment from a security perspective, since attacks to ICS may not only cause great economic losses to manufacturing companies but also put in risk the safety of operators. The security architecture presented in the next section has been designed according to the ISA/IEC-62443 [8] security standard for ICS. In the terminology of IEC 62443, vf-OS is installed as an industrial device, following the same flow as any certificated industrial device. In addition to this, vf-OS implements a centralized security management system based on the Security Content Automation Protocol (SCAP) [9] to enable automated vulnerability management, measurement and policy compliance evaluation of heterogeneous and complex systems, facilitating the alignment with OWASP and the management of IEC-62443.
- Software developers use a public development kit, i.e., the vf-OS Open Application Kit (vf-OAK) to develop vApps. This implies the possibility of introducing bugs and malware which can affect public services and/or internal services. The OWASP Secure Coding Practices Reference Guide and Checklist [7] are implemented in the vf-OAK to ensure that security aspects are taken into consideration in the development process. Additionally, as described in the next section, the security architecture implements a public key infrastructure (PKI)-based system to identify developers and several mechanisms to guarantee security during the application life cycle.
- Personal data protection: Multi-party architectures need to ensure the privacy of user personal data. The recent adoption of the GDPR [10] and the future launching (May 25, 2018) of the new regulation, implying mandatory enforcement, has a direct impact in how vf-OS manages personal data. vf-OS privacy has been designed with data protection by design and by default. vf-OS implements mechanisms to protect personal information (such as pseudonymization), inform of possible data breaches, ask for explicit consent when required, and provide records of processing activities from the vf-OS permanent logging service.

2.2 Security Architecture

Figure 2 illustrates the vf-OS Security Architecture which provides interoperability mechanisms compliant with the ISA/IEC-62443 secure ICS network architecture. This standard applies a defense-in-depth strategy where the network is divided into zones or segments according to the functionality of the systems connected to the network. The Enterprise Level 1 zone contains the vApps and other services that can be accessed through the Internet, like the enterprise content management system (ECM).

The Enterprise Level 1 is considered a second demilitarized zone. The Enterprise Level 0 zone connects other corporate services that can be accessed across the entire corporate network, like the customer relationship management (CRM) or enterprise resource planning (ERP) software. The Industrial Zone Level 2 interconnects the operative systems like the SCADA or MES Systems. The Industrial Zone Level 1 and 0 interconnect the most critical industrial control network components, PLCs, and field components like IO modules and sensors. Redundant switches interconnect systems in each zone. Firewalls implement filtering rules to limit network access between the different segments so that only allowed connections between levels can be established. This way, an attacker willing to penetrate the ICS will meet the different Firewalls preventing further access across the network and protecting critical industrial control components.

The microservice architecture adopted in vf-OS allows to deploy each vf-OS component at the optimal network segment according to the ISA/IEC-62443 defense-in-depth strategy. The Enterprise Level 1 hosts vApps that provide interoperability mechanisms to enable collaboration among supply chain networks, as well as external services, which are components that exchange information with cloud services. The Enterprise Level 0 connects the vf-OS Kernel Services, proving the core vf-OS services and the API connectors which provide interoperability mechanism with corporate software systems and applications. On the other hand, device drivers are located within the Industrial Zone Levels, depending on how they interact with automation equipment. Device drivers can implement industrial communication protocols like OPC UA [11] to interact with control and field components from the operation segment or can be embedded into PLCs or smart sensors.

vf-OS introduces a new segment in the Enterprise Level for the vf-OS Security Command Center, which is the vf-OS component that implements the authentication and authorization services that orchestrate the entire security concept. The Command Center implements a role-based access control–attribute–based access control (RBAC-ABAC) [12] model to implement access control and restrict access to data. The RBAC-ABAC model combines the best features of RBAC with attribute-based systems to improve security for distributed and rapidly changing applications. In this model, security policies [8] determine which manufacturing assets can be accessed

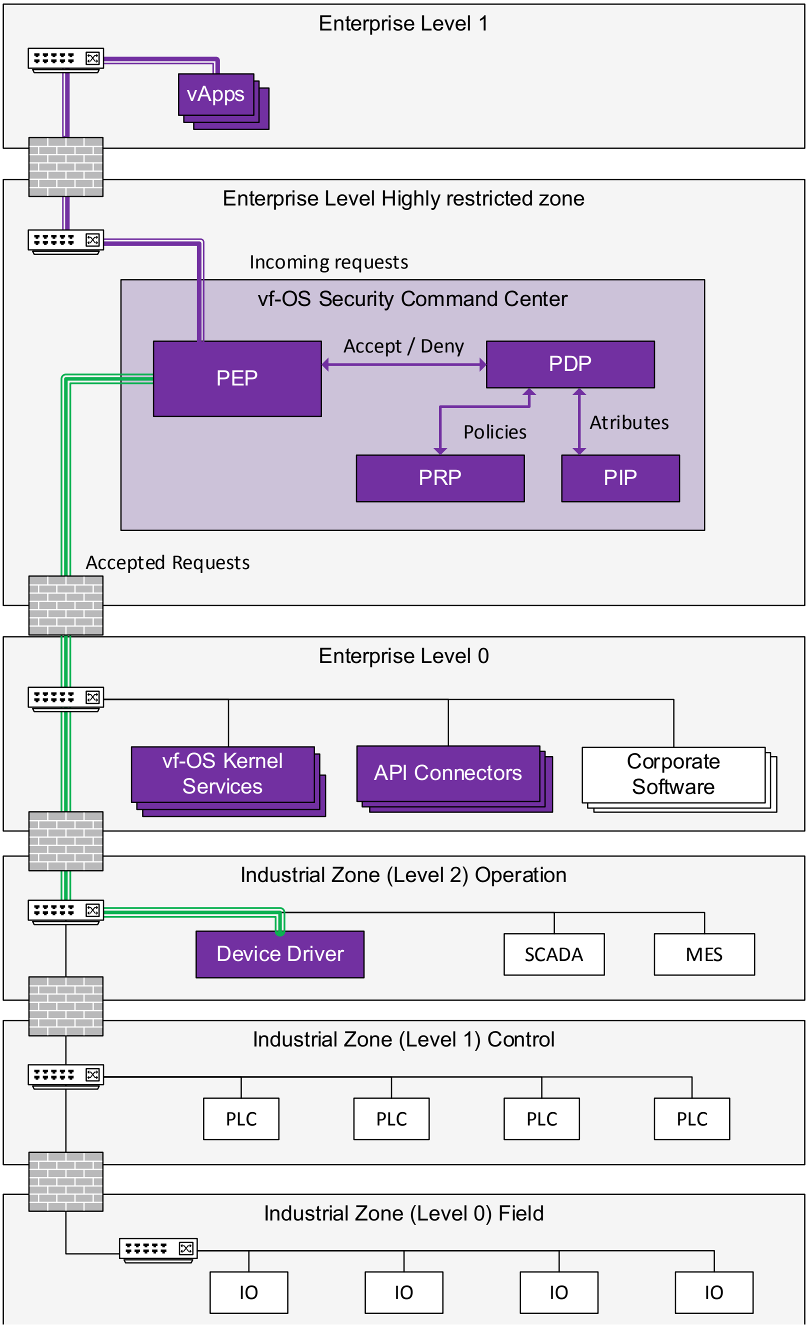

Fig. 2 vf-OS Secured Architecture

and what are the operations allowed (e.g., read or read/write). Defined security policies are later assigned to user groups in the RBAC-ABAC model. The Security Command Center acts as a security proxy. The internal Policy Enforcement Point (PEP) intercepts every request made by vApps and forwards it only when it complies with the access rules established by the security profile. The forwarding decision is made by the Policy Decision Point (PDP) which retrieves the policies and additional attributes, respectively, from the Policy Retrieval Point (PRP) and Policy Information Point (PIP) components. The Security Command Center also provides RESTful APIs to control the security model so that it can be flexibly adapted to every use case. The vf-OS Holistic Security and Privacy Concept is compatible with other open platforms such as FIWARE [13], and it is possible to securely integrate components from these external platforms (enablers).

Firewalls, on the other hand, restrict network access based on rules that determine which connections are allowed or restricted in each network segment. State-of-the-art application Firewalls implement application control by means of in-depth packet inspection to apply filters based on application layer rules. For instance, they are able to determine HTTP traffic and block connections, but they have no knowledge of ad hoc REST APIs, and therefore, they cannot apply more sophisticated security restrictions. This means that in the security architecture, vf-OS implements application layer security mechanisms, the underlying protocols (HTTPS) implement communication layer mechanisms, whereas Firewalls implement network layer security mechanisms. However, it is important to note that these mechanisms at the different layers are loosely coupled.

This is not the case if SDN technology is introduced in the architecture, since it allows to integrate switches and Firewalls in the holistic security concept, coordinating security decisions at the different layers to provide enhanced security, performance, and flexibility. Next section describes the SDN technology in the context of security for interoperability platforms as a means to achieve this integration.

3 SDN Network Layer Security

As explained above, the secured network architecture of ISA/IEC 62443 standard in Fig. 2 proposes the use of Firewalls to limit the exposure of industrial control devices to Internet attacks with a defense-in-depth strategy.

With this architecture, an attacker pretending to intrude the Industrial Zone (Level 1) Control network segment needs to attack each Firewall from the Enterprise Level 1 to gain access to the successive network segments. Basically, this consists of figuring out how to generate traffic that meets the security filtering rules programmed into each Firewall and find means to use this information in order to perform another attack to the next level. Application control allows 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 to some extent. The main limitation is the processing capacity of the Firewall to read complex context information. For instance, Firewalls are able to detect HTTP request for every method but they are not able to implement dynamic filtering rules adapted to the business logic of a specific REST API.

Conversely, SDN technology allows to implement this kind of advanced filtering techniques in order to mitigate security risks. SDN Firewalls were introduced in [5] SDN Firewalls, whereas [14] presents a SDN Firewall specifically designed for Industry 4.0. Basically, a SDN Firewall allows an external controller to modify the forwarding tables that define the behavior of the network. This not only means that the controller can configure the bridges between network segments but also to control the security configuration of every network interface. This takes the defense-in-depth strategy of ISA/IEC 62443 to a new level, since each network boundary faces other system boundaries through secured interfaces.

This concept of protective network structure for manufacturing systems with a specialized SDN Firewall based on the OPC UA and OpenFlow standards is presented in [14]. The SDN has two main functionalities: first, to detect automation devices automatically and group them into the appropriate network segment, and second, to integrate OPC UA application layer security mechanism into the SDN Firewall controller. This way, administrators need only to allow access between OPC UA server and clients. The SDN Firewall controller uses this information to set up the filtering rules applied at each network interface in the industrial zone.

The same concept can be applied in vf-OS to extend the protective network structure to the entire network and to integrate all the security mechanisms at the different layers. This concept is shown in Fig. 3. When a vApp wants to connect to a vf-OS component, the request is forwarded to the vf-OS Security Command Center. The PDP determines whether the connection is accepted or not depending on the defined security policies and attributes. The PEP enforces the decision, but this time, by controlling the approved physical connections in the SDN network, instead of acting like a proxy. Furthermore, more attributes can be defined at the device driver level to integrate specific industrial protocol security rules into the RBAC-ABAC model.

This way, the configuration and control of all the security mechanisms are integrated and centralized in the vf-OS Security Command Center. The network security configuration is dynamic so that connections are only allowed when vApps require them (temporal filtering) and only between the required network components (spatial filtering) which makes it harder for attackers to learn what kind of traffic meets the security rules.

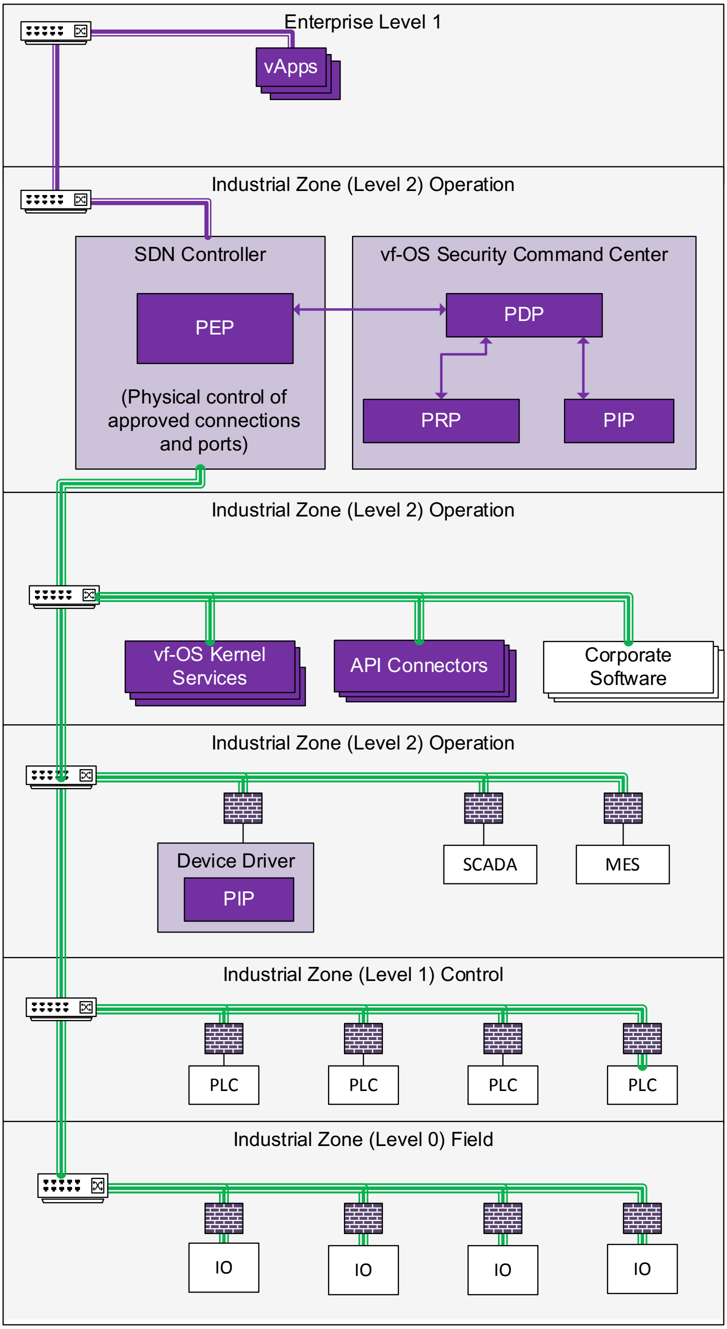
Enterprise Level 1
vApps
Industrial Zone (Level 2) Operation
SDN Controller
PEP
(Physical control of approved connections and ports)
vf-OS Security Command Center
PDP
PRP
PIP
Industrial Zone (Level 2) Operation
vf-OS Kernel Services
API Connectors
Corporate Software
Industrial Zone (Level 2) Operation
Device Driver
PIP
SCADA
MES
Industrial Zone (Level 1) Control
PLC
PLC
PLC
PLC
Industrial Zone (Level 0) Field
IO
IO
IO
IO

Fig. 3 vf-OS Security Concept with SDN Firewalls

4 Conclusions

Cybersecurity is a critical aspect in the design of interoperability platforms and ecosystems. This paper has presented the holistic security and privacy concept applied in vf-OS, which represents a challenging ecosystem due to the complexity and variety of elements involved (from the cloud to industrial environments). The security concept responds to the multifold thread model of this interoperability environment applying the most modern security technologies and standards.

In order to further improve security, flexibility, and performance, this paper introduces a SDN Firewall into the holistic security concept. This makes it possible to coordinate security decisions at the different layers, from the application layer, through the connection layer, to the network layer, in order to provide a centralized security response to cyberattacks in interoperability platforms and ecosystems. SDN Firewalls are inherently faster at traffic processing and can enhance the current possibilities of application Firewalls. In this sense, SDN Firewalls can implement more sophisticated rules for data inspection and filtering, based not only in the structure of packets, but also on the specific business logic of the different vApps and underlying REST microservices. Thus, the future research will address the possibilities of SDN Firewalls to detect malicious behavior or malicious entities, based on context knowledge (e.g., knowledge of installed manufacturing devices, vApps, users), rather than just analyzing isolated network data packets.

SDN Firewalls can also simplify the integration and management of the secure network architecture and defense-in-depth strategy promoted by cybersecurity standards for industrial control networks like ISO 62443. SDN networks can be controlled dynamically with software, meaning that the vf-OS Security Command Center could also potentially control the topology of the network based on the specific requirements of vApps at any given moment of time. This is another interesting line of work for the future research.

References

1. Kagermann, H., Helbig, J., Hellinger, A., & Wahlster, W. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group*. Forschungsunion.
2. Kletti, J. (2013). *Manufacturing execution system–MES* (1st ed.). Berlin: Springer.
3. Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The Impact of Control Technology, 12,* 161–166.
4. vf-OS Homepage. (2017). http://www.vf-os.eu. Last Accessed 31 Oct 2017.
5. Nunes, B., Mendonca, M., Nguyen, X., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials, 16*(3), 1617–1634.
6. Nadareishvili, I., Mitra, R., McLarty, M., & Amundsen, M. (2016). *Microservice architecture: Aligning principles, practices, and culture* (1st ed.). Sebastopol: O'Reilly Media Inc.
7. OWASP Homepage. (2017). https://www.owasp.org/index.php/Main_Page. Last Accessed 31 Oct 2017.

8. International Electrotechnical Commission (IEC) TS 62443-1-1 ed1.0. (2009). *Industrial communication networks—network and system security—part 1-1: Terminology, concepts and models* (pp. 7–83).
9. Radack, S. M. (2010). Security content automation protocol (SCAP): Helping organizations maintain and verify the security of their information systems. *ITL Bulletin*.
10. GDPR Homepage. (2018). https://www.eugdpr.org/. Last Accessed 15 Jan 2018.
11. OPC Foundation. (2010). *OPC unified architecture specification part 2: security model*.
12. Kuhn, D. R., Coyne, E. J., & Weil, T. R. (2010). Adding attributes to role-based access control. *Computer, 43*(6), 79–81.
13. FIWARE Homepage. (2017). https://www.fiware.org/. Last Accessed 31 Oct 2017.
14. Tsuchiya, A., & Fraile, F., Poler, R., & Ortiz, A. (2017). Software defined networking firewall for OPC UA MES systems. In *11th International Conference on Industrial Engineering and Operations Management, Springer, Valencia*.