Addressing Industry 4.0 Security by Software-Defined Networking

9

Rahamatullah Khondoker, Pedro Larbig, Dirk Scheuermann, Frank Weber, and Kpatcha Bayarou

9.1 Introduction

Preceded by three industrial evolutions with the virtue of innovation in basic technologies such as mechanics (first evolution, beginning in the 1780s), electricity (second evolution, beginning from the 1870s), and electronics and computation (third evolution, starting from the 1970s), the vision for the fourth industrial evolution (in German called Industrie 4.0) has been started by the German government in 2011 [1]. German activities are mostly driven by the German association with the title Platform Industrie 4.0. The aim of this campaign is to improve the economy of the European (especially German) region by creating platforms for smart factories where the key enablers are interconnection (Internet) of all of the components by information and communication technologies (ICT) including cyber-physical systems (CPS) and the Internet of things (IoT) [2].

Similar to Industrie 4.0, coexisting approaches are seen internationally, e.g., by the Advanced Manufacturing Partnership and Industrial Internet Consortium (IIC) in the USA, by Industrial Value Chain Initiative (IVI) in Japan, and Made in China 2025 and Internet Plus initiatives [3] in China. These associations also work together with the previously mentioned German association. There exist different concerns in the different countries, depending on the individual business structures and strategies, and the term of the fourth industrial evolution is synchronized with

R. Khondoker (✉) • P. Larbig • D. Scheuermann • F. Weber • K. Bayarou
Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT), Rheinstr. 75, 64295, Darmstadt, Germany
e-mail: rahamatullah.khondoker@sit.fraunhofer.de; pedro.larbig@sit.fraunhofer.de; dirk.scheuermann@sit.fraunhofer.de; frank.weber@sit.fraunhofer.de; kpatcha.bayarou@sit.fraunhofer.de

S.Y. Zhu et al. (eds.), *Guide to Security in SDN and NFV*, Computer Communications and Networks, DOI 10.1007/978-3-319-64653-4_9

the German initiatives. However, the general idea is always the same: Production machines shall be connected via the Internet and be equipped with automatic control of production processes and protection against attacks from inside and outside.

The International term for Industrie 4.0 is Industry 4.0/Integrated Industry [4], and we will use the term Industry 4.0 for the general idea mentioned above. The technologies that are currently available in the production, i.e., preceding Industry 4.0, will be referred to as "pre-Industry 4.0" in this chapter. The assumption is that "pre-Industry 4.0" production machines have only very limited Internet connectivity; hence, they have very limited usage of security functionalities and do not fulfill the security requirements necessary for Internet connectivity.

Similar to office/enterprise networks, IT security (with a dedicated focus especially on network security) is considered as one of the most important aspects of Industry 4.0 as the enabling information and communication technologies (ICT) may bring threats to production networks (e.g., due to vulnerabilities in the enabling technologies, lack of protection capabilities of industrial control systems protocols, etc.). Therefore, especially to ensure network security in Industry 4.0, the IUNO project has been launched by the German Federal Ministry of Education and Research (BMBF) [5].

The aim of IUNO is to identify security threats and risks for Industry 4.0 factories (sometimes called smart factories), develop proactive measures to tackle the identified threats and risks, and implement those measures in application scenarios corresponding to the four items *secure process* (customer-specific production), *secure data* (technological data market), *secure service* (remote maintenance), and *secure network* (visual security control room), respectively.

To contribute in achieving the aim of IUNO, software-defined networking (SDN) is investigated for Industry 4.0 since it can be used intelligently to automate manifold tasks, including, but not limited to, user administration, routing, monitoring, controlling, security, and configurability. These tasks could also be accomplished using traditional non-SDN-based proprietary networking devices (such as switches and routers), which however require manual effort. The proprietary networking devices are statically placed in a particular location in a network, necessary to configure each of those devices individually, complex (hardware part of a device contains billions of gates, and the software part consisting of OS and applications is the implementation of more than 6000 standard documents), not programmable (contains no open/standard API), and difficult to manage (having no centralized configuration/management possibilities).

To tackle these issues, SDN decouples control plane of a networking device from the data plane where the planes communicate with each other by using protocols such as OpenFlow [6] so that the data plane can be directly programmed. As shown in [7] which is authored by Open Networking Foundation (ONF), the SDN architecture consists of three layers: infrastructure layer, control layer, and application layer (see Fig. 9.1). The control layer consisting of a network operating system, also called SDN control software, enables programmability of the network devices located in the infrastructure layer through the so-called SDN southbound interface (SBI) protocols. Some examples of SBI protocols are OpenFlow, the Network

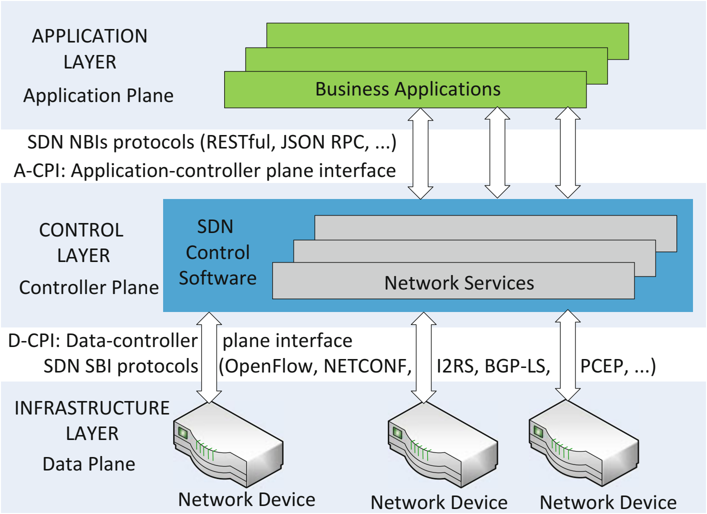

Fig. 9.1 SDN architecture from Open Networking Foundation [7]

Configuration (NETCONF) protocol, Interface to the Routing System (I2RS), Path Computation Element Protocol (PCEP), and Border Gateway Protocol with Link State (BGP-LS). The interface between the application plane and the controller plane is called application-controller plane interface (A-CPI). The application layer which implements business logics communicates with the controller located in the control layer through the so-called SDN northbound interface (NBI) protocols such as Representational State Transfer (REST/RESTful) and JavaScript Object Notation Remote Procedure Call (JSON-RPC). The interface between the controller plane and the data plane is called data-controller plane interface (D-CPI). There are many open-source and proprietary controllers in the market. Most prominent open-source ones are the Open Network Operating System (ONOS), OpenDaylight, Python version of network operating system (POX), and Ryu. A comparison of some controllers considering the criteria such as interfaces used, GUI availability, REST API support, documentation, programming languages support, TLS, and OpenFlow protocol support can be found in [8].

Motivated by the utilization of SDN architectures to improve network security such as OrchSec [9, 10] and AutoSec [11], this chapter describes how the security of Industry 4.0 could be improved by SDN. The architecture described in Sect. 9.2 is just an example for a pre-Industry 4.0 factory and its respective security status. From this state of the art, the requirements for Industry 4.0 are derived in Sect. 9.3. For example, two of the Industry 4.0 security functionalities, namely, industrial IDS/IPS and secure remote maintenance service, are explained in Sects. 9.4.1 and 9.4.2. Section 9.5 gives a short discussion on the relevance of the proposed SDN-based solutions for the security requirements mentioned before. Finally, the chapter is concluded with the summary in Sect. 9.6.

9.2 Security of Pre-Industry 4.0 Production Network

Pre-Industry 4.0 production machines and their network were not built to be connected to the Internet; therefore, their characteristics are different from office/enterprise IT components which were built considering Internet connectivity as shown in Table 9.1.

By deploying intermediate devices such as middleboxes (firewall/packet filter), however, industries started to connect their pre-Industry 4.0 production machines and networks to the Internet.

The protocols that are used within pre-Industry 4.0 production networks can be categorized into two types: classical Fieldbus and industrial Ethernet protocol. Some examples of protocols for production networks are shown in Table 9.2.

The production network protocols are not secure by design, therefore, lack of basic security mechanisms to provide confidentiality, authentication, and integrity.

Encryption mechanisms are required to ensure data confidentiality; however, no such mechanisms exist in these protocols as these were designed to fulfill the safety requirements such as short transmission time and high availability, not security. The encryption mechanisms from IT may not fulfill those requirements.

Authentication mechanisms (password based, certificate based, biometrics, multifactor, single sign-on, etc.) are required to protect from threats including message/identity spoofing and non-repudiation. Except Secure DNP3 (the security extension of DNP), no other classical Fieldbus and industrial Ethernet protocols in Table 9.2 provide authentication mechanism.

To protect data from tampering by man-in-the-middle attacks (i.e., message spoofing, identity spoofing, and replay attacks), integrity protection mechanisms

Table 9.1 Comparison of pre-Industry 4.0 production machine and enterprise IT component

Criteria	Production machine	IT component
Example	Shaping machine	Web server
Longevity (approximately in years)	10–30	0.5–3
Internet connectivity	No	Yes
Security (methods available)	Yes (isolated by air gap)	Yes
Safety (mechanisms available)	Yes	Yes
Updatability requirement	Seldom	Often
Availability requirement	High	High

Table 9.2 Examples of production network protocols

Classical fieldbus	Industrial Ethernet protocol
PROFIBUS	EtherCAT
Modbus	SERCOS III
DNP3	PROFINET
ControlNet	EtherNetIP
DeviceNet	ModbusTCP
Secure DNP3	POWERLINK

such as Secure Hash Algorithm 3 (SHA-3), Message Digest 5 (MD5), and Hash-based Message Authentication Code (HMAC) are required. However, no other classical Fieldbus and industrial Ethernet protocols except DNP3 and Secure DNP3 in Table 9.2 provide this mechanism. It is worthy to note that cyclic redundancy check (CRC) and checksum are not integrity protection mechanisms but error detection mechanisms.

In pre-Industry 4.0 production network, add-on security was used to protect the network, for example, Common Industrial Protocol Security (CIP Security) [12] was used as an add-on to protect the Ethernet/IP protocol by integrating authentication, encryption, and integrity check mechanisms.

For Industry 4.0, well-known, secure, and standardized protocols of the office networks such as Transport Layer Security (TLS), Internet Protocol Security (IPsec), Secure Socket Shell (SSH), Wi-Fi Protected Access 2 (WPA2), Open Platform Communications Unified Architecture (OPC UA), Data Distribution Service (DDS), Message Queue Telemetry Transport (MQTT), and Datagram Transport Layer Security (DTLS) could be used to secure the production networks. However, these protocols add latency and cannot guarantee any safety properties.

To improve the security of pre-Industry 4.0 production network, one or more security (hardware/software) devices such as a firewall or packet filter is used, though they cannot handle some security threats, for example, malware, when brought into the network using a memory stick (as happened in the Stuxnet scenario). Two general approaches are followed to deploy such a security system. One option is to place a complementary hardware device which consists of several security functionalities such as firewall and packet filter. Another option is to deploy a router which connects the production network with the Internet and can be configured to enable, for example, firewall, packet filter, etc. functions. In this case, no additional hardware device is needed for security.

In some cases, firewalls are used between the pre-Industry 4.0 production network and the Internet so that only the packets/flows matching the firewall rules are allowed to enter the production network and the unmatched packets/flows are rejected. Each packet/flow that is sent to the production network from the Internet is checked by the firewall against a set of rules that are called firewall rules and are defined either by the network administrator or by firewall vendor (these default rules are used when no expert network administrator is available). Some simple firewall rules are shown in Table 9.3 where each rule consists of a *rule number*, the *protocol* for which the rule is valid, the particular network or port the packet departs *from*, the particular network or port *to* which the packet is sent, and the *action* to be taken where two valid actions are *allow* and *deny*.

Besides firewall, a network address translation (NAT) is also used in pre-Industry 4.0 production network. Though the original purpose of NAT was to alleviate the problem of "Shortage of IPv4 addresses to identify all devices in the Internet as it can address 2^{32} devices uniquely," however industries mistakenly use it as a security module. A NAT, which is usually integrated in the edge router, translates from the private IP address to the public IP address (in case of outgoing traffic) so that only that public IP address is visible in the outside world while keeping the address of

Table 9.3 Some exemplary firewall rules

Rule No.	Protocol	From	To	Action
1.	IP	217.224.0.0/11	217.10.48.0/20	Allow
2.	IP	217.10.48.0/20	Any	Allow
3.	TCP	Any	5060	Deny
4.	UDP	Any	69	Deny
5.	DNS	Any	Any	Allow
6.	SMTP	Any	Any	Allow

the production machines hidden. In case of incoming traffic, the NAT translates from the public IP address to the private address. However, NAT alone (without firewall) does not protect from stateless NAT devices that allow all types of traffic even from the attackers. Besides, NAT alone cannot prevent outbound attacks from Stateful NAT hosts [13].

The disadvantages of these security solutions are stated below:

1. Proprietary/vendor locked and therefore these solutions are not programmable.
2. Static in nature as, for example, the firewall rules are predefined for a long duration and placed in a particular point.
3. Difficulty in configuration when there exist many such devices which are managed one by one.
4. No central overview of the configuration as each of the security devices is treated individually.

Considering a large company which requires to configure several security devices, each of these devices is configured manually. To configure several devices manually in a consistent way could be difficult to manage as there is no central overview of the configuration. As manual configuration is also time-consuming, the production machines may not be online during that time period which could result in production downtime.

Therefore, Industry 4.0 production networks will require network devices which will be programmable and centrally managed so that new security policies could be deployed immediately as a response to attacks.

9.3 Industry 4.0 Production Network: A Scenario

An architectural scenario for Industry 4.0 production network is shown in Fig. 9.2. Such a network may include production network, office network, SDN switches, and central platform. Several machines including shaping, drilling, and milling are connected to the production network.

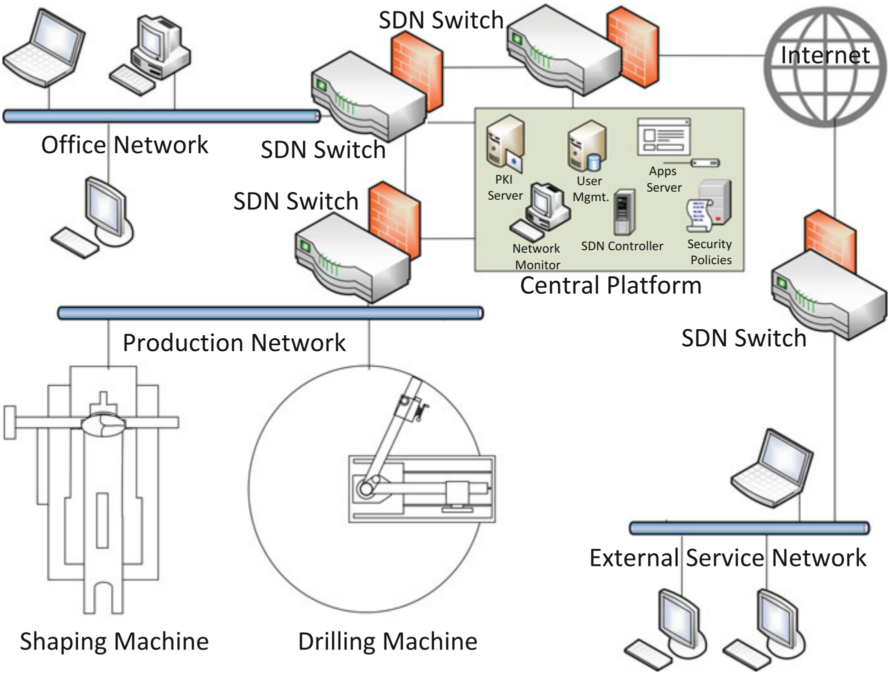

Fig. 9.2 A scenario of Industry 4.0 production network

In this scenario, the central platform server consists of components such as PKI server, application (app) server, user administration and management, network monitor, SDN controller, security policies, routing, etc.

One of the expectations for the success of Industry 4.0 is to increase protection of production machines and components without sacrificing their availability. Therefore, Industry 4.0 production network should support both proactive (encryption, firewall, etc.) and reactive (IDS/IPS) mechanisms. One way to achieve this aim is that the configuration efforts for the firewalls should be minimum which can be achieved by employing SDN-based switches in the networks that can be automatically programmed to create dynamic firewalls. Another way is to be able to detect and mitigate machine faults and illegitimate intruders automatically. This requires an intrusion detection system (IDS), referred to as industrial IDS here to differentiate it from the IDS of an office network. Whereas an office network IDS supports TCP/IP, UDP/IP protocol stacks, industrial IDS supports classical Fieldbus and industrial Ethernet protocols as well.

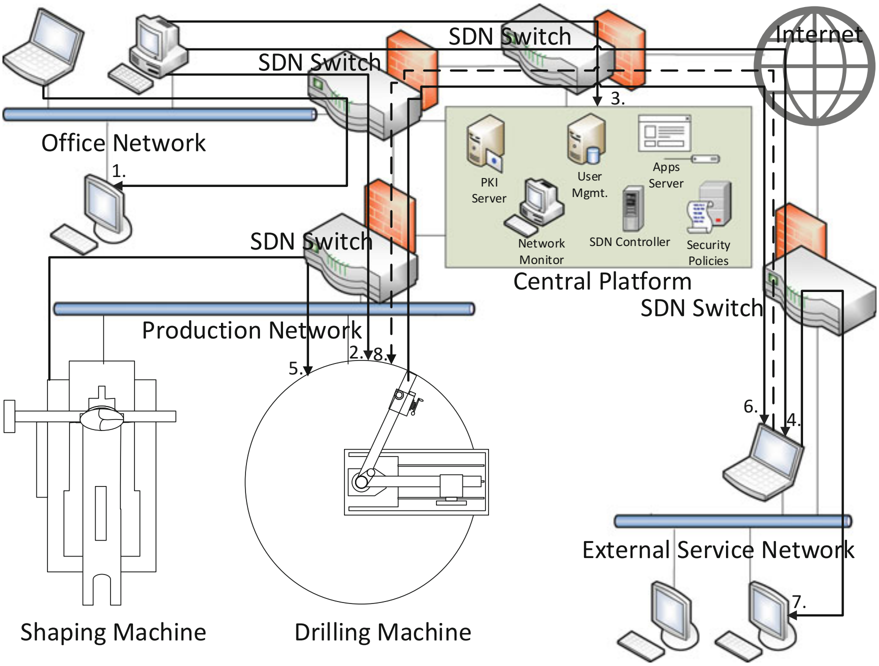

Fig. 9.3 Attack scenario of Industry 4.0 production network

9.3.1 Attack Model

Industrial networks with their often sophisticated structure, involving several network segments and hierarchies, are not easy to protect efficiently against illegitimate traffic originating from sources located at both the outside (outsider threats) or the inside (insider threats) of the network. The threat surface of an Industry 4.0 production network scenario is shown in Fig. 9.3 where the bold black color and dashed black color lines represent insider and outsider threats, respectively.

Some of the insider threats are shown in the figure marked with the bold black color lines and are enumerated in the following:

1. A node in the office network attacks another node(s) in the same network.
2. A node in the office network attacks one or more production machines located in the production network.
3. A node in the office network attacks the central platform.
4. A node in the office network attacks one or more nodes in the Internet.
5. A production machine attacks another production machine.
6. A production machine attacks one or more nodes in the Internet.
7. A node in the external service network attacks another node in that network.

Besides, employees may (un)intentionally download the malwares (virus, Trojans, worms, etc.) from the Internet using e-mail, browser, or other applications. They might also bring the malwares in their USB or other external memory drives. These malwares could be the source of insider threats.

Outsiders could attack the central platform, the office network within the factory, or the production network. This outsider threat is marked as threat no. 8 with the dashed black color line.

To protect industrial networks from both insider and outsider threats, some security functionalities are described in the following: industrial IDS, dynamic firewall, and secure remote maintenance service. These applications are hosted in the app server.

9.4 Examples of Industry 4.0 Security Functionalities

In industrial communication, protection mainly focuses on reactive security, that is, detecting and mitigating any unwanted actions (such as network traffic originating from untrusted sources). This comes naturally as, in contrast to office IT installations, availability and safety have the top priorities for production networks and confidentiality only plays a minor role there. Additionally, these requirements must often be fulfilled by equipment that uses unsupported and outdated software [14] not well suited for the use in industrial installations. A major problem results from the fact that while production machines are built to run multiple decades, the computer operating system that executes the machine-controlling software is typically considered archaic after only a few years. Furthermore, it is a typical case that neither operating systems nor control software are patched or upgraded during the lifetime of a production machine. This aversion to software updates in production machines is justified by the very fragile update processes of the most used operating systems that pose a significant threat to a machine's availability.

Still, attacks on these vulnerable machines were hardly possible since they were only connected to a local network. They did not communicate with the world outside the factory and thus never had to deal with everyday malware activities. However, with the advent of the new industrial revolution, more and more direct or indirect ways are built to send data to those machines in order to allow customers to customize their products or to let maintenance providers work remotely. If these data exchange corridors are established with legacy machines which still run unmaintained and vulnerable software, it can enable attackers and competitors to take control of production.

In the long run, these vulnerable systems will become replaced, and new technology is required that introduces update processes which do not interfere with a system's operation [15, 16]. In the short term, however, it is crucial to protect the existing technology as good as possible while not interfering with its functionality and safety properties.

Thus, we propose an extensive monitoring layer to be introduced by factory operators that passively collects and correlates input data from multiple data sources:

- **Communication data, traffic samples:** Network taps and monitor ports extract copies of packets observed on Ethernet-based field bus installations, SCADA networks, and office networks. The major challenge here is the sheer number of protocols in use. Almost every influential vendor of industrial automation products has established its own protocol. In order to be able to efficiently extract the relevant data out of the captured traffic data, parser generators (like HILTI [17] and Spicy [18]) and packet processing languages (like P4 [19]) can be used, as shown by Udd et al. [20].
- **Event management:** Existing security information and event management (SIEM) systems provide access to log files from the office IT world, including the perimeter firewalls. Additional collectors need to be developed by SIEM integrators to read out and forward events from the SCADA systems and logic controllers to the central IDS.
- **Enterprise management sources:** These sources add metadata to the pool of information provided to the IDS by making information available that describes what to expect when and where. This does contain sets of assignments. Examples are:
  - Employee timetables provide assignments between employees and work time. This can be used to detect account abuse (i.e., log-in, while employee is not working).
  - Inventory listings provide assignments between MAC addresses and device owner.
  - Quality assurance reports provide assignments between time and production quality to correlate system changes to overall production efficiency.
- **Engineering sources:** Provides boundary conditions of operation inside machine specification. Specification documents and data sheets of the devices used in production help in interpreting the field bus traffic to decide if the observed messages might indicate a sabotage attempt, in order to ensure that the software that is being sent to the devices is known to operate inside these specifications. Thus, this data source can also contain hashes and/or signatures for known PLC software to assess any programming actions.

The data that is collected should be preprocessed by the source and then sent to the central intrusion detection system that is outlined in the following section. Preprocessing and filtering are required to reduce the amount of data that is sent to the central IDS, as some data sources can be quite data intensive. Especially modern field bus protocols can generate continuous streams of control data at high bit rates [21] while not providing relevant input as long as the known cycles are performed. Still, a small and unexpected change can be a clear indicator of compromise.

This process can employ reporting protocols using incident descriptors as proposed by the Intrusion Detection Message Exchange Format (IDMEF, [22]) and Incident Object Description Exchange Format (IODEF, [23]) Requests for Comments (RFC) in order to transport the information to the IDS.

9.4.1 Industrial IDS

The ultimate goal of an intrusion detection system for industrial networks is identical to that of a conventional IDS: detecting unwanted actions in the protected networks. These actions include attack attempts from external sources as well as sabotage acts from employees. However, the approaches differ in detail as an IDS in a production environment must not modify or suppress any communication since it may be relevant for safety. This results in the fact that an industrial IDS has to be deemed a passive device that relies on human interaction to counter any detected threats.

Another difference from conventional networks is the complexity of the observed processes in industrial network scenarios. While in IP-based office communication there is a small set of protocols (such as TCP) transporting all kinds of information (e.g., HTTP), in industrial networks, a large set of protocols (see Table 9.2 in Sect. 9.2) is used to transport machine control data. Thus, the complexity is based on the variety of means of transport and not on the transmitted data itself. This simplifies the processing of the payloads which in turn allows multiple approaches on how to generate IDS events out of the observed traffic and traffic patterns:

- **Rule-based anomaly detection:** This standard approach uses attack signatures to detect well-known malicious actions inside the network. All incoming communication is matched against a signature database in the IDS which triggers an alarm in case of a match. While this technique is rather basic, it also has some valuable advantages in industrial networks: The rules can be audited and verified to ensure correct operation and a low amount of false positives. Occurring threats can be classified into risk levels to make prioritization easier when an attack on multiple targets is launched. Additionally, signatures can be exchanged between networks and users to profit from the experience gathered in other installations. However, a major drawback is the inflexibility of this approach when targeting new attacks that have not been known before. If the attackers know what signatures are in place, they can easily circumvent the detection mechanism.
- **Machine learning:** Typically, industrial machines are operated for long periods of time without any significant changes of the production process. At the same time, industrial automation protocols often transport fixed-size and well-defined payloads to be processed by the machines. This fact makes the data exchanged in those networks a good candidate for input of machine learning algorithms that can be used to identify traffic anomalies. When introducing such mechanisms in a network, the algorithms usually start a learning phase first to accommodate to the expected traffic in the environment. In this period of time, the network operators must make sure that no unwanted or malicious actions take place and that all use cases are covered. After the learning phase is completed, the algorithm will then compare any incoming traffic with the previously seen patterns and raises an alert when the deviation between them is too high. On the positive side, an IDS based

on machine learning is very versatile and can be compatible with many protocols and use cases, as it dynamically adapts to the data that is presented. While this saves work for the IDS vendor, the users have to cope with several problems: First, they need to conduct a well-planned learning phase where nothing must interfere with this process or the resulting detection mechanism may be erratic. Also, if anything is changed in the way the machine works, another learning phase must be started to adapt to the changes made. The whole system is rather obscure as there is no easy way to audit and verify the resulting mechanisms. Additionally the output of the learning process can hardly be transferred to other machines and networks, most likely only to relatively similar installations.

- **Programmatic incident investigation:** This new approach supplies the users with tools that enable mimicking the actions of a human network administrator in case of a detected anomaly. Such a system shall provide a way to define actions that are taken after an initial detection to further substantiate the suspicion of a malicious activity. An incident investigation system thus needs access to external data sources that supply the required metadata that enables it to reach a verdict. These sources are mentioned in the beginning of Sect. 9.4. Obviously, the advantages of such a system are the very low amount of false positives combined with the fact that it instantly supplies the administrators with crucial details in case of an attack. Additionally, those systems can be configured to not only trace signs of attacks but also to monitor and manage production efficiency. This can put the high price of setup and maintenance of such systems into perspective.

These three approaches can and should be applied concurrently within an industrial IDS to improve the overall detection mechanism. These approaches could be implemented as SDN applications within the SDN controller when efficiency is given more priority than flexibility or outside of it when flexibility and multiple controllers support are given more importance. The advantage of SDN-enabled hardware in those scenarios is apparent, as they enable fine-grained control over the type of data to extract and send to the IDS for further inspection. When using OpenFlow protocol as an SDN SBI protocol, it supports 12 matchable fields in version 1.0 and 41 fields in version 1.4 [24]. The filtering and preprocessing of data, which can be done efficiently in SDN hardware and SDN controllers, can substantially reduce the load on the IDS and reduce or mitigate the impact of, e.g., denial of service (DoS) attacks.

9.4.2 Secure Remote Maintenance Service

There is no standard definition of the term remote maintenance or administration. For administrating (i.e., accessing, monitoring, repairing, controlling, etc.) an IT system component (such as a server, router, switch, computer) from a remote site (the remote place where the service engineer is located), a remote maintenance service is used. As there is no specific "remote" distance, it can range from several meters to several thousand kilometers. In terms of Industry 4.0, the components to be remotely managed, configured, or maintained are parts of industrial production machines located in the production site.

Remote maintenance does not only reduce OPEX for the enterprises by saving travel and accommodation costs for their employees to be physically in the production site but also increase production efficiency by maintaining (e.g., monitoring, identifying, and repairing) the problem with no travel delay. By intelligently utilizing wireless and wired communication technologies, remote maintenance is possible [25]. Therefore, from the 1990s, several approaches have been proposed to access, monitor, and maintain control processes remotely. Some of these approaches are Distributed Aircraft Maintenance Environment (DAME [26]), SCADA.web [27], and e-Diagnostics. However, security was not their main focal point. e-Diagnostics considered security in the guidebook revision 2.1 [28].

Until now, the main application of remote maintenance in IT and office environment was remote desktop, that is, accessing a computer from another computer where the screen of the remote computer is seen in the screen of the local computer and the remote computer can be operated using the local computer's keyboard and mouse. The mostly used software for remote desktop is Virtual Network Computation (VNC) which uses Remote Framebuffer Protocol (RFP) [29]. The VNC server (VNC server and X client) is installed in the remote computer, and the VNC client (VNC client and X server) is installed in the local computer. The problem with the VNC software is the high configuration effort required for both the client and the server. Besides, according to RFC 6143, "VNC Authentication is cryptographically weak and is not intended for use on untrusted networks."

To solve the abovementioned problems of the VNC software and to offer manageability and add-on security, a central server between the client and the server is used in products like TeamViewer and Netviewer. Irrespective of licenses (free and proprietary), there are around 80 remote desktop software (such as rdesktop, TeamViewer, and GoToMyPC) that are available in the market. Extensive comparison of those software (OS supports, features) can be found at [30]. In terms of security, on the one hand, software like TurboVNC has no built-in encryption and access permission request; on the other hand, software like TeamViewer has AES-256 built-in encryption and requires access permission requests.

The main features of remote desktop and remote maintenance are opposed to each other in Table 9.4. Teradici Personal Computer over Internet Protocol (PCoIP) solution [31] is similar to remote desktop; however, the product is optimized for performance (supports two or four displays, 60fps). In terms of security, it supports AES-128/AES-256 Suite B ciphers. According to their secure remote connections feature, "Mitigate the risk associated with remote data storage on desktops and laptops with Workstation Access Software. Our PCoIP protocol encrypts and authenticates all transmissions – and only transmits encoded pixels, not data."

9.4.2.1 Commercial Solutions for Remote Maintenance

Several providers such as Netbiter [32], Genua [33], Phoenix Contact [34], and Siemens [35] offer products for remote maintenance security in industrial context. Netbiter remote management provides three different communication gateways (EasyConnect 220, 310, 350) to be placed in the production site. These gateways are connected to the system to be monitored using Modbus (Serial or Ethernet),

Table 9.4 Remote desktop versus remote maintenance

Criteria	Remote desktop	Remote maintenance
OS supports	Windows, Linux, Mac, iOS, Android, BlackBerry, OS/2, Windows Mobile, FreeBSD	Windows (e.g., Siemens SIMATIC IPC), Linux
Security protocols	AES, SSH, SSL/TLS	SSL/TLS, AES
Application protocols	RDP, VNC, X11	
Communication protocols	Ethernet, TCP/IP	CIP, EtherNet/IP, DeviceNet, CompoNet, ControlNet, process automation (i.e., PROFIBUS, Modbus), ICS (MTConnect, OPC)
Managed by organization	FCC, ITU, CEPT, CITEL	ODVA, Object Management Group (OMG)
Applications	Working in a remote computer	Building automation, substation automation, automatic meter reading, vehicle automation

EtherNet/IP, and I/O. In addition to providing hardware products, Netbiter offers three different services for their customers: remote access, view and control, and manage and analyze. The first two services which support one remote user and one production system to be remotely accessed are free with hardware gateways, but the last one which supports multiple remote users and multiple production systems to be remotely accessed is subscription based. In terms of security, on the client side, Netbiter QuickConnect software creates a secure tunnel to the Netbiter gateway through a mobile or fixed network. The communication between the client and the gateway is encrypted. Optionally, Netbiter also provides a two-step verification method (password log-in and SMS-based verification). Netbiter stores data received from Netbiter gateway to Netbiter Argos data center in the cloud so that these data can be used for different purposes including visualization, forensic, error investigation, and forecasting. Netbiter's monitored data between the gateway and the cloud is encrypted.

Similar to Netbiter communication gateways, Genua offers a hardware box called genubox which is also installed in the production site where the machine (called supervised machine) is located which will be remotely monitored by the service engineer. Locally, a wired connection is established between the genubox and the supervised machine; however, the communication between the genubox and the supervised machine is not encrypted. For the global connection, genubox has both firewall and VPN functionalities, and all of the communication between the service engineer computer (the client) which is located outside the production site (remote site) and the gateway which is located in the production site is encrypted. To protect from repudiation, Genua records all of the activities of the remote maintainer in a video file. In addition, Genua offers a graphical user interface (GUI) for the settings of the remote access, for example, a service personnel is allowed to access a machine remotely on Monday between 10:00 and 12:00 o'clock.

Phoenix Contact offers a platform called mGuard Tele Service for the secure remote maintenance. In the production site, it uses a hardware called mGuard industrial rs to connect to the machine to be monitored/supervised. This hardware has integrated mGuard firewall technology and hardware-based encryption. On the client/service center side, a hardware is used, called mGuard bladepack, which provides both a firewall and VPN gateway. Therefore, all of the communication between the remote site (mGuard bladepack) and industrial site (mGuard industrial rs) is transmitted through an IPsec tunnel. Phoenix Contact has mGuard device manager (mdm) to centrally manage all of the mGuard devices. Siemens offers an industrial modem SCALANCE M which ensures remote access to distant plants with the integrated firewall and VPN security functions [35].

9.4.2.2 Standards for Secure Remote Maintenance Service

In the area of remote maintenance, standardization activities currently haven't progressed very far. Actual activities mainly concentrate on the definition of security recommendations by the German Federal Office for Information Security (BSI). A set of security recommendations for remote maintenance solutions for IT in enterprises [36] and in the production [37] have actually been defined. BSI defined eight basic access rules for remote maintenance for IT in enterprises (three rules for home and small enterprise networks, three rules for big companies and governments, and two rules for security protection means for remote maintenance service providers) [37]. Though these rules are for IT in enterprises, they also generally apply for the production network. For improving the security of remote maintenance for industrial production, BSI defined a set of recommendations categorized into architecture, secure communication, authentication mechanisms, organizational requirements, and miscellaneous [38]. To improve industrial control system (ICS) security, BSI defined possible internal threats and mitigation mechanisms [37], top 10 threats and countermeasures for the years 2012 and 2014 (intrusion via remote access was the fifth threat in 2014 and was the topmost threat in 2012) [39], and two use cases swimming pool [40] and service technician [41]. In the first use case, the remote control interface of the component in the swimming pool (for heating, chlorine mixture, etc.) that was directly connected to the Internet was misused by the attacker. In the second use case, several control centers were infected by a virus that was unintentionally brought by the service technician in his USB stick from his personal computer.

9.4.2.3 Requirements for Secure Remote Maintenance Service for Industry 4.0

Existing solutions are based on well-known operating systems (OSs) such as Linux and Windows. According to [42], Kaspersky is building an industrial operating system (IOS) considering "Security by Design." As results of the Industry 4.0 or similar campaign, many such OSs might be developed in the future considering parameters such as security, performance, host/network size, SDN, virtualization environment, cloud, etc. Therefore, one of the requirements of the Industry 4.0 solution is to be independent of the OS. In addition, existing solutions do not provide any centralized management and control facilities for access rights where the access rules must be deployed on several machines concurrently.

9.4.2.4 Dynamic Firewalls for Secure Remote Maintenance

Dynamic firewalls are the most important component to realize the secure remote maintenance service for industrial networks to protect from both the insider and outsider threats. Typically, considering a real-world industrial network, several firewalls (see Sect. 9.2) have to be applied to effectively shield sensitive passages (both physical and organizational) between different networks and their segments against potentially harmful traffic. Hence, in most cases, gaining access to a certain network port of a specific industrial machine from outside the industrial network (e.g., from the Internet) is typically prevented by a cascade of firewalls. However, such a serial arrangement of shields also complicates a legitimate reach-through from foreign networks to components inside the industrial network. For example, this might be required in scenarios where machine condition information have to be monitored more or less frequently by the machine manufacturer or where software updates have to be uploaded to a production device (hence, in typical remote maintenance scenarios). Manually opening pinholes of every concerned firewall (and closing them again after the legitimate access mission has been completed) would cause unfeasible expenditure. SDN-based dynamic firewalling provides a solution for the automated instant reconfiguration and synchronization of rules for an arbitrary number of firewalls on a data path between defined sinks and sources within a network.

SDN-based dynamic firewalling rests upon an approach first described in the year 2012 in [43] to define and enforce individual-related or role-specific firewall policies. In this approach that emanated from a research project called DynFire funded by the German Federal Ministry of Education and Research, a novel central network entity called firewall manager is introduced. Besides being able to gain and dynamically maintain an overview on the network topology including further security-related network characteristics, the firewall manager administers access policies for every individual (or their functional roles, respectively, such as service technician for device X). In case of an access request from an authenticated individual to a specific network resource (such as a production device connected to an industrial network), by analyzing the network topology, the firewall manager identifies the network intersections that will be passed by the traffic flow caused by the intended access. Subsequently it will update the rules of all concerned firewalls in the network to allow the required data flows to pass. Once the access session involving the data flow has been completed, the firewall manager will again update the firewall rules, now closing the pinholes that had been opened before upon the access request.

9.4.2.5 SDN-Based Remote Maintenance Security Architecture

To achieve secure remote maintenance, as mentioned previously, several rules were defined by the BSI [36]. To go into more detail, for home or small business, the following rules should be considered:

1. Remote maintenance/diagnostics session must be started by the machine operator.
2. The remote maintenance connection must be encrypted.
3. The remote user or technician must be authenticated before accessing the system.

In addition to these rules, the following rules should be considered especially by large enterprises and government offices:

4. At least during the remote maintenance session, the object to be repaired should be isolated from the rest of the networks to avoid any (intentional/unintentional) access to other machines or servers. At least one packet filter should be used for the isolation.
5. Configuration effort for the security gateway should be minimal.
6. The activities of the technician should be logged.

To fulfill these requirements, especially minimizing configuration efforts for the security gateway, the SDN-based security architecture is proposed as shown in Fig. 9.4.

The architecture works are as follows:

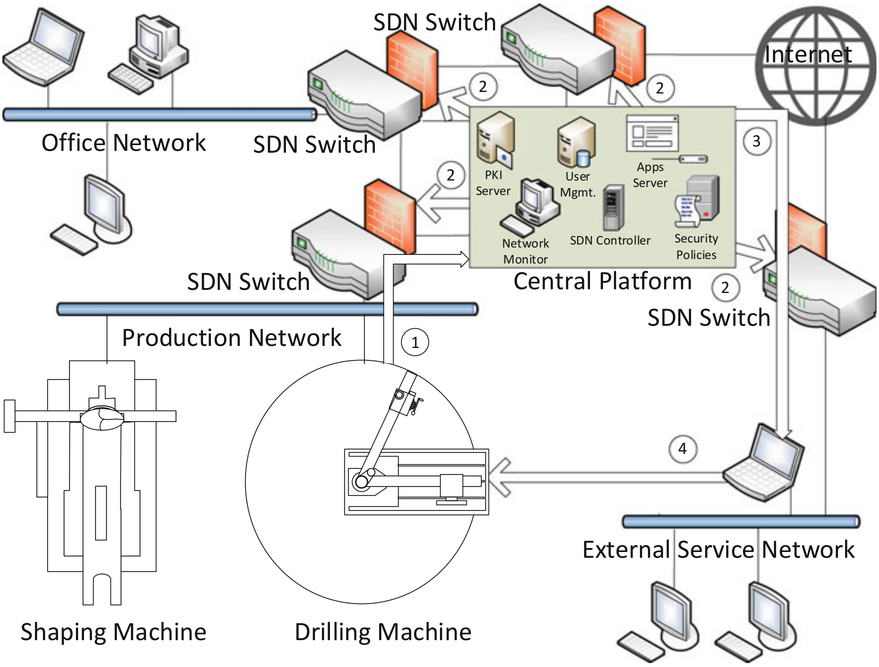

Fig. 9.4 SDN-based remote maintenance security architecture

1. Whenever an event is triggered by the production machine, for example, in a result of some error, one component is detached or a forged component is attached, the production machine sends a message to the central platform (where the SDN controller is located) for an action.
2. The central platform then checks the security and other policies (e.g., responsible person for the maintenance, security assertions, etc.) for this particular event. After selecting the maintenance engineer who is online, the central platform uses the SDN controller to configure all of the SDN switches between the engineer and the production machine conforming security policies. The assumption here is that the laptop/computer is online. If this is not the case, then an e-mail/SMS/IM is sent to the engineer to bring his/her device online.
3. The central platform then configures the engineer's laptop/computer according to the security policies. After that, it signals the engineer to start maintenance.
4. The maintenance engineer has now a connection with the production machine which conforms the security policies.

9.5 Discussion on Relevance of Proposed SDN-Based Security Solutions

In the last sections, we depicted a number of security solution requirements for Industry 4.0 (such as that respective solutions must be able to work independently and allow for dynamic and automatic action). Furthermore, several specific security functionalities were introduced, such as an industrial IDS, secure remote maintenance service, and dynamic firewalls. For each of these functionalities, respective SDN-based implementations were outlined.

In general, the SDN approach with the control layer separated from the application and network layer allows for the designing of powerful network service infrastructures providing an overall view of the whole network. Furthermore, SDN enables the central analysis and instant control of the network traffic on any given link. Hence, SDN does not only provide a basis for the flexible deployment of dynamic high-performance network environments but also introduces a very effective platform for comprehensive IT/cyber security solutions including monitoring/attack detection combined with effective capabilities for attack mitigation (e.g., through filtering or dynamic traffic re-routing).

These advantages of SDN are especially valuable in Industry 4.0 environments, where general network requirements such as high performance and high availability meet security requirements such as automatic threat detection and mitigation. For example, in case of industrial IDS, large amounts of data must be processed in order to securely detect unwanted actions. For this purpose, SDN solutions are useful for filtering and preprocessing the data and mitigating DDoS and further attacks. For a secure remote maintenance access solution, the proposed SDN-based security architecture provides a platform to completely fulfill the given BSI security guidelines.

9.6 Conclusion

In this chapter, we discussed the potential to use SDN as a basis for IT/cyber security solutions for Industry 4.0. Legacy firewalls with their static behavior and the lack of a central network/security policy overview and configurability will no longer be acceptable in modern and industrial networks connecting industrial machines and their components with the Internet. Industry 4.0 needs dynamic, easily configurable, and central policy-based security mechanisms that can be provided by intelligently using/adapting SDN technologies. Toward this, as examples, two security functionalities for Industry 4.0 were discussed in this chapter: an industrial intrusion detection system (IDS) and a secure remote maintenance service. When SDN will be used as a basis technology for Industry 4.0, more security components and services will be created and deployed easily as this will provide an innovation platform for the next industrial evolutions let alone Industry 4.0.

Exercise

1. What is the meaning of the number in "Industry 4.0," and what is the meaning of the preceding numbers 1–3?
2. What are the two general types of protocols to be used in production networks?
3. What are the Industry 4.0 similar initiatives from the USA, Japan, and China?
4. How many layers ONF SDN architecture have, and what are those layers and their functions?
5. Why is security an important aspect for Industry 4.0?
6. Please name some classical Fieldbus and industrial Ethernet protocols.
7. As an add-on to Ethernet/IP protocol, which security mechanism is used?
8. What are the disadvantages of non-SDN-based security solutions?
9. Why is current IDS/IPS not appropriate for Industry 4.0?
10. What are the advantages of remote maintenance compared to local maintenance?
11. Which protocol is used by the VNC software that is defined in RFC 6143? What are the advantages and drawbacks of this protocol?
12. BSI defined eight access rules for remote maintenance. What are those rules?
13. According to BSI top 10 threats and countermeasures document, what was the topmost threat in 2012?
14. Similar to the Table 9.3, please create a firewall rule to disable all connections from the IP address 46.38.224.0/24 to 217.224.0.0/11.

Answer

1. Check 9.1
2. Check 9.2
3. Check 9.1

4. Check 9.1
5. Check 9.1
6. Check 9.2
7. Check 9.2
8. Check 9.2
9. Check 9.4.1
10. Check 9.4.2
11. Check 9.4.2
12. Check 9.4.2
13. Check 9.4.2
14. **Solution:** Protocol: IP, From: 46.38.224.0/24, To: 217.224.0.0/11, Action: Deny

References

1. Zukunftsprojekt Industrie 4.0. https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html. Online; Accessed 18 Nov 2016
2. Hermann M et al (2016) Design principles for industrie 4.0 scenarios. In: 2016 49th Hawaii international conference on system sciences, pp 3928–3937
3. Heilmann D et al (2016) Industrie 4.0 im Internationalen Vergleich. Eine Studie des Handelsblatt Research Institute, pp 1–144
4. Deutsche Bank Research, Taking point industry 4.0: huge potential for value creation waiting to be tapped. Created on 23 May 2014. http://www.dbresearch.com/servlet/reweb2.ReWEB?rwsite=DBR_INTERNET_EN-PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000335628. Accessed 18 Nov 2016
5. IUNO, Nationales Referenzprojekt, IT-Sicherheit in Industrie 4.0. http://www.iuno-projekt.de/ (German national research project, available in German only). Online; Accessed 18 Nov 2016
6. McKeown M, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, Shenker S, Turner J (2008) OpenFlow: enabling innovation in campus networks. SIGCOMM Comput Commun Rev 38(2):69–74
7. ONF (2014) SDN architecture. ONF Technical Report TR-502, Open Networking Foundation, June 2014
8. Khondoker R, Zaalouk A, Marx R, Bayarou K (2014) Feature-based comparison of software defined networking (SDN) controllers. In: ICCSA, pp 1–7
9. Zaalouk A, Khondoker R, Marx R, Bayarou K (2014) OrchSec: an orchestrator-based architecture for enhancing network-security using network monitoring and SDN control functions. In: NOMS, pp 1–9
10. Zaalouk A, Khondoker R, Marx R, Bayarou K (2014) OrchSec demo: demonstrating the capability of an orchestrator-based architecture for network security, academic demo. In: ONS, pp 1–2
11. Khondoker R, Larbig P, Senf D, Bayarou K, Gruschka N (2016) AutoSecSDNSemo: demonstration of automated end-to-end security in software-defined networks, IEEE NetSoft 2016. In: IEEE NetSoft, pp 1–2
12. Batke B, Wiberg J, Dube D (2015) CIP security phase 1, secure transport for EtherNet/IP. In: 2015 ODVA industry conference
13. Davis R, The myth of network address translation as security. White paper, F5. https://f5.com/Portals/1/Cache/Pdfs/2421/the-myth-of-network-address-translation-as-security.pdf. Online; Accessed 02 Dec 2016
14. Higgins KJ (2014) Windows XP Alive & Well in ICS/SCADA networks. Information week darkReading, Oct 2014

15. Poimboeuf J, Jennings S (2014) Introducing kpatch: dynamic kernel patching. Technical report, Red Hat, Feb 2014
16. Pavlík V (2014) kGraft – live patching of the Linux kernel. Technical report, SUSE, Maxfeldstrasse 5 90409 Nuremberg Germany, Mar 2014
17. Sommer R, Vallentin M, De Carli L, Paxson V (2014) HILTI: an abstract execution environment for deep, stateful network traffic analysis. In: Proceedings of the 2014 conference on internet measurement conference. ACM, pp 461–474
18. Sommer R, Amann J, Hall S, Spicy: a unified deep packet inspection framework dissecting all your data. Technical Report TR-15-004, International Computer Science Institute Berkeley, 1947 Center Street, Suite 600, Berkeley, California, 94704, Nov 2015
19. Bosshart P, Daly D, Gibb G, Izzard M, McKeown N, Rexford J, Schlesinger C, Talayco D, Vahdat A, Varghese G et al (2014) P4: programming protocol-independent packet processors. ACM SIGCOMM Comput Commun Rev 44(3):87–95
20. Udd R, Asplund M, Nadjm-Tehrani S, Kazemtabrizi M, Ekstedt M (2016) Exploiting bro for intrusion detection in a SCADA system. In: Proceedings of the 2nd ACM international workshop on cyber-physical system security. ACM, pp 44–51
21. PROFIBUS User Organization, Haid-und-Neu-Str. 7 76131 Karlsruhe Germany. PROFINET design guideline, version 1.04 edition, Nov 2010
22. Debar H, Curry D, Feinstein B (2007) The intrusion detection message exchange format (IDMEF). RFC 4765 (Experimental), Mar 2007
23. Danyliw R, Meijer J, Demchenko Y (2007) The incident object description exchange format. RFC 5070 (Proposed Standard), Dec 2007. Updated by RFC 6685
24. GT/Coursera SDN Course Travelogue – Week 5, https://www.sdnskills.com/learn/gtcoursera-sdn-course-travelogue-week-5/. Online; Accessed 04 Apr 2017
25. Thompson HA (2004) Wireless and internet communications technologies for monitoring and control. Control Eng Pract 12:781–791
26. Distributed Aircraft Maintenance Environment from 2002, http://www.cs.york.ac.uk/dame. Online; Accessed 03 Mar 2016
27. SCADA.web, https://www.scada-web.net/default.aspx. Online; Accessed 03 Mar 2016
28. Wohlwend H, e-Diagnostics guidebook: revision 2.1. http://www.sematech.org/docubase/document/4153deng.pdf. Online; Accessed 03 Mar 2016
29. Richardson T, Levine JR (2011) The remote framebuffer protocol. RFC 6143, Mar 2011. https://rfc-editor.org/rfc/rfc6143.txt
30. Comparison of remote desktop software, https://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software. Online; Accessed 03 Mar 2016
31. Teradici PCoIP (PC over IP) solution, http://www.teradici.com/products-and-solutions/pcoip-products/remote-workstation-card. Online; Accessed 03 Mar 2016
32. Netbiter remote management, http://www.netbiter.com/. Online; Accessed 03 Mar 2016
33. Genua genubox, https://www.genua.de/loesungen/fernwartungs-appliance-genubox.html. Online; Accessed 03 Mar 2016
34. Remote Services Security / Secure Remote Maintenance, http://www.phoenixcontact-cybersecurity.com/en/solutions/remote-services-security. Online; Accessed 03 Mar 2016
35. Siemens Industrial Network Security, http://www.industry.siemens.com/topics/global/en/industrial-security/network-security/Pages/Default.aspx. Online; Accessed 03 Mar 2016
36. Recommendation: IT in the Company. BSI publications on cyber security. Basic rules for protecting remote maintenance accesses. BSI Recommendation, June 2013. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_054E.pdf?__blob=publicationFile&v=4
37. Recommendation: IT in Production. Industrial Control System Security. Inside threat. BSI Recommendation, May 2013. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_061E.pdf?__blob=publicationFile&v=2. Online; Accessed 04 June 2016
38. BSI Empfehlung: in der Produktion, Fernwartung im industriellen Umfeld. BSI Recommendation, Jan 2015. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108.pdf?__blob=publicationFile&v=3 [available in German only]. Online; Accessed 04 June 2016

39. BSI recommendation: IT in production, industrial control system security, top 10 threats and countermeasures 2014. BSI recommendation, May 2016. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf?__blob=publicationFile&v=2. Online; Accessed 04 June 2016
40. BSI Empfehlung: IT in der Produktion, Fallbeispiel Schwimmbad. BSI Recommendation, Feb 2014. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_095a.pdf?__blob=publicationFile&v=3 (available in German only). Online; Accessed 04 June 2016
41. BSI Empfehlung: IT in der Produktion, Fallbeispiel Servicetechniker. BSI Recommendation, Mar 2014. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_095c.pdf?__blob=publicationFile&v=2 (available in German only). Online; Accessed 04 June 2016
42. Bruner J (2013) Industrial internet the machines are talking, 1st edn. O'Reilly Media, Sebastopol
43. Marx R, Kuntze N, Rudolph C, Bente I, Vieweg J (2012) Trusted service access with dynamic security infrastructure configuration. In: 18th Asia-Pacific conference on communications (APCC). IEEE, 2012

Rahamatullah Khondoker is with Fraunhofer SIT and TU Darmstadt since January 2013. Before that, he worked in TU Kaiserslautern from where he completed Dr.-Ing. in computer science on the topic "Description and Selection of Communication Services for Service Oriented Network Architectures" after completing M.Sc. in computer science from the University of Bremen. He was selected as a top ten researcher in 2015 by the academics.de. In addition, he was awarded from Ericsson in the year 2008 and from the FIA Research Roadmap group in October 2011. On 8 July 2015, he completed "University Teaching Certificate" from TU Darmstadt. He worked with the DFG project (PoSSuM), BMBF projects (G-Lab, G-Lab Deep, FutureIN, IUNO), EU projects (PROMISE, EuroNF, PRUNO), and several industry projects. Currently, his focus is on the security of Future Internet Architectures including SDN, NFV, 5G, IoT, and Industry 4.0.

Pedro Larbig studied computer science at the Technical University of Darmstadt and was hired as a research assistant by the Center for Advanced Security Research Darmstadt (CASED) where he developed tools for testing security properties of wireless routing protocols. As a long-term developer of software in C for network encryption and authentication protocols, he gained a deep practical understanding of these mechanisms. Joining Fraunhofer SIT in 2011, he now works on designing and implementing new cryptographic systems and analyzing the flaws of existing ones. While he implements cryptographic authentication algorithms, a strong focus is put on managing secrets securely. He gained intensive knowledge about how attackers can use or abuse protocols to leak information and how they gain control over remote systems or networks, broadening the spectrum to an adversary's perspective.

Dirk Scheuermann completed his diploma in mathematics at Technical University Darmstadt in 1994 and his Ph.D. at Justus-Liebig University Giessen in 1998. Both his diploma thesis and his Ph.D. thesis were done in cooperation with Fraunhofer SIT and dealt with cryptography. Since 1998, Dirk Scheuermann is working as a researcher at Fraunhofer SIT. His major interests are cryptography, smart card technology, data formats, protocols, and anomaly detection. In the last years, he worked in several EU projects (e.g., EVITA) and BMBF projects (ESUKOM, ANSII) in these areas. Actually, he is strongly involved into the IUNO project with the major task of designing cryptography-based piracy protection concepts for Industry 4.0.

Frank Weber is the deputy head of the Mobile Systems and Mobile Networks Department at Fraunhofer SIT. He holds a diploma with a focus on computer engineering and a Ph.D. in network technologies. Before joining Fraunhofer SIT in 2013, from 2003, he has contributed to a number of both public- and company-funded R&D projects in the fields of network technologies and real-time communications, first as a member of the Research Group for Telecommunication Networks at Frankfurt University of Applied Sciences, Germany, and from 2009 as a freelancing engineer.

From 2006 to 2012, he has been an associated member of a research cooperation team of the Centre for Security, Communications and Network Research (CSCAN) at Plymouth University, UK. His current research focus is on various security aspects of upcoming and future network architectures, such as SDN and 5G, and their applications, such as real-time communications and Industry 4.0.

Kpatcha Bayarou received his diploma in electrical engineering/automation engineering in 1989, a diploma in computer science in 1997, and his doctoral degree in computer science in 2001, all from the University of Bremen in Germany. He joined the Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT) in 2001. He is the head of the Mobile Systems and Mobile Networks Department that focuses on cyber-physical systems and future Internet including vehicular communication. In addition, he managed several EU and nationally funded projects and published several conference papers related to security engineering of mobile communication systems, mobile network technology, NGN (next-generation networks), and future network technologies like SDN/NFV and 5G.