Gesellschaft für Informatik e.V. (GI) GI. (Hrsg.): INFORMATIK 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 1781

Secure Unidirectional Security Gateways for Industrie 4.0

Christele Larissa Moussi Djeukoua[1] Timothee Guiraud[2] Edita Bajramovic[3] Josef Schindler[4] Karl Waedt[5]

Abstract: Secure data exchange between different geographical sites (e.g. industrial manufacturing facilities, power plants, research labs, and manufacturer test facilities) is an important part of cybersecurity. It is for example addressed by section 13 "Communications Security" of ISO/IEC 27002:2013. ISO/IEC 27033-4:2014 gives guidance for securing communications between networks using security gateways (firewall, application firewall, Intrusion Protection System, etc.). While the newest part of the multipart ISO/IEC 27033 standards series, ISO/IEC WD 27033-7 "Information technology Network security Part 7: Guidelines for network virtualization security" is more on the abstraction of physical components involved in communication, this paper aims to emphasize the fiber optical network communication-based security between very specific Cyber-Physical Systems (CPS). In this case, secure means a strictly reduced feedback channel.According to ISO/IEC 27033-4, essentially, the approaches described in this paper would be classified as physically unidirectional security gateways. In this paper, requirements and concepts will be presented which are beneficial for a scalable use in Industry 4.0 applications for highest (hardware-enforced) unidirectional communication and which can coexist with Firewall and Demilitarized Zone (DMZ) approaches that are also needed for complex IACS architectures.

Keywords: Security Gateway; Fiber Optical Network; Secure Communication; Forensic Readiness; Industrial Automation; Control System

1 Introduction

Mentioned for the first time in 2011 at the Hanover Fair, the term Industrie 4.0 (fourth industrial revolution) was created by the German government to promote connected production and digital convergence between industry, businesses, and other processes. It is a collective term for the technologies and concepts of a value chain organization that creates together Cyber-Physical Systems (CPS) and the Internet of Things (IoT) [HPO16, IE20a].

[1] Friedrich-Alexander-University (FAU) Erlangen-Nuremberg, IT Security Infrastructures Lab, Martensstrasse 3, 91058, Erlangen, Germany larissadjeukoua@yahoo.fr

[2] Framatome GmbH, ICETA-G Department, Paul-Gossen-Straße 100, 91052, Erlangen Germany timothee.guiraud@protonmail.com

[3] University of Erlangen-Nürnberg, IT Security Infrastructures Lab, Martensstrasse 3, 91058 Erlangen, Germany edita.bajramovic@fau.de

[4] Friedrich-Alexander-University (FAU) Erlangen-Nuremberg, Chair of Electrical Energy Systems (EES), Cauerstraße 4, 91058, Erlangen, Germany josef.s.schindler@fau.de

[5] Framatome GmbH, ICETA-G Department, Paul-Gossen-Straße 100, 91052, Erlangen, Germany karl.waedt@framatome.com

IoT belongs to one of the most dynamic and exciting areas of ICT (Information and Communication Technologies). Aiming to connect physical entities to computer systems through networks, IoT uses electronic components that interact with the physical world as building blocks. It bases on sensors and actuators of any type, such as thermometers, accelerometers, video cameras, microphones, relays, or industrial equipment for manufacturing or process-controlling. While actuators will act on physical entities, sensors will collect information about the physical world. For controlling physical entities, provision of contextual, real-time, and predictive information is necessary that impacts both physical and virtual entities. Therefore, mobile technology, cloud computing, big data, and deep analytics (predictive, cognitive, real-time, and contextual) play an important role in collecting and processing data to achieve business objectives [IE18, IE20b].

2 Problem statement

The digitalization of manufacturing introduces danger to the integration of IT and critical infrastructures, which could affect the industrial manufacturing process (malware, spyware, loss of data integrity, or problems with the availability of information). With increased interconnectivity and potential impact on functional or nuclear safety, Cyber-physical Systems (CPS) and related Industrial IoT (IIoT) gradually become more sensitive targets of cybersecurity attacks [TSS17]. To effectively detect such attacks with minimum delay, forensic readiness and means for fast evaluation of related events are mandatory. Forensic readiness intends to maximize an environment's ability to collect credible digital evidence on the one side and to minimize the cost of forensics in incident response on the other [BSJ10].

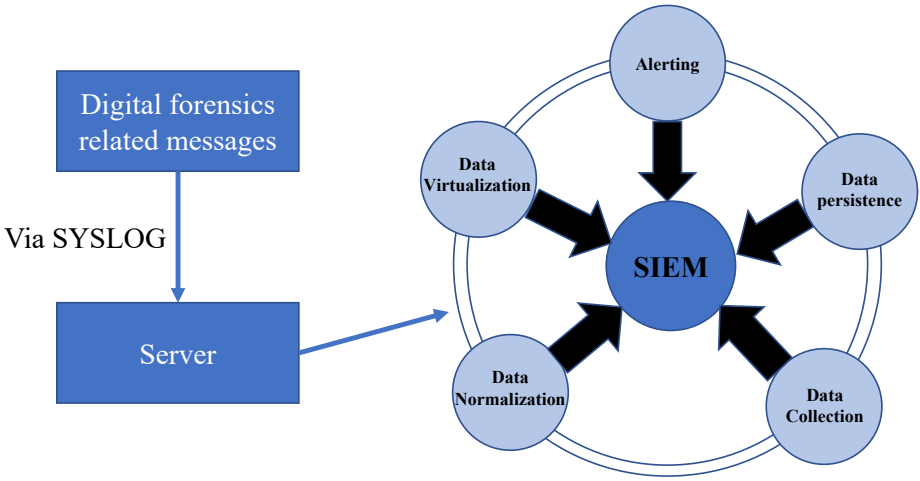

Fig. 1: Current IT-solutions for detecting cybersecurity attacks

In the global economy, there is a new kind of software criminality that can cause data availability and reliability problems for companies. Current commercial solutions are not suited for jointly meeting the specific safety and cybersecurity requirements [ET20]. As a common practice in the IT domain, digital forensics readiness-related messages can be sent via SYSLOG towards a server that processes them into a Security Information and Event Management (SIEM) system. This idea is presented in figure 1 [FS07]. This paper discusses how to design and deploy secure unidirectional gateways to minimize potential threats and unexpected situations. In this context, the following Research Questions (RQ) arise:

- What is important from the security side according to the requirements of the implementation of Industry 4.0 by using unidirectional secure gateways?
- What high-reliability real-time behavior can be assured despite unidirectional communication?

This paper aims to present a solution to these research questions.

3 Secure unidirectional gateways: data diode

The International Electrotechnical Commission proposes new standards for power plants and critical infrastructure [IE19b, IE19a, IE20a]. As requested by those standards with joint requirements on safety and security, there shall be no retroaction from a SIEM system (or security monitoring system in general) to the safety automation systems, IIoT, and thus to the cyber-physical systems (CPS) [IE19b, IE19a]. The gateways replace firewalls in some industrial network environments, providing absolute protection to control systems and Operational Technology (OT) networks for attacks originating in external networks. Accordingly, the data related to forensic readiness (e.g. from gateways and service units) has to be sent via data diodes towards a SIEM system, like described in figure 2.

3.1 Definition

An Optical Data Diode is an analogy to the electronic diode that permits current flow in one direction only. It is a method to execute a unidirectional data transfer between two computers. Usually, a sender of a unidirectional connection will transmit data only if the transmission is acknowledged at the physical layer (ISO/OSI Layer 1) and the transport layer (ISO/OSI Layer 4). The data diode assures that data is transmitted despite not having any acknowledgment mechanism. In the case of an optical fiber solution, there is no fiber optic link between the transmit port of the transceiver on the receiving side of the data diode and the receiving port of the transceiver on the transmitting side of the data diode. Visual inspection of the transceivers should easily show that they have not been tampered or replaced with a component that can both transmit and receive [Ba16].

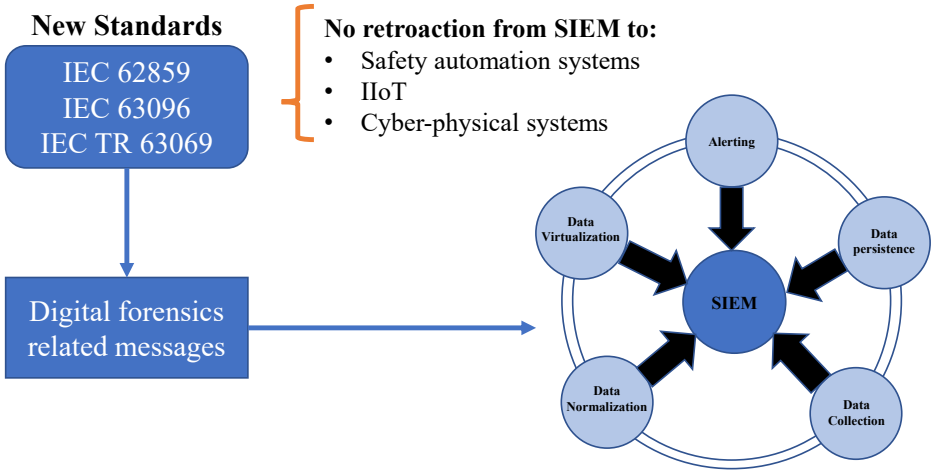

Fig. 2: Solutions for power plants and critical infrastructure with joint requirements on safety and security

3.2 Advantages of a data diode

Data diodes play an important role in the comprehensive protection of networked control systems. High-security, one-way data communication at sensitive interfaces enables the transfer of information to a maintenance service without the system being exposed to cyber risks. This section uses protection principles to illustrate the benefits of using data diodes for Industrie 4.0 [Ba16].

- **Integrity**: The entire data flows to the receiver together with strong cryptographic hash values. That assures the verification of data integrity by the receiver.
- **Availability and Reliability**: The transferred data is almost simultaneously accessible on both systems. The transmission works even if individual telegrams fail.
- **Confidentiality**: Optional data is encrypted if sensitive. Unauthorized individuals have no access to confidential data. Additionally, the latter has protection against any malicious attacks (e.g. intrusion or hacking). The hardware structure is not complex. This factor is only relevant if the data is not 'short-lived'.
- **High volume and real-time**: High volume data transmission is possible in real-time with configurable cycles.
- **Flexibility**: Different numbers of transmitters and receivers.
- **Portability**: Optical Data Diodes can be applied with different operating systems, such as Windows or Linux.

- **Transmission**: On ISO/OSI levels 4 (UDP) and 2 (LLC)
- **End-to-end logging**: On sender-side for forensic readiness and for offline evaluation of logs to detect manipulations
- **Forensics**: Ability to smartly compare logs from redundant receivers (one receiver does not need to know who the other receivers are)

3.3 Application fields of data diodes

To guarantee information security or protection of critical digital systems, such as Industrial Automation and Control Systems (IACS), from cyber attacks, unidirectional network devices are typically used [IE19b]. In many industrial application unidirectional data flow is sufficient, e.g. for monitoring the health of equipment that is susceptible to ageing, e.g. the shafts of steam turbines, or the concentration of chemical solutions used in different industrial applications, especially with slow gradients. For security applications secure unidirectional communication is also a major benefit, e.g. for the transfer of logging information towards a Security Information and Event Management (SIEM) system. Other fields where data diodes are in using are: IT bridge - Sending/receiving emails from open to critical/confidential networks - Secure cloud connectivity of critical OT networks - Database replication - Data mining - Trusted back-end and hybrid cloud hosted solutions (private / public) - Secure data exchange for data marketplaces - Secure credential/ certificate provisioning - Secure cross-data base sharing - Secure printing from a less secure network to a high secure network (reducing print costs) - Transferring application and operating system updates from a less secure network to a high secure network - Time synchronization in highly secure networks - File transfer - Streaming video - Sending/receiving alerts or alarms from open to critical/confidential networks - Government - Commercial companies [Wik21].

For these applications there are some commercial solutions available on the market. However, these are targeting selective unidirectional transmission lines via a set of protocols that are in principle designed to be bidirectional, e.g. file sharing via TCP/IP. In order to be transparent towards the user applications these solutions mimic the acknowledgements at the network communication layer, while making use of dedicated hardware and servers (for protocol conversion/acknowledgement mimicking) at both sides of the unidirectional communication. This dedicated hardware typically certified according to a high Evaluation Assurance Level (EAL), with additionally increases the equipment cost.

A transport protocol is necessary so that the data can be transferred from one computer to another. A distinction is made between TCP, UDP or LLC. The UDP standard allows the fast transport of data packets and to track the order of transmission of information. In contrast, TCP establishes a connection to the end host, where the data transmission excludes the mixing of information, your loss, delay [TW09]. LLC is a bit like TCP and UDP, except that it runs on simple Ethernet and is limited to the maximum datagram length at the ISO/OSI layer 2. This type LLC1 has no confirmation and basically sends unconfirmed data to a

receiver, making it very similar to UDP. LLC2 is a variant where connections are made and properly received packet data is acknowledged. So this is more like TCP - except for many fine-grained protocols for dynamically changing networks, so there are no flags or windows or other complexities that make TCP suitable for long-distance traffic. Since data must be sent unidirectionally, the UDP protocol is suitable. The User Datagram Protocol (UDP) is a connectionless high-level communication protocol. It offers better real-time characteristics than TCP, because in contrast to TCP it employs no transparent retransmission or error correction mechanisms which checks for every packet whether it has arrived in1 cluding proper sequence of packets. Nevertheless it can be guaranteed, that no packets are lost in local networks, provided point-to-point topology is in use [EFS17].

Currently data diodes for different application scenarios are prototypically implemented with a focus on reliability for different use cases and forensic readiness. By the integration as a thin layer on existing automation hardware for example, use cases with multiple receivers can be considered: data is transferred unidirectionally from one sender to various receivers that are located in diverse zones. It is also possible to regulate which data has to flow towards which receiver (see figure 3). There are also use cases with given unreliability assumptions regarding the transmission lines, real-time requirements, provisions against spoofing and user interface considerations (e.g. regarding SIEM supported log evaluations and incident handling). To ensure the effectiveness of these application scenarios, practical results shall be provided based on different prototype implementations, including the consideration of high data volumes and transmission performance.

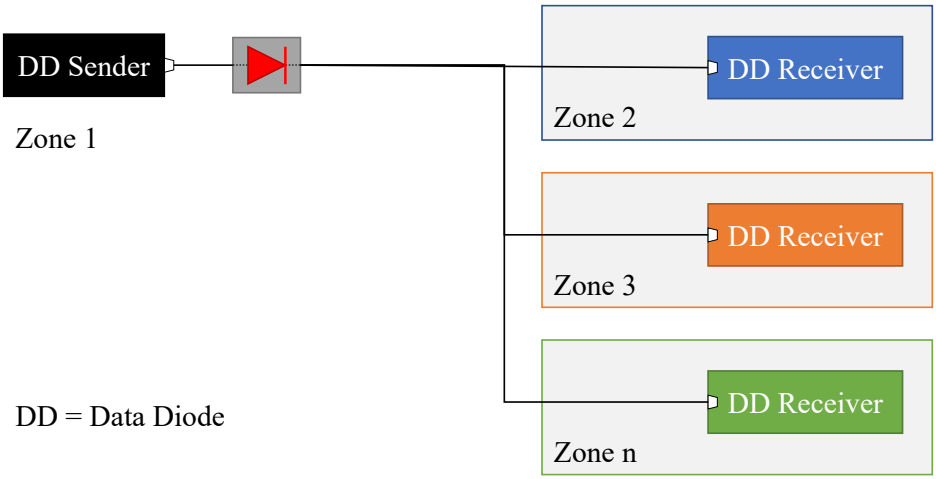

Fig. 3: Data transfer from one sender to various receivers

4 Conclusion

The aim of the paper was to conduct research in the importance of secure unidirectional Security Gateways for Industrie 4.0. The section 2 of this paper showed that the explosion of interconnectivity creates a new potential danger, what can have an impact on all the processes of a company. The fact of the need for increased data volumes and availability in real time requires new infrastructures and adaptations to the handling of information. It can be expected that current commercial solutions are not able to guarantee both specific security and cyber security requirements or to reduce the risks of cyber-attacks, such as the loss of data integrity, data availability etc. According to the on the figure 2 related standards for power plants and critical infrastructure, computer systems should be typically airgapped with data diodes to assure that no information can physically flow back . The results of in this paper presented analysis show that the usage of unidirectional gateways (data diodes) can reduce common security risk factors in the manufacturing area.

Optical Data Diodes are applicable in many different ways, depending on how data need to be transferred. There can be either applied with two computers only or with numerous ones at the same time. As messages cannot be acknowledged, each message has to be sent multiple times (with appropriate identifiers, hash values and optionally encryption). It shall be assumed that any single message can be lost (when sending via UDP or LLC) but at least one of the duplicates is not lost with sufficiently high reliability.

References

[Ba16] Bartels et al., K.: Handreichung zum 'Stand der Technik im Sinne des IT-Sichergeitsgesetzes (ITSiG)'. Technical report, TeleTrusT – Bundesverband IT-Sicherheit e.V., Berlin, DE, 2016.

[BSJ10] Barske, D.; Stander, A.; Jordaan, J.: A Digital Forensic Readiness framework for South African SME's. In: 2010 Information Security for South Africa. pp. 1–6, 2010.

[EFS17] Eggert, L.; Fairhurst, G.; Shepherd, G.: UDP Usage Guidelines (RFC8085). Standard, Internet Engineering Task Force (IETF), 03 2017.

[ET20] ETSI: Cyber Security for Consumer Internet of Things: Baseline Requirements (ETSI EN 303 645:2020). Standard, European Telecommunications Standards Institute (ETSI), Valbonne, FR, 06 2020.

[FS07] Freiling, Felix C.; Schwittay, Bastian: A Common Process Model for Incident Response and Computer Forensics. In: 2010 Information Security for South Africa. pp. 19–40, 2007.

[HPO16] Hermann, Mario; Pentek, Tobias; Otto, Boris: Design Principles for Industrie 4.0 Scenarios. In: 2016 49th Hawaii International Conference on System Sciences (HICSS). pp. 3928–3937, 2016.

[IE18] IEC: Internet of things (IoT) – Reference Architecture (ISO/IEC 30141:2018). Standard, International Electrotechnical Commission (IEC), Geneva, CH, 08 2018.

[IE19a] IEC: Industrial-process measurement, control and automation - Framework for functional safety and security (IEC TR 63069:2019). Standard, International Electrotechnical Commission (IEC), Geneva, CH, 05 2019.

[IE19b] IEC: Instrumentation and control systems - Requirements for coordinating safety and cybersecurity (IEC 62859:2016+AMD1:2019 NPPs). Standard, International Electrotechnical Commission (IEC), Geneva, CH, 10 2019.

[IE20a] IEC: I&C and EPS – Security controls - Version 4 (IEC 63096:2020 NPPs). Standard, International Electrotechnical Commission (IEC), Geneva, CH, 10 2020.

[IE20b] IEC: Internet of things (IoT) – Industrial IoT (PD ISO/IEC TR 30166:2020). Standard, International Electrotechnical Commission (IEC), Geneva, CH, 05 2020.

[TSS17] Tupa, Jiri; Simota, Jan; Steiner, Frantisek: Aspects of Risk Management Implementation for Industry 4.0. Procedia Manufacturing, 11:1223–1230, 2017. 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27-30 June 2017, Modena, Italy.

[TW09] Trick, U.; Weber, F.: IP, TCP/IP und Telekommunikationsnetze: Anforderungen - Protokolle - Architekturen. Oldenbourg Verlag, Munich, DE, 2009.

[Wik21] Unidirectional network. https://en.wikipedia.org/wiki/Unidirectional_network, Online; Accessed: 2021-06-04.