Proceedings
3rd GI/ACM Workshop

Standardisation on Industry 4.0 Automation and Control Systems

Edited by

Jan de Meer
Joachim Hof
Axel Rennoch
Karl Waedt

24th September 2018
Berlin, Germany

Online version

http://nbn-resolving.de/urn:nbn:de:0011-n-5185555

urn:nbn:de: 0011-n-5185555

Contacts

Mr. Axel Rennoch
Fraunhofer Institute for Open Communication Systems FOKUS
email: axel.rennoch@fokus.fraunhofer.de

Mr. Jan de Meer
smartspacelab.eu GmbH
email: demeer@acm.org

Technical Program

of the 3rd GI/ACM Workshop

on ‚Standardization of Industry 4.0 Automation and Control Systems' 24. September 2018,

at ‚Smart Data Forum' @ FhG Heinrich-Hertz-Institute, Berlin

Workshop Objectives:

- I4.0 Cyber Defense Strategies
  i.e. Industrial Consortia, Forum International de la Cyber Securite (FIC) & ANSSI & BSI, DKE etc.

- I4.0 Best Practices of Trustworthiness, Security, Privacy, Safety
  i.e. Organizational Approaches on Operational Security Management (OSM), IoT, Smart City, Sensor Networks, Smart Metering, SIEM etc.

- I4.0 Standards & IT Laws & EU Regulations
  i.e. IT Laws, Regulations, Standards of EU and its member states, i.e. TTIP, CETA, DIN/DKE, IEC 62443 IACS, VDE 0199 MMI, IEEE 1671 ATML, ITU-T F.748 IoT, ETSI ISG ISI etc.

Workshop Co-Chairs:

demeer@ACM.ORG (**Jan deMeer**, WS General Chair)
karl.waedt@framatome.com (**Karl Waedt**, WS Co-Chair)
axel.rennoch@fokus.fraunhofer.de (**Axel Rennoch**,WS Co-Chair)
hof@insi.science (**Hans-Joachim Hof**, WS Co-Chair)

Workshop Sponsors and Supporters:

Gesellschaft für Informatik GI,
German Chapter of the ACM,
Fraunhofer Institute for Open Communication Systems (FOKUS).

Workshop Technical Program:

İncludes but is not limited to the following issues:

- Formalized Test Purposes
- Application Interfaces in OPC-UA
- Security Gaps in I4.0
- Digitizing impact to the I4.0 World of Work
- Potential of Change of Blockchain Technology
- Hardware Virtualization Technology
- Secure Interoperability
- Challenges of the Triad ‚Security, Safety and Availability' in the I4.0 World

Workshop Speakers:

1. *Andre Wardaschka DEKRA Exam GmbH Bochum et al:*
   ‚Formalized Test Purposes for an Industrial Security Profile';

2. *Tobias Wolff FhG IPK Berlin et al:*
   ‚Test Services for Interoperable and secure shop-floor IT Application Interfaces in OPC-UA;

3. *Venesa Watson University of Siegen, Faculty of Science and Engineering et al*:
   ‚Time-sensitive Ethernet Technology for next Generation CPS/I4.0';

4. *Asmaa Telabi University of Siegen, Faculty of Science and Engineering et al:*
   ‚Secure Interoperability of I&C and IT Systems';

5. *Steffan Tönnissen University of Osnabrück, Wirtschaftsinformatik et al*:
   ‚Welches Veränderungspotenzial weist die Blockchain Technologie für die Branche Logistik auf?';

6. *Asmaa Tellabi University of Siegen, Faculty of Science and Engineering et al:*
   , Security Aspects of Hardware Virtualization Technologies for Industrial Automation and Control Systems';

7. *Michael Köpferl Giesecke+Devrient GmbH Security München et al*:
   ‚Security, Safety and Availability Triad in a Real-world Industrial Environment and Resulting Challenges';

8. *Venesa Watson Framatom GmbH Erlangen et al*:
   ‚Addressing Security Gaps in Industries seeking to adopt I4.0;

Formalized Test Purposes for an Industrial Security Profile

Axel Rennoch[1], André Wardaschka[2] and Sascha Hackel[1]

Abstract: Quality assurance becomes an emerging aspect due to interoperability and security issues in a growing network of IoT devices and systems regarding the future digitalized community. In this contribution, we present working activities to provide a common understanding for testing fundamental security requirements from the industry. In particular, first results are explained and discussed around the widespread standard IEC 62443 [IE01]. In our approach the standardized notation TDL-TO [ET01] for the definition of test purposes has been applied to support a unified presentation and semantics.

Keywords: IoT, Testing, Security, TDL, TTCN-3, Standardization.

1 Introduction

The estimated flood of IoT devices in the upcoming years need to be secured to avoid critical incidents that may lead economic or even worse to personal damage. Today, many examples for IoT security requirements can be found, e.g. [DK01][GM01]. The appropriate tests, that describes how to ensure the requirements, are mostly their business case or simply do not exist. Unfortunately, this situation leaves a patchwork delays the development of a general standard in this field. Consequently, there is a need for a catalogue of test definitions that address a generic minimum security level for IoT. This paper presents such a catalogue that describes formal test purposes in a systematic manner.

2 Application of IEC 62443-4-2 security requirements for IoT

Currently, multiple standardization bodies are working in parallel on reference architectures, terminologies and requirements for IoT. In addition, a couple of IoT-Security related recommendations and guidelines have been issued on national and European level. The root cause for the sudden push may be found in the appearance of the Mirai botnet and other security-related incidents as they demonstrated that weak IoT-Security impacts not only single IoT devices but even complete networks far beyond IoT.

Every single activity has been started for a very good reason and first results have already been published. Nonetheless, they appear to be a problem for vendors and consumers for the following reasons:

[1] Fraunhofer FOKUS, SQC, Kaiserin-Augusta-Allee 31, 10589 Berlin, axel.rennoch@fokus.fraunhofer.de, sascha.hackel@fokus.fraunhofer.de
[2] DEKRA Exam GmbH, Dinnendahlstr. 9, 44809 Bochum, andre.wardaschka@dekra.com

- Recommendations and guidelines are not binding
- National standards mean additional effort for international operating vendors
- International IoT standards are not available now and probable not for years
- Most IoT standardization activities focus on functional Security only

Recommendations and guidelines are typically meant to support vendors in implementing IoT security. There is no way for consumers to compare products that have been implemented according the same recommendation or guideline. This is because the requirements are not binding. It is up to the vendor to select the parts he considers important. Furthermore, these documents are not often maintained and risk becoming outdated over the time (in difference to formal standards).

National standards typically differ from country to country if not derived from the same high-level international standard. In the worst case, they contain not only complementing but also conflicting requirements. Companies that intend to sell their products in different countries would therefore have to adapt the product according to national specifics. This results in nation specific products meaning additional effort and costs for vendors and consumers.

Standardization takes time. Standards are not done on the fly but often take years until publication. This is not because of lack of ideas. Every security expert is able to come up with a set of important requirements. The challenge is to have all stakeholders contributing from the very first beginning to cover all relevant aspects and to gain a wide acceptance at the end. The stakeholders are typically coming from different areas: standardization, certification, testing, consulting, tooling, vendors and consumers – all with different interests and priorities that need to be balanced. Furthermore, standardization is typically not the only task for domain experts. Therefore, the duration that is needed to finalize a standard by far exceeds the effort.

Last but not least, current IoT standardization activities focus primarily on functional security requirements. The secure development process is not quite often considered as mandatory.

The international standard series IEC 62443 seems to solve all these issues. It was originally targeted to serve the different needs of asset owners, service providers and vendors in the area of security for industrial automation and control systems. Due to its generic nature, it appears that this standard is also applied to other areas beyond automation and control systems. After a decade, most parts have reached the approved or final draft status and are ready to be used. In addition to functional requirements on system and component level, it provides also process related requirements for a secure development lifecycle. These development process requirements ensure that necessary product updates are always done with the same quality.

The standard IEC 62443-4-2 defines *technical* security requirements for components in industrial automation and control systems. It is applicable for products used in domains

such as production and the area of critical infrastructure. Each requirement is mapped to at least one of four security level, where level four is the most demanding one. As the requirements are neither bound to specific environments, architectures nor technologies they may also be applied to other domains as well. Relevant requirements may be selected by defining a domain-specific subset. The subset is realized by so called profiles which are an integral part of IEC 62443. Therefore, the functional IEC 62443 product requirements may also be applied to IoT products by defining an IoT specific profile for IEC 62443-4-2. The benefit of this solution is the readymade set of functional requirements as a foundation. It is about the right selection of a subset of requirements to be applied to IoT rather than re-inventing the wheel by defining yet another set of security requirements only for IoT. The task would even more extensive, as IoT itself already covers a wide range of vertical domains from consumer to industrial IoT devices each having different security demands. This kind of multiplication is prevented by the usage of the same foundation (IEC 62443) and the definition of domain specific profiles.

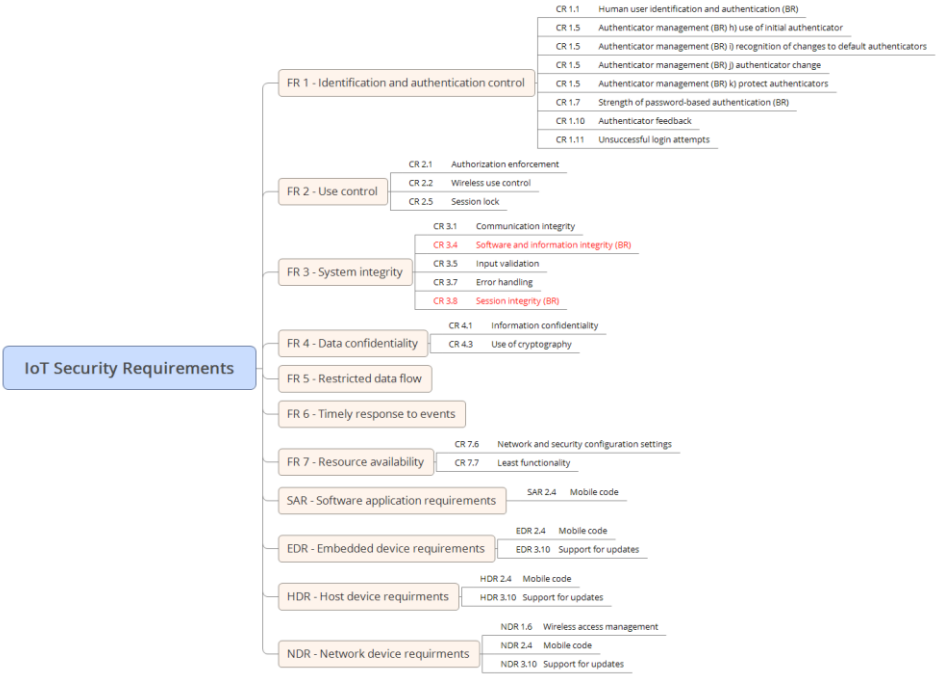

Fig. 1: Initial basic IoT security profile proposal, based on IEC62443-4-2 [IE01]

As a starting point, a minimum level of security has been defined specifying a generic IEC 62443-4-2 based IoT-profile. This basic IoT profile is meant to define an entry security level in especially for consumer IoT but to be fulfilled by any IoT device. It may be superseded by other profiles in case a higher security level is demanded e.g. in an industrial

environment. The basic IoT profile started with requirements that are marked by the standard for the lowest security level, that is security level 1 (SL1). The basic IoT profile then excluded especially those requirements, which were meant for integration into a network management system or not feasible due to IoT typical limitations. This is why e.g. requirements related to auditing, centralized management, secure boot and DoS- or malicious code protection have been excluded from the initial proposal (see Fig. 2). These basic IoT requirements have been subject for formal test descriptions as detailed in the following chapters.

3 Test Descriptions

Since multiple decades, it is one of the best practice for test engineers, introducing an activity during the test development process that produces some documentation about the target test objectives. At ETSI, the output of this step is the so-called "Test Suite Structure and Test Purposes (TSS & TP)" document [ET06].

In industry and standardization, you may find multiple notations and design templates for the definition of test purposes. The contents differ due to the scope of aspects but also on the degree of details. Since it is the intention to provide our results and documents, also for certification or labelling purposes, we decided to apply a more detailed description including structure and styles already developed by, and used in, standardization bodies. Therefore, two techniques appear suitable, the UML-based notation (UTP) from the OMG [OM01] and the TDL-based approach from ETSI [ET01].

Especially in the context of non-functional testing and due to its simplicity, we followed the test development approaches from ETSI and its Test Description Language TDL. In particular, we apply TDL-TO, i.e. the part 4 of TDL, that is dedicated for the test objective definitions. The predecessor of this notation has been known as TPLan in the past [ET04]. Today TDL-TO is used in several technical committees at ETSI, e.g. for the Intelligent Transport Systems [ET05].

4 TP Sample

In the following, we explain the initial work on selected security test purposes covering requirements from the proposed industrial profile presented before.[3] The current version of the TDL-TO package addresses around 20 test purpose definitions. Each contains a unique TP identifier, a prose text for the test objective and a section for references to the original requirements. Furthermore, the TDL-TO language elements used are the structured test objective (consist of initial condition, expected behaviour, final condition)

[3] This work is part of an ETSI TC MTS project [ET03] and in progress.

with an optional PICS selection reference, event sequences, time conditions (label and constraint), as well as declaration of entities, related activities, and data (types and values).

For example, figure 2 presents a session lock test purpose that addresses the security requirement for closing an inactive session after a specified time duration. The formalized model for this test objective includes “Initial conditions”, i.e. test preamble, and the “Expected behaviour” that is divided into a trigger by the tester or evaluator at time label “t1” (line 186) and the expected reaction from the implementation under test (IUT) after a defined duration (line 191), including closing the communication session as well as some related indication for the user. The “then” branch (line 190) here represents the test criterion for a successful test run.

```
165    Test Purpose {
166        TP Id TP_63_1_Session_Lock
167
168        Test objective
169            "Ensure the IUT provides the capability to prevent further access by initiating
170             a session lock after a configurable time period of inactivity."
171
172        Reference
173            "IEC 62443 CR 2.5, section 6.7.1a(i)"
174
175        Initial conditions
176        with {
177            the IUT entity "being in" the "initial state" and
178            the Manufacturer entity provides the credentials
179        }
180
181        Expected behaviour
182        ensure that {
183            when {
184                the Evaluator entity provides the "time period of inactivity" containing
185                    duration set to "session lock duration";
186                and (.) at time point t1 : the Evaluator entity enters the credentials containing
187                    account identifier indicating value "valid account identifier",
188                    account authenticator indicating value "valid account authenticator";
189            }
190            then {
191                (!) duration after t1 : the IUT entity "closes current session"
192                and the IUT entity indicates a message containing
193                    account access indicating value "access denied",
194                    "current session" indicating value invalid;
195            }
196        }
197    }
```

Fig. 3: Sample Security TP using TDL-TO

It has to be noted that the authors of TDL-TO specifications need to provide the predefined keywords in a TDL package domain description about involved entities (“IUT”, “Administrator” etc.), relevant events (“provides”, “being in” etc.) and data declarations (“credential list”, “password_list” etc.). Such common definitions may be included in a separated package as part of a common library and need to be imported from the TP modules.

5 Conclusions

The work covers selected industrial security requirements provided by IEC [IE01]. Selected requirements can be collected and specialized to form an industrial security profile. According to the ETSI methodologies, test purposes have been defined with TDL-TO. Implementation of the test purposes depend on the testing type and available tool. In case of automated testing of security functions, the application of TTCN-3 technology [ET02] appears as most appropriate (cp. IoT-Testware [EC01]). For test purposes that require penetration testing specialised test harness supporting e.g. fuzzing technology is needed.

References

[DW01] de Meer, J.; Waedt, K.: New Security Standards for Industrial Automation and Control Systems, based on IEC 62443-4-2 (IACS/SCADA). In (Mayr, H.C.; Pinzger, M. (Eds.): INFORMATIK 2016, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn, p. 537-541, 2016.

[EC01] Eclipse Foundation technology project IoT-Testware, https://projects.eclipse.org/projects/technology.iottestware

[ET01] ETSI ES 203 119-4 V1.3.1: Methods for Testing and Specification (MTS); The Test Description Language (TDL); Part 4: Structured Test Objective Specification (Extension), 2018.

[ET02] ETSI ES 201 873 V4.10.1: Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3, 2018.

[ET03] ETSI MTS Test Specification for foundational Security IoT-Profile, https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=54751.

[ET04] ETSI ES 202 553 V1.2.1: Methods for Testing and Specification (MTS); TPLan: A notation for expressing Test Purposes, 2009.

[ET05] ETSI TS 102 868-2 V1.4.1: Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 2: Test Suite Structure and Test Purposes (TSS & TP), 2017.

[ET06] ETSI brochure Interoperability Best Practices, https://portal.etsi.org/CTI/Downloads/ETSIApproach/IOT_Best_Practices.pdf.

[GM01] GSMA IoT Security Guidelines & Assessment, https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

[IE01] IEC 62443-4-2: Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components, 2017.

[OM01] OMG: UML Testing Profile. https://www.omg.org/spec/UTP/About-UTP/

Test services for interoperable and secure shop-floor IT application interfaces in OPC-UA

Frank-Walter Jäkel[1], Tobias Wolff[1] and Leonard Hackel[1]

Abstract: The need of interoperable and secure IT interfaces of manufacturing equipment and related test services in the context of plug-and-produce is essential in the scope of digital transformation. The paper will focus on a test service validating the compliance of new machinery regarding the manufacturing IT infrastructure and applications such as production data acquisition (PDA). It will be demonstrated in terms of a prerequisite for interoperability and using OPC-UA [LM16].

Keywords: Shopfloor, Digitalisation, Test, Interoperability, Plug-and-Produce.

1 Introduction

The application of the Internet of Things in business practice is already a reality in many places. It is expanding rapidly in production seen by approaches such as industrial internet of things (IIoT). This is a challenge for equipment or tool provider and the users or buyers. Simple security mechanism can lead to interoperability barriers between machinery components. Just cut-off security and reduce required data acquisition (find in industry on buyer side) cannot be the final solution especially it can create additional risks. This can lead to the dangers of insufficient data security, malfunction or lack of interoperability and can result in production stops and in economic damages.

Industrie 4.0 together with digital transformation needs an IT infrastructure able to link, control and monitor equipment on the shop floor. This require compatibility between such IT infrastructure and the digital interfacing of the equipment. Incompatibility can lead to a stop of production, later start of production or even crash of machinery. The requested behaviour calls plug-and-produce [Dr16] derived from the IT term plug-and-play [Dr16]. Physical or digital systems with plug-and-produce functionality can easily connect as well as just switch on and work. Today plug-and-produce for manufacturing equipment is still oriented to a physical integration. Manufacturing tool providers are just start to see interoperability as an important challenge of the digital components of their machines. They still try competition by using non-compatibility with their competitors. The users of the machinery such manufacturing plants already praxis the issue of different machines not working together in the target IT infrastructure. From project experiences and discussions with industrial partners, it is no more only big automotive companies also

[1] Fraunhofer IPK, Pascalstraße 8-9, 10587 Berlin, frank-walter.jaekel@ipk.fraunhofer.de, tobias.wolff@ipk.fraunhofer.de, leonard.hackel@ipk.fraunhofer.de

smaller manufacturing enterprises have difficulties to integrate new machinery and they were blocked by incompatibilities. Therefore, the plug-and-produce capability for the digital interface of the equipment is required by the digital transformation of manufacturing enterprises.

Frameworks and protocols are essential to ensure a plug-and-produce for the digital interface. Approaches such as OPC-UA [In17] for industrial implementations of internet of things (IoT) provide solutions starting to be used in industry. Test mechanism are on the way to ensure security and compliance for protocols and frameworks [Pe17]. Nevertheless, the application-oriented configuration of interfaces are very specific. This calls for easy to use solutions to check the digital interface in the context of the application demands and specified configurations.

A configuration approach is used to configure an adapter, to test the devices in the sense of a Cyber Physical System (CPS) or to test the IoT interface of the devices. This is the buyer's/user test method to ensure that the machine supplier has specified the interface according to the requirements. But even before the plant operator makes a decision for or against the purchase, the operator wants to test whether the extension by a production module fits into the existing production and no problems arise. This requires an emulation of the relevant system components and the specified interface. Both the testing of the interface of modular system components and the emulation of entire production systems is an important component and facilitates the work of system integrators on the user side.

The paper describes a potential solution to ensure the conformity of a machinery digital interface with a given IT infrastructure. The solution takes OPC-UA for the software implementation. However, in the future also other options such as, DDS, CoAP or MQTT [In17] under consideration.

2 General description

The digital part of the manufacturing devices or machinery requires an IT interface to interlink with other machinery or to a digital network. The machine supplier might buy the digital part from specific providers. At this stage, a specific label proving security behaviour and compliance to a standard protocol would support a basis for interoperability of the machinery interface. This needs to be extended by application-oriented functions specified by the buyer/user. An example of such function is the conformity to existing enterprise application interfaces. Standards such as OPC-UA are helpful but not enough to ensure the interoperability because of specific compliance demands on the buyer/user side. Therefore, the provider needs to deliver an adapted interface. Both the provider and the buyer needs to check the interface against the specific demands of the buyer. To create such a check the interface specification needs to be described in a formal way to be used as a configuration of the check. The OPC foundation provides a XML format to describe

the configuration of nodes and value types. This has been used in the prosed solution. An enrichment was necessary to describe specific aspects, which have to be checked.

The conceptual system architecture (Figure 1) of the prosed solution consists of the following parts:

- An adaptor for the validation of conformity regarding a given machinery interface and configured by a requested OPC-UA node setting. “ValidationAdaptor” is the name of this component.
- An emulation of a CPS also configured with a requested OPC-UA node setting. The role of this emulation is to simulate specific OPC-UA settings. This provides an opportunity to test the Validation Adaptor. The name of this component is CPS Emulator.

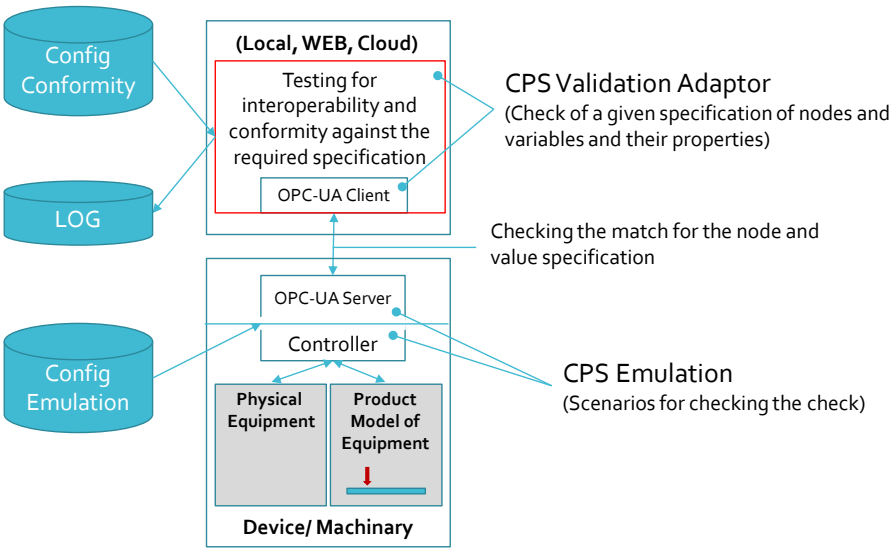

Figure 1: Conceptual system architecture for Validation Adaptor and CPS Emulator

The buyer as well as the provider are potential users of the solution. The buyer can use it to check their specification and provide it to the provider as a feature to improve the interface development. The provider can use the validation adaptor for quality checks and the buyer can use it for the final check of the new delivered device or machinery, see also Figure 2.

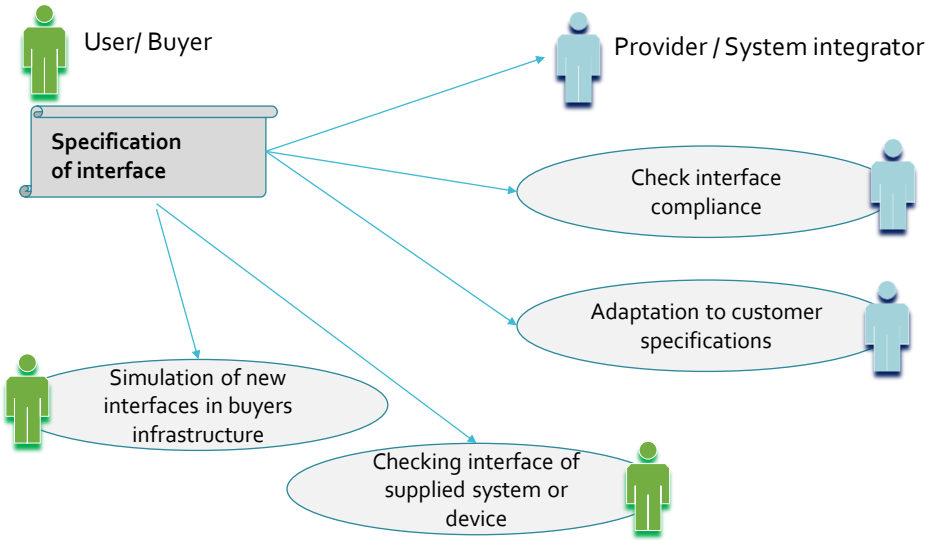

Figure 2: Application view on the use of Validation Adaptor and CPS Emulator

3 Conformity Check and Validation Adaptor

This service is responsible to check one CPS based on the configuration and potential scenario models. Each machine in the shopfloor IT has a different interface configured by the machine tool manufacturer. In order to reduce the risk of failure during the integration of machines into the existing IT infrastructure, these interfaces must be tested according to the buyer's specifications. The validation adapter has been developed for this purpose. This consists of the adapter itself, a configuration file, a graphical interface and a file in which the result of the test is written. The adapter uses the configuration file to connect to the CPS interface and check the interface for the description of the interface functionality in the configuration file. In the first step, the OPC UA communication technology was selected for the interface.

For the adapter the open source project Milo of the Eclipse Foundation was used. This framework implements OPC functionalities such as creating and connecting OPC UA clients, reading and writing variables and publishing and subscribe. Extensions are the reading of a configuration file, the usability with the help of a graphical user interface, the writing of the results into a file and the conformity algorithm itself.

The first prototype uses a self-created XML format as configuration file. Figure 3 shows an example of a sample section. The configuration contains a description of the test and the system to be tested. These two files together are the test configuration. Then there is

the node structure, which is divided into individual nodes. Each node is uniquely determined by a name, NodeID and its parent node. By extending the adapter with a graphical interface, the test configuration can be created by the user. TCP/IP as an example can then be selected as the connection protocol. The configuration then requires an IP address, as well as a port and especially for OPC UA a security mechanism used. The operator also decides what is being tested. Whether the variables correspond to a specific data type or whether the node structure in the server meets expectations. This automatically creates the test configuration from the validation adapter and saves it in a file. The node structure with the information about the nodes is then saved in another file. In future, the OPC Foundation standard will be used for the node structure. It provides an XML format to describe the entire address space of a server, but it is also possible to specify nodes and their relationship to each other.

```
<description>
    <name>Configuration file for the Testware</name>
    <versionsyntax>1.0</versionsyntax>
    <versiondocument>1.0</versiondocument>
    <guid>b98a47e5-84e6-4e9f-9999-b861dcea6c85</guid>
    <datecreation>19.03.2018</datecreation>
    <creator>Tobias Wolff</creator>
    <datevalidation>21.03.2018</datevalidation>
    <validator>Tobias Wolff</validator>
</description>

<testsystem>
    <cps>GESI OPC UA Server</cps>
    <rootnode>
        <name>Root</name>
        <nsindex>0</nsindex>
        <identifiertype>Numeric</identifiertype>
        <identifier>84</identifier>
    </rootnode>
    <ip>opc.tcp://141.58.122.40:</ip>
    <port>4841</port>
    <security>none</security>
</testsystem>

<node>
    <name>Objects</name>
    <nsindex>0</nsindex>
    <identifiertype>Numeric</identifiertype>
    <identifier>85</identifier>
    <parent>
        <name>Root</name>
        <nsindex>0</nsindex>
        <identifiertype>Numeric</identifiertype>
        <identifier>84</identifier>
    </parent>
    <attributes>
        <nodeclass>Object</nodeclass>
        <param1>
            <attribute>Eventnotifier</attribute>
            <value>None</value>
        </param1>
        <param2></param2>
        <param3></param3>
        <param4></param4>
    </attributes>
</node>
```

Fig. 3: XML Configuration File

The graphical user interface allows the selection of different configuration and result files. If a configuration file has been selected, the test can be started or the user can display the

configuration and check the data. Displaying the result file follows the same principle. The user can also use the interface to write his own configurations.

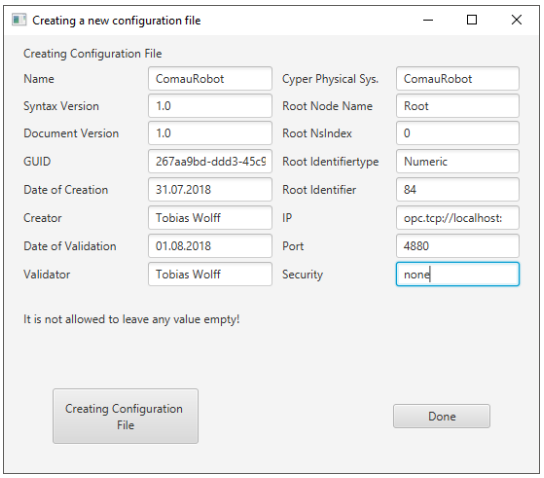

Fig. 4: Creating a new Configuration

Figure 4 illustrates the dialog of creating a new configuration. Here for example, the test configuration of the validation of a local OPC UA server (CPS Emulator). Various parameters, such as a GUID or system name, are defined here. This allows the tests to be clearly identified. In addition, data such as creation date and author are of interest. Among other things, the configuration also contains the parameters that the adapter needs to connect to the server. For OPC UA, an IP address, a port and security are required.

How does the validation of an interface work?

The validation adapter first reads the configuration and establishes a connection to the server specified in the configuration. The individual nodes of the configuration are then checked. Two variants are possible. Either the nodes are addressed uniquely using their NodeID or only a name of the node and its parent node is specified. In OPC UA the NodeID of a node is always unique, whereas the name of a node is divided into display name and browser name. Figure 2 shows an example from our local OPC UA server. We tested the validation adapter against this server emulation. With the help of the program UA Expert [UA18] it is possible to display the node structure of a server graphically. Figure 2 shows the information from the two "inputsVariable" nodes. Both have the same display name, but different browser names. According to the OPC UA standard, the browser names should always be unique if possible. Also, both are different from their parent node. This parent-child relationship and the browser name enable the adapter to identify the node.

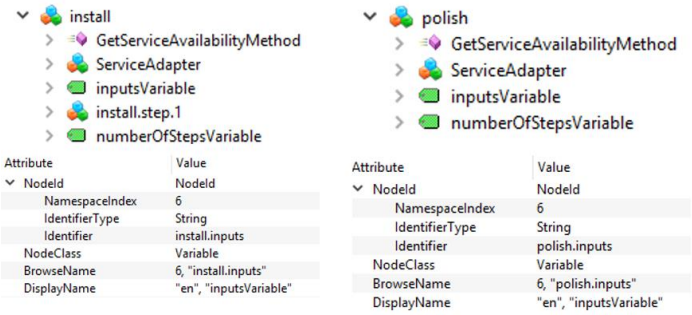

Fig. 5: Visualization of Nodes

After validation of the interface, the result is written to an XML file. Figure 6 shows a section. In addition to the description of the test, the individual results are logged in the file. In this section, the adapter was able to connect to the server and perform the validation. The first specified node exists in the server, could be addressed by its NodeID, and is a subnode of the specified top node.

```
<testsystem>
    <cps>GESI OPC UA Server</cps>
    <rootnode>
        <name>Root</name>
        <nsindex>0</nsindex>
        <identifiertype>Numeric</identifiertype>
        <identifier>84</identifier>
    </rootnode>
    <ip>opc.tcp://141.58.122.40:</ip>
    <port>4841</port>
    <security>none</security>
    <result>
        <boolean>true</boolean>
        <text>Connection established</text>
    </result>
</testsystem>
<node>
    <name>Objects</name>
    <nsindex>0</nsindex>
    <identifiertype>Numeric</identifiertype>
    <identifier>85</identifier>
    <result>
        <boolean>true</boolean>
        <text>Parent/Child relationship is correct</text>
    </result>
    <parent>
        <name>Root</name>
        <nsindex>0</nsindex>
        <identifiertype/>
        <identifier>84</identifier>
    </parent>
</node>
<node>
```

Fig. 6: The Result of Validation

Up to now, the adapter has been used in two cases. In the first step with the local OPC UA server of the IT architecture, afterwards with a server located in the cloud. The project is intended to realize the control of the machines with the help of a cloud.

Furthermore, a first test in the real factory process at a customer is in progress.

4 Emulation of CPS

The emulation enables system integrator to test the behaviour of a specific machine configuration in predefined or user-specific conditions and environments. Without the emulator, the system and integration tests can only be executed once the new CPS arrives on the shop floor. However, this can be done earlier if one uses the emulator. Additionally, different scenarios such as failures can be simulated without risk of production breaks or other misbehaviour, thus reducing risk of economic damage.

A running emulator will not be distinguishable from a real CPS. This lifts work from system integrators by omitting configuration activities once the emulator is embedded into the running machine cluster. For example, in OPC UA a client will not see if the server it is accessing is an emulator or a running CPS. Once the new CPS arrives, it can simply be swapped out for the emulator after ensuring conformance to specification (e.g. using the validator). This reduces production line down time to a minimum.

5 Usage / Example

An initial industrial application of the Validation Adaptor takes a “production data acquisition system” and its OPC-UA interface demand. It is to access an OPC UA server and retrieve information about the running process as well as about the production equipment. This use case provides an optimal environment for testing the Validation Adaptor and the CPS emulation.

The buyer specified the node structure of the server. Only names were used and no NodeIDs, therefore the adapter at first had to be extended by a routine that solves this problem.

The configuration could then be derived from this specification. Since the adapter had to be tested in real factory operation before use, the CPS emulation configuration was developed in parallel. In this server emulation the node structure was created and the validation adapter could check it with the configuration.

In this way it is possible for the system integrator to check both the machine provider and the user side. From a technical point of view it is now possible to check OPC UA clients as well as server interfaces.

6 Conclusion and next steps

The problem of ambiguity of names became clear from the application case of production data acquisition. In OPC UA only the NodeIDs are unique, the names can exist several times. If the nodes are addressed using the names, there must be no ambiguity between them. During validation, the adapter should detect these multiple names and provide an adequate solution.

In addition to addressing the nodes, other attributes of the node are important for the system integrator. For example, if a temperature value is to be written, but the node has not been initialized as an integer but as a Boolean variable. This means that writing is not possible, an error occurs and a system failure may occur. The Validation Adapter is therefore extended to include a check of data types.

In addition to these enhancements, work is also being done on the usability of the graphical user interface and the presentation of results.

In the current version of the Validation Adapter, the Milo framework of the Eclipse Foundation is used in an early version. During the development some problems occurred, because not all functionalities, as provided by the OPC UA specification, are implemented. Besides the Eclipse Foundation, there are numerous other manufacturers that offer OPC UA frameworks. These are mostly commercial, but better documented in the process and offer better support during development. Therefore, a move to other frameworks are planned.

References

[LM06] Leitner, Stefan-Helmut, Mahnke Wolfgang: OPC UA – Service oriented Architecture for Industrial Applications. ABB Corperate Research Center, 2016.

[Dr16] Belden Inc., https://www.belden.com/blog/industrial-ethernet/plug-and-produce-is-key-for-the-smart-factory-of-the-future-part-1, Stand: 27.08.2018.

[UA18] UA, Unified Automation GmbH, https://www.unified-automation.com/de/produkte/entwicklerwerkzeuge/uaexpert.html, Stand: 29.08.18.

[In17] Plattform Industrie 4.0: Industrie 4.0 Plug-and-Produce for Adaptable Factories: Example Use Case Definition, models and Implementation. In Public Relations (Federal Ministry for Economic Affairs and Energy). Berlin, 2017.

[Pe17] Pfeiffer, Thomas: Realisierung eines verteilten IT-Systems auf Basis von OPC UA, Universität Stuttgart, S. 74-80 , 2017.

[Si18] Siemens AG, https://www.siemens.com/global/en/home/products/automation/tia.html, Stand: 22.08.2018.

Time-Sensitive Ethernet Technology for Next Generation CPS/Industry 4.0

Venesa Watsons[1] and Jochen Sassmannshausen[2]

Abstract: Cyber-Physical Systems (CPS) represent a collection of computing components and networks used to monitor and control physical processes. CPS are deployed in several domains, including the electricity grid and industrial automation, generally as a part of the industry 4.0 (I4.0)/next generation effort. An integral part of the CPS is its communication network, where Ethernet-based technology is generally used to implement the physical and data link layers. However, as the critical features of CPS include time synchronization, reliability, interoperability, scalability and real-time operations, standard Ethernet is insufficient. As such, it is extended Ethernet variants that are commonly found in CPS domains. In fact, industry players are endorsing TSN (Time-Sensitive Networking) with OPC UA, as the communication backbone for the next generation. This paper compares TSN to other time-sensitive Ethernet technology, namely PROFINET, AFDX (Avionics Full Duplex Switched Ethernet), TTE (Time-Triggered Ethernet) and AVTP (Audio Video Transport Protocol), to determine their suitability and advantages for use in next generation CPS.

Keywords: CPS; I4.0; next generation; TSN; OPC UA; PROFINET; AFDX; TTE; AVTP;

1 Introduction

Industry 4.0 (I4.0) is described as the fourth industrial revolution, where manufacturing is digitally transformed through accelerators such as IIoT and the convergence of IT and OT, to realize smart, connected factories, with accelerated system performance and robustness [WS17]. For I4.0, Cyber-physical systems (CPS) represent one enabling component – the others being IoT (Internet of Things) and cloud computing [IS17] [AE17]. CPS (e.g. SCADA/Supervisory Control and Data Acquisition) integrate physical processes, computation and networking, where the latter two elements are used to monitor and control the physical processes. As CPS are designed to interact and interoperate with systems from different manufacturers that support processes with varying performance requirements, special importance is placed on the communication technology. In that, this communication technology must provide support for reliability, fault-tolerance, scalability, real-time operations, low cost and time synchronization. In industrial plants, CPS utilize proprietary (e.g. EtherCAT) and open communication standards (e.g. PROFINET) to support these requirements. However, as interoperability becomes a chief requirement with I4.0, proprietary standards become less favourable.

[1] University of Siegen, Faculty of Science and Engineering, Chair for Data Communication Systems, Hölderlinstraße 3, Siegen, 57068, venesa.watson@uni-siegen.de
[2] University of Siegen, Faculty of Science and Engineering, Chair for Data Communication Systems, Hölderlinstraße 3, Siegen, 57068, jochen.sassmannshausen@uni-siegen.de

Even so, industry players are also considering emerging standards, such as ARINC 664 (specifically, part 7: AFDX - Avionics Full Duplex Switched Ethernet), TTE (Time-Triggered Ethernet), TSN (Time Sensitive Networking) and AVTP (Audio Video Transport Protocol), to enhance or replace open industrial standards. In fact, several industry leaders have expressed support for TSN to realize I.40 and IIoT infrastructures [BR16] [Av14]. Thus, signaling the need for advanced communication technology to optimally support the increased connectivity between diverse processes, systems and domains.

This paper compares AFDX, AVTP, PROFINET and TTE, to evaluate their suitability for next generation CPS, such as found in power plants. The arguments presented seek to highlight the advantages of TSN, and how other time-sensitive standards can prove to be as competitive. This paper is arranged as follows: section 2 looks at the communication architecture evolution from I3.0 to I4.0, and the resulting demand for time-sensitive Ethernet technology. Section 3 provides an overview of time-sensitive technologies, with descriptions of the mechanisms for traffic shaping, policing and so forth. Section 4 evaluates AFDX, AVTP, PROFINET and TTE according to these mechanisms of section 3. The discussion and conclusion are presented in section 5.

2 CPS in Industry 4.0

The communication networks in an I3.0 infrastructure follow a pyramid approach, where the network architecture is often referred to as an "*automation pyramid*" (Fig. 1) [KH17] [Gr17]. The automation pyramid is characterized by a rigid communication structure, where the complex industrial networks and applications are separated into functional levels. For example, CPS typically operate from the Enterprise and Supervisory levels. In this pyramid structure, communication is boundless horizontally, but restricted vertically. As such, direct communication across multiple layers of the entire automation system, seldom occurs. Systems built on this structure are strictly hierarchical and not very flexible [KH17] [Gr17]. However, with the I4.0 application requirements and the new enabling technologies, automation networks must move away from this rigid pyramid model, to allow faster and boundless vertical communication. For this, a pillar approach is proposed, referred to as an "*automation pillar*" (Fig. 1) [KH17] [Gr17]. As shown, the evolution from automation pyramid to automation pillar sees most changes occurring at the control level, whose functions are merged with the (lower) field level and the (upper) supervisory and enterprise levels. Further, the control level then transitions into a highspeed communication tunnel, relying on the services of a time-sensitive, communication technology to support the fast, vertical exchanges across the pillar architecture [Gr17][Be16].

As a globally-accepted standard that is inexpensive, ubiquitous and offers high throughput, Ethernet-based technology is envisioned for this highspeed tunnel. However, it is the time-sensitive variants that are solely considered, as they eliminate unfavourable characteristics, such as traffic collision and unbounded latency that are intrinsic to

standard Ethernet. For instance, the I4.0 automation pillar is projected to be more open and flexible and capable of supporting expansive communication services [KH17] [Gr17]. Industry players anticipate leveraging CPS functions to have more far-reaching impact in I4.0 architectures. In that, mixed-criticality processes such as remote maintenance by an operator or a remote data request by a regulator should be seamlessly and efficiently facilitated by the communication technology implemented. Standard Ethernet does not have the mechanisms to support reliable, time and mission-critical data exchange, robust fault-tolerance and mixed-criticality processes. As Fig. 1 indicates, TSN is a suitable standard for the I4.0 infrastructure and is considered as the fore-runner [KH17] [Gr17]. In later sections, select time-sensitive Ethernet technology are discussed as viable options for next generation CPS.

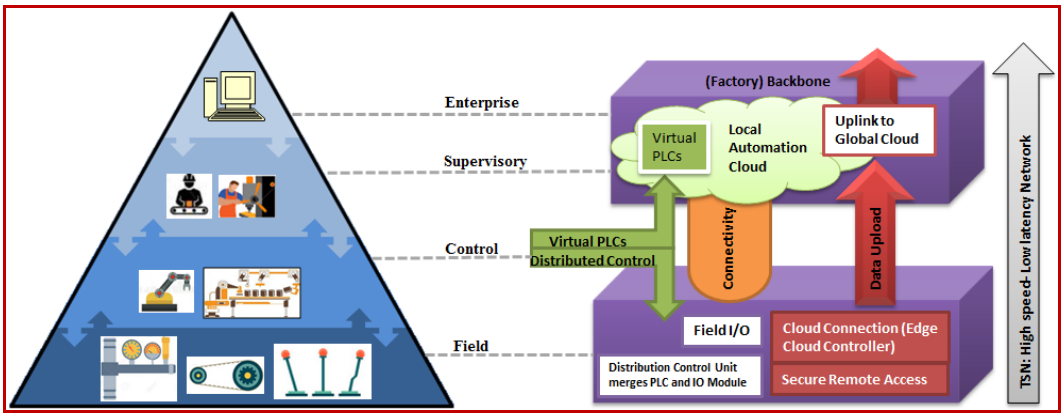

Fig. 1: I3.0 Automation Pyramid Transformation into I4.0 Automation Pillar [Gr17].

3 Time-Sensitive Ethernet Services

Time-sensitive Ethernet denotes Ethernet-based communication standards that add services to standard Ethernet to achieve real-time data exchange, amongst other advantageous properties. These services, though common among AFDX, AVTP, PROFINET and TTE, have different implementations. These differences, as will be discussed later, can give a communication standard special advantage over the others. The services that follow have been chosen as they suitably address the communication requirements in next generation CPS – mixed criticality support, fault-tolerance, time-sensitive data exchange, and reliable communication.

3.1 Traffic Categorization

In an I4.0 infrastructure, CPS will see increased traffic volumes, with each stream associated with its own time and mission-critical needs. Simply put, traffic streams can

be either critical or non-critical, and mechanisms must be available to identify and classify traffic in a similar manner. Critical traffic denotes those streams of data that must be delivered within a short and specific time, especially where safety requirements are considered. Non-critical traffic consists of data where delivery period is not as strict. However, a wider categorization may be necessary to support the diverse traffic streams that are expected. In that, some traffic streams may fall in-between critical and non-critical. For instance, a traffic stream with critical data that has time delivery requirements akin to non-critical traffic should not be treated as non-critical. As an example, the IEC 61850 standard for the electric grid, specifies two traffic categories – time-critical and less time-critical – each with additional subcategories of traffic [IE13]. Therefore, where time-sensitive Ethernet is projected to replace commonly used standards, those with inclusive traffic categorization mechanisms are more favourable.

3.2 Traffic-Shaping

Traffic-shaping is used to regulate traffic based on network resources and traffic categorization to prevent resource misuse and subsequent failures. This mechanism is typically achieved with scheduling algorithms that follow any of the below unexhausted list of policies [In10] [Fi17]:

First-in-First-out (FIFO): traffic is sent in order the arrival, regardless of priority. Higher priority traffic may experience unfavourable delay.

Pre-emptive: lower priority traffic is interrupted while in transmission, to allow higher priority traffic. This means that the lower priority traffic must be retransmitted again later, and that the bandwidth used for the pre-empted low priority traffic is wasted.

Scheduled Transmission/Timely-Block: the schedule of the high-priority traffic is used to calculate when a frame is expected to arrive. Traffic is then scheduled so that there is no current transmission when the high-priority traffic is to be sent.

Shuffling/Non-pre-emptive: higher priority traffic waits until the traffic in transmission is finished. This introduces a delay to the higher priority traffic, but bandwidth is not wasted.

Weighted Fair Queuing/Weighted Priority: Each traffic stream or traffic category is assigned a weighted amount of network service, which determines its delivery period.

Communication standards can use a single algorithm that follows one of the above policies or use at least two algorithms that follow differing policies, to optimize scheduling. The choice of algorithms is a determinant factor in the timeliness and efficiency of the data exchange.

3.3 Traffic-Policing

Intentional and unintentional sources of errors, such as sporadic/babbled traffic, can

result in misuse or inundation of network resources. It is therefore necessary to ensure that mechanisms are in place to detect and isolate errors, to prevent total system failure. Traffic policing services are responsible for monitoring traffic streams on the network and enforcing compliance to the network design rules. Where traffic is non-compliant, preventive measures must be present to protect the network from any resultant negative impacts. These are necessary to ensure network availability. Typical network design rules concern the allotment of and compliance to this allotment of network resources, such as link capacity, transmission window, transmission rate, traffic size, and frame correctness. The dependability of a network is reliant on the correct functioning of the traffic flow. Data exchange must be reliable and stable, even in the presence of errors. This is especially critical in power plant environments, where availability is of vital importance for safety and security. Further, as the increased connectivity in I4.0 infrastructures implies increased sources of errors, robust traffic policing mechanisms are essential for next generation CPS.

3.4 Time Synchronization and Bounded Latency

Time-sensitive data exchange is possible without time synchronization, as this service is not essential for timely delivery. Even so, with the use of a clock reference, time synchronization services can offer even greater control. For example, operators at a power plant can precisely predict when and where a data exchange has or will take place. This offers special advantage in network planning and design, as well as in traffic scheduling. Further, time synchronization supports auditing and forensic investigations tracking of security events, network errors and resource usage. However, one major disadvantage with time synchronization is that an erroneous clock and/or the loss of synchronization can cause major communication disruptions. In fact, clock references and clock synchronization mechanisms represent prime attack points for attackers seeking to cause severe failures, such as DoS. As such, time synchronization mechanisms should have functions that ensure dependable clock reference. Further, time synchronization is insufficient on its own to ensure timely delivery. When traffic flows across a network, it will experience jitter – for example, as introduced by multiplexing and contention with other traffic. The effect of jitter is unpredictable and could cause unfavourable delays. To minimize the effect of network delay, and in doing so, ensure predictable throughput (determinism), mechanisms to bound latency become necessary. The overall effect is support for guaranteed quality-of-service (QoS), through improved system efficiency. Time-sensitive Ethernet technology must therefore provide mechanisms to enforce and protect precise timing.

4 Evaluation of Time-Sensitive Ethernet

The previous section provided an overview of the services that are characteristic of time-sensitive Ethernet technology, which make them viable for next generation CPS. The

descriptions indicate the existence of a symbiotic relationship among the services – as it is observed how any one service supports at least one other service. The relative advantage of the implementation of these services in AFDX, AVTP, PROFINET and TTE, is evaluated to determine the strengths and weaknesses of these standards. First, the selected standards are summarized below.

4.1 Overview of Time-Sensitive Ethernet Standards

TSN is a set of IEEE 802.1 sub-standards that add extensions to standard Ethernet, to allow deterministic, time-critical communication [WS17] [TT17]. However, the TSN protocol is situated at the data link layer of the OSI model, and as such, is typically combined with other standards. For example, TSN is proposed for use with OPC UA (Open Connectivity Unified Architecture) in I4.0 architectures. OPC UA, as defined by IEC 62541, is a platform and vendor-independent standard that supports device interoperability, by providing services that allow different devices to communicate with each other [IE16b]. TSN services are also deployed for the benefit of time-critical applications in AVTP, which is defined in IEEE 17222016 Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks. Here, consideration is given to the industrial context (industrial automation and control networks). AFDX is an implementation of the ARINC 664 standard and denotes the electrical and protocol specifications for data exchange between Avionics Computer Systems [AR09]. AFDX has three (3) components, namely, the Avionics Subsystem, the End System, and the AFDX Interconnect. AFDX derives its time-sensitive properties from the services fulfilled by the subcomponents of the above-listed main components. These include virtual links (VLs), a scheduler, and a forwarding table. As an example, each VL has three (3) properties that are used to support time-sensitive mechanisms: (1) BAG (a bandwidth allocation gap) - the minimal interval (milliseconds) between Ethernet Frames that are transmitted on the VL; (2) Lmax - the largest Ethernet frame, in bytes, that can be transmitted on the VL; and (3) VL link capacity - the maximum share of the total capacity of the physical link.

ARINC 664 traffic is also observed in TTE, which is described as a time-division multiple access (TDMA) extension to standard Ethernet designed to meet the hard deadlines required by real-time networks [Ch15]. TTE uses the services as defined by SAE AS6802 to support the requirements of time-critical applications. These services facilitate the design of advanced integrated systems that utilize asynchronous and synchronous communication [GE09]. TTE uses a switched Ethernet network, and connected systems can be grouped according to traffic criticality and communication approach (asynchronous or synchronous) [GE09]. Finally, PROFINET is an industrial Ethernet standard that uses three communication services to support the specific application needs. These are: standard TCP/IP, real-time (PROFINET RT), and isochronous real-time (PROFINET IRT). PROFINET uses layers 1 to 4 and 7 of the OSI model, but PROFINET RT and IRT bypass the TCP/IP layers (3 and 4) to support time-critical requirements [PR17] [In14]. PROFINET is different to PROFIBUS, as it is based

on Ethernet, but the communication structures are similar. There is a master/slave topology with predefined time schedule and time slots where communication is allowed [Ve10] [AR15].

4.2 Traffic Categorization

Traffic categorization and time synchronization services lend support to real-time operations in AVTP, AFDX, TTE and PROFINET. In AFDX, there is no distinct traffic classification, except for inside the switch, where additional scheduling is also done. Here, traffic is classified as high priority or low priority [AR09]. Nevertheless, as AFDX does not dictate specific implementation methods, the system designer can use the VL and subVLs (maximum of 4 subdivisions of a VL), along with their associated properties - BAG and Lmax - to prioritize traffic. With TTE, there are four categories of traffic: (1) Protocol Control Frame (PCF) - used to establish and maintain synchronization; (2) Time-Triggered (TT) frames - dispatched according to a predefined communication schedule; (3) Rate-Constrained (RC) frames - simply ARINC 644 traffic, where similar AFDX-type properties are observed; and (4) Best Effort (BE) frames - treated as normal Ethernet network [Ch15] [GE09]. Similarly, AVTP has four classes of traffic: (1) SR class A - has a required latency of 2 milliseconds; (2) SR class B - required latency is 50 milliseconds; (3) Control traffic - includes IEEE 802.1 AS generalized Precision Time Protocol (gPTP) and IEEE 802.1Qat Multiple Stream Reservation Protocol (MSRP); and (4) Best effort (BE) - includes low-effort, low-priority Ethernet traffic [IE16a].

With OPC UA TSN, up to eight traffic classes can be defined, which are each associated with a QoS priority that determines how they are handled [IE16c]. With PROFINET, there are three different traffic classes: (1) PROFINET CBA (component-based automation) - non-time critical data, for example TCP/IP communication (class A); (2) PROFINET IO – for real-time transmission of data, which allows both cyclic and acyclic transmission (class B); and (3) PROFINET IO IRT - allows transmission times of 250µs and maximum jitter of 1µs (class C) [Fr09] [MG14]. Classes B and C require specialized hardware instead of standard Ethernet components. The PROFINET guideline distinguishes between three conformance classes that defines requirements to the communication hardware. Only class A conformance can be met with standard Ethernet hardware, cyclic scheduling and precise clock synchronization (<1µs tolerance and bus cycle times <1ms) as required by RT; and IRT data can only be met with additional efforts and dedicated hardware [PR11].

4.3 Time Synchronization

Time synchronization is defined in TTE, PROFINET and AVTP. In a TTE network, end systems and switches are set as synchronization masters, compression masters or synchronization clients [GE09]. The TTE time synchronization follows a twostep process, which involves these TTE nodes. The compression masters use the average

relative arrival times of PCFs sent by the synchronization masters, to create new PCFs. These are then sent to synchronization clients, to complete the time synchronization process [GE09]. With AVTP, IEEE 802.1AS is used to achieve precise timing and clock synchronization across the distributed network nodes. IEEE 802.1AS specifies the operation of time-aware systems on a bridged LAN. There are time-aware endpoints, with one serving as the grandmaster (the primary source of time information). Then, time-aware bridges, which receive time information from the grandmaster, apply corrections to compensate for delays in the LAN and the bridge itself, and retransmit the corrected information. Any time-aware system with clock sourcing capabilities, can be a potential grandmaster. The Best Master Clock Algorithm (BMAC) is the selection method used to ensure that all the time-aware systems use the same grandmaster [IE16a]. OPC UA/TSN also uses IEEE 802.1AS for time synchronization. PROFINET uses the *so-called* Precision Transparent Clock Protocol (PTCP). Time synchronization is required for isochronous real-time (IRT) applications with defined timeslots. PROFINET allows a maximum error of 1µs in the time slots. This requirement allows achievement of a very low jitter (<1µs). IRT data will be sent at the beginning of every bus cycle. After IRT data is transmitted, the rest of the bus cycle is used to transfer lower priority telegrams [Fr09].

There is no time synchronization function described for AFDX. Instead, it enforces upper (500µs) and lower bounds on latency to enforce a strict time limit on traffic delivery [AR09]. TTE also enforces bounded latency and jitter, but selectively. These limitations are only applied on time-triggered and rate constrained traffic streams [GE09]. AVTP also selectively uses bounded delay –it is only enforced on time-critical traffic. AVTP defines low latency SR class A traffic with a maximum latency of 2ms over 7 hops, and for SR class B traffic, 50ms over 7 hops. AVTP also specifies that SR class A and SR class B streams each have a Max Timing Uncertainty (the maximum amount of transfer delay allowed) of 125µs and 1000µs, respectively [GE09]. Concerning OPC UA/TSN, the combination of IEEE 802.1Qbv for scheduling and IEEE 802.1AS for time synchronization, facilitates traffic scheduling and transmission that are precise to the microsecond (µs). In doing so, deterministic transmission and QoS is achieved, and latency and jitter are optimally minimized [IE16c]. For PROFINET, the end-to-end latency depends on the traffic class and ranges from 100ms down to <1ms for Motion Control applications (class C). The end-to-end delay also depends on the bus cycle times and other factors like the message length and the cable length used (maximum 100m according to the Ethernet standard). Cyclic IRT data is sent at the beginning of each bus cycle and a bus cycle can be shorter than 250µs. The analysis shown in [Fr09] calculates a maximum delay of <450µs in a scenario where an IRT-message is forwarded via 4 hops. IRT data has deterministic behaviour regarding both end-to-end latency and jitter. The communication topology and all IRT feeders must be determined during system design [Fr09].

4.4 Traffic Shaping and Policing

Traffic shaping and traffic policing are observed in all the selected specifications. For AFDX, traffic shaping occurs at the sending End System, where traffic streams are monitored for conformance to their assigned BAG and Lmax properties. Here, traffic is scheduled for transmission based on the implemented scheduling algorithm. Additional scheduling is conducted at the AFDX switch, where the token bucket algorithm is used to control the traffic flow, and a FIFO policy is used at the egress ports. Traffic policing is conducted at the AFDX switch where frames are checked for frame correctness and resource compliance; and at the destination End Systems, where the frame sequence number is used to detect unexpected or duplicated frames. Non-conformant frames are dropped. TTE recommends that a non-pre-emptive algorithm must be used, and that pre-emptive algorithms can also be included for traffic shaping. The TTE-enabled switch performs the policing functions, where frames are checked for conformance to network allowances (frame size and link capacity). As TTE uses a time parameter, frames are also checked for schedule conformance. Non-compliant frames are dropped [Ch15] [GE09].

AVTP uses IEEE 802.1Qav to provide guarantees for critical data streams. IEEE 802.1Qav defines two scheduling algorithms for critical and non-critical AVTP traffic. The first is the Strict Priority (SP) Selection, which is the default algorithm that is used to select non-critical data frames for transmission [Fi17] [IE16c]. The second is the Credit Based Shaper (CBS) Selection, which is used to select critical data frames for transmission. IEEE 802.1Qat is then used to police the use of bandwidth – it reserves network resources to ensure QoS requirements are met for critical data streams [Fi17] [IE16c]. Once a route is confirmed as suitable for traffic delivery, it is reserved/registered for the stream in question, and explicitly deregistered once it is no longer in use. Any unused bandwidth is used for BE traffic [IE16a] [AV13] [TF13]. In OPC UA/TSN, IEEE 802.1Qbv provides the scheduling services. Network access is granted per traffic class, so that only one traffic class can have access to the network at any one time. This process uses a precise schedule, and communication is at a fixed repetitive cycle [IE16c] [IE17]. IEEE 802.1Qcc provides traffic policing services – it considers the needs of professional, consumer, automotive and industrial markets, therefore, additional streams reservation classes are considered [IE17] [ZK17].

PROFINET controls traffic flow through reserved link capacity for IRT data that is sent according to a predefined cyclic schedule. The rest of the data (both RT and non-critical data) is sent after the IRT data. The switches have separate queues for RT data and non-critical data, RT data has higher priority and is sent first in a bus cycle [Fr09]. The design of the schedule of time slots for cyclic data is part of the system design and is later stored in the components of the system. The first part of a bus cycle is reserved for class 3 IRT data. The rest of a bus cycle is used to transmit class 2 and class 1 RT telegrams and non-critical TCP/IP data. Here, priority tagging according to IEEE 802.1Q is used to distinguish between high-priority and low-priority telegrams. The system ensures that that transmission of data is completed at the end of a bus cycle [Fr09]

[HM17]. PROFINET can be used in a switched network, but it does not define services at the switch. As such, traffic policing becomes the responsibility of the network nodes.

5 Discussion and Conclusion

Based on the comparative evaluation (summarized in Table 1) TSN sub-standards, TTE and PROFINET provides defined, inclusive traffic categorization, which consider time-critical to best effort traffic. With AFDX, traffic is not defined in this manner, but can be implemented through strategic customization of the VLs and subVLs. Regarding time synchronization, in addition to bounded latency, this allows for more accurate transmission in AVTP, TTE and PROFINET. AFDX uses solely bounded latency, but this difference does not make AFDX any less competitive in supporting real-time operations. In fact, as bounded latency is not selectively applied in AFDX (as opposed to the others), deterministic throughput can be guaranteed for all traffic streams. As it concerns traffic shaping, the use of more than one traffic-shaping algorithm in the selected standards presents an opportunity for optimal resource management. The additional support as provided by the traffic policing mechanisms serve to make the network more robust. However, there is concern about the use of pre-emptive algorithms in TTE, as this can result in wasted bandwidth and unchecked delays of low priority traffic. Also, the traffic shaping mechanism at the sending End System in an AFDX network, indicates that all traffic will experience uniform delay, which runs counter to expectations for special treatment of high priority traffic. Finally, the absence of traffic policing definition in PROFINET may result in wasted bandwidth. In that, faulty traffic might use considerable network resource before being detected by a network node. However, as a PROFINET/TSN was recently announced [PI17], this presents an opportunity for TSN traffic shaping mechanisms to be deployed to compensate for this unfavourable service.

The overall CPS requirements can be supported by AFDX, TTE, PROFINET and AVTP. This paper discusses some of the strengths and weaknesses of these standards, to demonstrate their readiness for next generation CPS. Consideration must be given to a mixed implementation of these Ethernet technology, which may be an advantageous strategy, as opposed to reliance on a single standard. Additionally, whilst TTE, AFDX, PROFINET and AVTP are compatible with Ethernet, an open and globally accepted standard, this does not translate to interoperability – an important feature for I4.0. OPC UA has already been identified as the premier standard for I4.0 system interoperability and has been tested to demonstrate its compatibility with TSN [BR16] [Av14]. In fact, to ensure its compatibility and to cement its footing in I4.0 and IIoT infrastructures, OPC UA was extended to provide a publisher/subscriber model, which is more suitable for such large architectures. It is this version of OPC UA that is used in OPC UA/TSN [BR16] [Av14]. TTE, AFDX, PROFINET and AVTP will also require more tangible comparison, such as through performance comparison that is driven by test cases. These test cases must include testing under similar conditions, such as similar scheduling

constraints, timing/latency requirements and network load. These test cases will serve to further demonstrate the suitability of these time-sensitive technology for CPS, and the proposed use of a diverse communication technology infrastructure.

Standard	Traffic Categorization	Traffic-Shaping	Traffic-Policing	Time Synchronization and Bounded Latency
ARINC 664 Part 7: AFDX	Customizable through VLs and subVLs	Chosen policy at End System; Token bucket and FIFO at the switch	Checks for network allowance and frame format compliance. Checks for unexpected and duplicated traffic.	No time synchronization defined. Upper (500µs) and lower bounds for latency is defined for all traffic.
AVTP	4 types defined	Strict Priority Selection and Credit-based Shaper	Checks for network allowance compliance.	gPTP for time synchronization. Bounded delay enforced for time-critical traffic.
PROFINET	3 types defined	Reserved link capacity for IRT data	Undefined. Provided by nodes.	PTCP for time synchronization. Bounded delay is based on traffic type.
TTE	4 types defined	Chosen strict priority and non-preemptive algorithms	Checks for network allowance compliance. Checks for unexpected traffic.	Time synchronization is defined. Bounded delay enforced for TT and RC traffic.

Tab.1. Summary of services offered by Time-Sensitive Ethernet specifications.

Acknowledgements

Some of the addressed cybersecurity related topics are being elaborated as part of AREVA GmbH's participation in the "SMARTEST" R&D (20152018) with German University partners, partially funded by German Ministry BMWi.

Bibliography

[AE17] Aberdeen Essentials: Industry 4.0 and industrial IoT in manufacturing: a sneak peek, http://www.aberdeenessentials.com/opspro-essentials/industry-4-0-industrial-iot-manufacturing-sneak-peek/, accessed: 16/11/2017.

[AR09] Aeronautical Radio Inc (ARINC): Specification 664: aircraft data network, part 7 – deterministic networks.

[AR15] ARC Advisory Group: How Profinet and industrie 4.0 enable information-driven industries, https://www.phoenixcontact.com/assets/downloads_ed/global/web_dwl_promotion/EN_PROFINET_und_Industrie_4_0_ARC_White_paper_LoRes.pdf, accessed: 16/11/2017.

[AV13] AVnu Alliance Broadcast Advisory Council: How big do my pipes need to be? – traffic shaping & infrastructure planning, http://avnu.org/wp-content/uploads/2014/05/AVnu-AABAC_Traffic-Shaping-Infrastructure-Planning_Andre-Fredette.pdf, accessed: 16/11/2017.

[Av14] Avnu: OPC UA TSN achievements from combined IT-OT leader investment, http://avnu.org/wp-content/uploads/2014/05/SPS-IPC-Joint-Press-Release-FINAL.pdf, accessed: 16/11/2017.

[Be16] Belden: The changing face of future automation networks, http://www.pressreleasefinder.com/Belden/BLDPR442/en/, accessed: 16/11/2017.

[BR16] B&R Automation: OPC UA TSN – field-tested, field-proven, https://www.br-automation.com/smc/e19f6c3e6ebdf58307c92f8a2f1a56b2cb6f3207.pdf, accessed: 16/11/2017.

[Ch15] Chaudron, J.: TTEthernet theory and concepts, http://etr2015.irisa.fr/images/presentations/TTEthernet_ETR_2015_Rennes.pdf, accessed: 16/11/2017.

[Fi17] Finn, N.: Time-sensitive and Deterministic Networking Whitepaper, https://mentor.ieee.org/802.24/dcn/17/24-17-0020-00-sgtg-contribution-time-sensitive-and-deterministic-networking-whitepaper.pdf, accessed: 06/12/2017

[Fr09] Frank, H.: Industrielle kommunikation mit Profinet – hochschule Heilbronn, https://www.hs-heilbronn.de/1749571/profinet, accessed: 6/12/2017.

[GE09] GE Fanuc: TTEthernet – a powerful network solution for advanced integrated systems, https://bcourses.berkeley.edu/files/66071161/download?download_frd=1&verifier=wt3Ass5zlL3xWAIaWeTTBxZKQt2KKVeOChJzXh5r, accessed: 16/11/2017

[Gr17] Greenfield, D.: Automation networks: from pyramid to pillar, https://www.automationworld.com/automation-networks-pyramid-pillar, accessed: 16/11/2017.

[HM17] Heitzer, B., Mottok, J.: Real-time behaviour of Ethernet on the example of PROFINET, https://www.hs-regens-burg.de/fileadmin/media/fakultaeten/ei/forschung_projekte/MAPR_Ver%C3%B6ffentlichungen/ARC_Heitzer.pdf, accessed: 6/12/2017.

[IE13] IEC 61850-1 Communication networks and systems in substations – Part 1: Introduction.

[IE16a] IEEE 1722-2016: IEEE standard for a transport protocol for time-sensitive applications in bridged local area networks.

[IE16b] IEC 62451-1 OPC unified architecture – part 1: overview and concepts.

[IE16c] IEEE: 802.1Qbv - Enhancements for scheduled traffic, http://www.ieee802.org/1/pages/802.1bv.html, accessed: 6/12/2017.

[IE17] IEEE: 802.1Qcc - Stream reservation protocol (SRP) enhancements and performance improvements, http://www.ieee802.org/1/pages/802.1cc.html, accessed: 6/12/2017.

[In10] Intech: Analysis of switched Ethernet for real-time transmission,

https://www.intechopen.com/books/factory-automation/analysis-of-switched-ethernet-for-real-time-transmission, accessed: 16/11/2017.

[In14] Innovasic, Inc.: Profinet RT vs. Profinet IRT, http://www.innovasic.com/news/industrial-ethernet/profinet-rt-vs-profinet-irt/, accessed: 16/11/2017.

[IS17] I-Scoop: Industry 4.0: the fourth industrial revolution - guide to Industrie 4.0, https://www.i-scoop.eu/industry-4-0/#The_building_blocks_of_Industry_40_cyber-physical_systems, accessed: 16/11/2017.

[KH17] Kleineberg, O. and Hummen, R.: Time-sensitive networking (TSN) and cyber security: will TSN make my automation network less secure? (webinar), accessed: 27/7/2017.

[MG14] Ming, L., Guang, L.: Analysis of the PROFINET IO protocol. In: 4th International Conference on Instrumentation and Measurement, Computer, Communication and Control, pp. 945-949, 2014.

[PI17] PI: Integration of TSN in PROFINET makes great strides, https://www.profibus.com/newsroom/news/integration-of-tsn-in-profinet-makes-great-strides/, accessed: 6/12/2017.

[PR11] PROFIBUS & PROFINET International: PROFINET IO conformance classes – guideline for PROFINET IO, https://www.profibus.com/download, accessed: 6/12/2017.

[PR17] PROFIBUS & PROFINET International: Profinet industrial Ethernet for advance manufacturing, http://us.profinet.com/technology/profinet/ accessed: 16/11/2017.

[TF13] Teener, M., Fredette, A., Boiger, C., Klein, P., et. Al: Heterogeneous networks for audio and video using IEEE 802.1 audio video bridging. In: IEEE 101 (11) pp. 2339 – 2354, 2013.

[TT17] TTTech: IEEE TSN (Time-Sensitive Networking): A deterministic Ethernet standard, https://www.tttech.com/technologies/deterministic-ethernet/time-sensitive-networking/.

[Ve10] Verwer, A.: Overview and applications of PROFINET, http://www.profibus.com/uploads/media/pxddamkey[9234]_FA_2010_Oct_3_Introduction_to_PROFINET_PeteBrown.pdf.

[WS17] Watson, V., Sassmannshausen, J., Tellabi, A., and Lou, X.: Interoperability and security challenges of industrie 4.0. In Proc. 47th Jahrestagung der Gesellschaft für Informatik e.V. (GI) Chemnitz, pp. 973-985, 2017.

[ZK17] Zuponcic, S. and Klecka, R.: TSN Influences on ODVA Technologies: IEEE-802.1, Avnu, IETF. In: Industry Conference & 18th Annual Meeting, 2017.

Secure Interoperability of I&C and IT systems

Mithil Parekh[1], Yuan Gao[2], Asmaa Tellabi[3] and Karl Waedt[4]

Abstract: End-to-end networking across all levels represents a challenge to communication of Instrumentation and Control (I&C) system in Nuclear Power Plant (NPP) [IE15b]. OPC-unified architecture (OPC-UA) provides users with security, reliability, compatibility and portability in end-to-end communication [IE16a]. From an end-user perspective, a uniform platform that enables direct embedding of products into the current infrastructure, without the need for any additional components, is required. An OPC-UA can be dispensed completely, without the need for additional drivers or infrastructures. For an example, SIPLUG®, monitoring instruments for electric drives, is integrated with OPC-UA sensors. The solution is used in the nuclear industry for monitoring critical systems in remote environments, without affecting the availability of the system. Earlier, SIPLUG® utilized a proprietary data exchange protocol, similar to most of the applications in the nuclear energy sector – which results, however, in a difficult integration into existing facility infrastructures, and the outlay for various aspects, such as data buffering or data analyses, always linked with extra costs. Therefore, with an open and international standard (IEC62541) – the challenge of "end-to-end data availability" can potentially be solved with OPC-UA [IE16a]. Moreover, in current generation NPPs, considering the time and budget limitations, commercial-off-the-shelf (COTS) products are also involved. At this point, OPC-UA will have potential benefits over Modbus protocol, which is popularly supported by industrial components due to its widespread use. However, in the Modbus protocol, there is a fair amount of variation in the protocol itself and in its physical layer definition, which creates problems in multi-vendor applications. OPC-UA enables integration between various layers of the automation pyramid, from sensor up to the ERP system. This is an efficient and simple method for raising systems to the next level of industrialization and making them fit for nuclear industry applications.

Keywords: OPC-UA, I&C System, HMI, Security.

[1] Otto-von-Guericke University Magdeburg, Research Group Multimedia and Security, Universitätsplatz 2, 39106 Magdeburg, mithil.parekh@ovgu.de
[2] Otto-von-Guericke University Magdeburg, Research Group Multimedia and Security, Universitätsplatz 2, 39106 Magdeburg, yuan.gao@ovgu.de
[3] University of Siegen, Faculty of Science and Engineering, Chair for Data Communication Systems, Hölderlinstraße 3, Siegen, 57068, asmaa.tellabi@student.uni-siegen.de
[4] Framatome GmbH, Henri-Dunant-Str. 50, Erlangen, 91058, karl.waedt@framatome.com

1 Introduction

The trend at the Office-IT layer, as well as in parts of the Operations layer in NPP, is towards open interfaces and service-based technologies [IE16a]. Applications at the higher level are concerned with consolidating information from different sources, putting it together into reports, and summarizing those into key performance indicators and other decision-support metrics. Therefore, it is important that there is an easy access to the all fundamental sources to permit combining and evaluating data through many functions and applications. Early assumption is that OPC-UA will be the protocol of choice for incorporating the Office-IT layer with Control-level protocols such as Modbus. OPC-UA provides a rich information model and standardized messaging, and also permits interoperability between the different event-processing and automated evaluations applications. Also, any cross-enterprise management system must be scalable and secure. All aspects of the OPC-UA requirements have been created not only with robust security but also with a wide range of scalability considerations.

Apart from interoperability, security is an important aspect [IE16]. Due to the budget restrictions, COTS have highly involvement in I&C system [IE11] [IE16]. So, security would relate to the communication between various systems provided by vendors. Security has many additional aspects and these should also be considered when deploying a system [Vw17].

Security aspects include e.g. encryption and signing of data transferred between two systems. Other security aspects are the identification of applications (server and client), the authentication and authorization of the user of the client application, the transmission of data through firewalls and auditing [OP17]. When considering security, it is important to also take into account the environment where the applications will be executed. Applications could run in a Windows domain, a windows user group, on a standalone machine or in a mixed operating system environment.

2 OPC-UA – The Perfect Unification

Communication standards, such as IEC 62541 (Open Connectivity Unified Architecture (OPC UA)) and IEC 61850 (Communication Networks and Systems in Substations), are used to facilitate interoperability. Because all protocols when boiled down to the basics represents moving data between applications, there are those that want to elevate one protocol to replace all others. Already there are many discussions and forums pushing one protocol versus another. The reality is OPC-UA is not designed to replace every protocol at all levels of the enterprise. What OPC-UA does aim to do is provide interoperability to all levels, which means it will counterpart application-level protocols and other industry-specific standards, including ‘classic’

OPC and Modbus. So, OPC-UA is designed to unify and enhance the power of existing applications and protocols [BM16]. In addition to interoperability, IEC 62541 addresses the security of data exchanges.

3 Example: General Architecture of I&C System

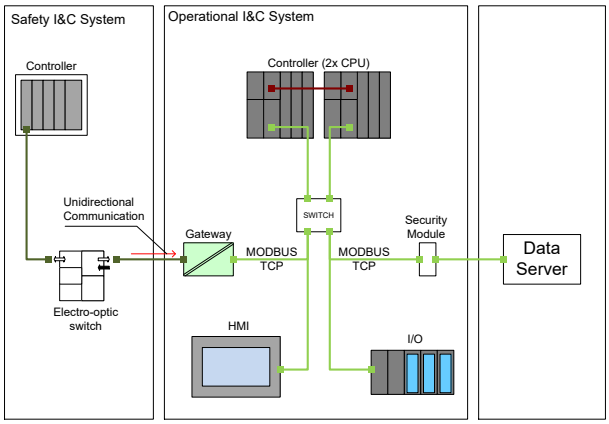

Fig. 1: General Architecture Of I&C System.

As indicated in Fig. 1, the information provision of relevant process control signals is carried out with the process data and information system DATA-SERVER. For data transmission from the control system, the MODBUS TCP protocol is used for DATA-SERVER. The example presented here, is partly following Public Reference Architecture (PRA) derived in [Rc16]. The control system is divided into two parts, consisting of an Operational I&C system classified according to IEC 61226 in Cat-C and a Safety I&C system classified in Cat-A [Yg16] [Kw15].

In this example, an Operational I&C is built with the process control system and contains redundant (two channels) devices in the control cabinets. Both channels of the control system communicate with the DATA-SERVER via the MODBUS TCP protocol. An intervening security module acts as a firewall and protects against unauthorized access to the control technology.

Here, the Safety I&C system does not support the MODBUS TCP protocol. Therefore, a gateway is required. The gateway receives the telegrams of the Safety I&C system and provides the data via the unidirectional MODBUS TCP protocol, for read-out by the redundant controller in operational I&C system, which transfers the data to the DATA-SERVER [Kw16][KD16]. The unidirectional connection consists of an Electro-optical switch, to physically prevent the interaction of the Operational I&C to the Safety I&C system [IE11] [IE13].

The MODBUS TCP protocol is a communication protocol based on client-server architecture. The following security aspects are considered while configuring a system:

1. Since the Safety I&C system does not support direct MODBUS communication, a gateway (Hardware + Software) is required.
2. Unidirectional data transmission from Safety I&C system to Operational I&C system.
3. Restricted authorized access to Operational I&C system from DATA-SERVER.

4 Embedded Security in OPC-UA

From the example above, this section will show how security measures are being incorporated by default to the system using OPC-UA. OPC-UA contains some of the most common aspects of Security. Security aspects include encryption and/or signing of data that is being transmitted between two systems, the identification of applications (server and/or client), the authentication and authorization of the user of the client application, and the transmission of data through firewalls and auditing. When considering security, it is also import to consider the environment in which the applications are executing [IE10].

OPC-UA has a specification (Part 2) that describes security threats and attacks and ways the OPC-UA standard is designed to mitigate these threats and attacks. Furthermore, OPC-UA has security-related functionality included throughout the 13 part specification. OPC-UA as a standard is not tight only to a single communication transport or operating system. Thus, it defines security at a layer above the transport. This ensures that as new transports are added security will be maintained. Other transports may add an additional layer between TCP and OPC-UA. The security aspects of OPC-UA were designed to be easily advanced as security standards further develop

without making alterations to applications. It was also modelled and made use of current best practices in security. Overall, OPC-UA has security abilities.

5 Encryption and signing of the data flow between systems

In our example, restricting unauthorized access from DATA-SERVER to Operational I&C system, is one security aspect. The functionality in OPC-UA which is the signing of the data flow (message) ensures that no one can change what is sent and received. It requires the creation of a cryptographic signature that can be simply recreated by the receiver of the message. If something has been altered, the receiver will not receive the same signature and can confirm the message has been modified. Encrypting includes signing to the next level and only the recipient can even read what is in the message. It uses a cryptographic translation of what is in the message, so that only the receiver has the required information to decrypt the message.

In OPC-UA, the default transport options have Signing and Encryption allowed. Here, configuration in controller can choose which communication options are available to DATA-SERVER to use for connection. Therefore, all Certified Servers and Clients are required to support this security aspect and it is provided by stacks and tools that are used to develop the application. The configuration only has to be performed on controller and DATA-SERVER only has to select which of the available communication option to make use of. Since OPC-UA was built for multiple platforms, comparable methodology can be applied for communicating between Operational and Safety I&C system. This functionality does not modify for domain-based, work groups or multiplatform-based applications.

6 Identification and securing applications

For the communication among Safety I&C system, Operational I&C system and DATA-SERVER, it is necessary to ensure that an application is communicating only with appropriate applications, e.g. no man in the middle or rogue server or client or that the given client is only communicating with an approved server and the server is responding only to an approved client [IE06]. This goes beyond restricting what a

user/application does, since it controls which application occurrence are allowed to communicate with other applications [IE10].

In OPC-UA, this functionality is provided by default. All applications are required to support this functionality to be certified in software. The same application installed on two different controllers can be configured with different access rights. The access rights apply to clients as well as servers, so the same client installed on two different controllers can have different servers allowing access. For an example, a standard client that is installed on two HMIs (for two different areas in a plant) would have different lists of servers that they are allowed to connect to. This is accomplished in OPC-UA by the use of Certificates. All Applications have a distinctive certificate assigned to them and a trust list that specifies which other certificates (applications) are to be trusted (allowed). OPC-UA has announced Global Discover Service functionality (part 12) that makes deploying certificate much easier.

6.1 User access rights

When a plant is in operation, different operators (users) are given different process execution. This is the restriction of what items in a controller (as a server) can be accessed and in what method they can be accessed (read/write/browse) by a given user (via HMI, as a client) [Mp16]. For an example, is the user allowed to read values, write values, browse the address space, etc. This authorization of access indicates that the user has been acknowledged and authenticated. The client (HMI application) must provide credentials to the controller acknowledging the user that is executing the application. User Access restrictions can be very wide e.g. it can apply to the entire controller or can be specified down to individual item in a controller. User access can also be ignored and could be configured for anonymous access.

In OPC-UA, three options for acknowledging a user exist e.g. a user account and password, Kerberos tokens or certificates. All applications must support Username/password, which is the easiest to apply, but it could require more work to configure e.g. it must be configured on each application. Kerberos is a standard method of exchanging user identities without exchanging passwords. It is supported by windows domains and easily implemented in an environment that has a Kerberos token server. Certificates are an easy extension of OPC-UA, since the certificate handling is already required for identification of applications. The selection of which manner of identifying

user is application specific. Once the user is acknowledged and authenticated, the application can restrict the access rights for a given user with respect to read/write browse etc.

6.2 Firewall

In our example, security module is used in systems to protect controller in Operational I&C system. Its role is also to restrict access points from intrusion (from DATA-SERVER). Furthermore, security module restricts the types of connection that are allowed, the ports to which connection are allowed and the communication protocols allowed. They are becoming mandatory in most systems to ensure security.

OPC-UA defines a fixed port or ports for a communication channel. The actual port is established by the endpoint(s) and protocol(s) exposed by the server. The HTTP protocol can run over the default port 80, which is rarely blocked. Client (here DATA-SERVER) initiate all communication so no out bound communication. The fixed ports and client initiated communication result in very easy firewall configuration. The OPC Foundation configuration tool (depending on the firewall being used) performs this configuration.

7 Case Study : SIPLUG® [OP17]

We have seen till now, OPC UA is suitable option for secure interoperability within I&C system, and for communicating with Office-IT equipment. Irrespective of the platform, application or communication protocol used for a component, replacement or later integration to I&C system is made possible with OPC UA. AREVA's product, as a fitting example, is a valve monitoring device (SIPLUG®), which is available for an uncomplicated integration to I&C system in NPP.

SIPLUG® takes measurements of the current and voltage used by a valve's actuator motor to assess the condition of the valve. This information is used for proof of operability of the system, which is a requirement in the nuclear power industry as well as other regulated industries.

Product developers have realized a number of key benefits from implementation of the OPC UA Embedded Server Software Development Kit (SDK). From an end user perspective, native UA connectivity allows products to be tied directly into infrastructure without the need for additional components. The small OPC UA embedded SDK also meets organization's requirements from a supplier standpoint. Its applicability to the nuclear context is demonstrated by AREVA. Realizing the potential of OPC-UA in sensors, AREVA started integrating these into monitoring instruments (SIPLUG®) for mountings and their associated electric drives.

7.1 Challenges

SIPLUG® is used in the nuclear market for remote critical system monitoring without impacting the system availability. As with most nuclear applications, the SIPLUG® traditionally relied on a proprietary communications protocol, making it more difficult to integrate with already existing plant infrastructure utilized for everything from data buffering to data analysis.

7.2 Shifting to a new solution

It was required to find a solution, making it possible for their reporting package and historian to access the SIPLUG® data directly. This would eliminate the need for additional drivers and infrastructure. Additional signals such as pressure and temperature available at plant floor level can be easily used to increase the accuracy and pertinence of the data evaluation. OPC UA embedded brings native OPC connectivity down to the sensor, controller and device level and hence makes integrated enterprise a reality for the end users.

Furthermore, due to today's growing emphasis on secure connectivity, organizations always deliver the highest levels of security in its products to respond to potential attacks on the infrastructure. Having OPC UA run in their devices natively to secure the data connectivity is well aligned with product's requirements. As mentioned earlier, OPC UA has a standard, state of the art security model built in for each OPC UA applications. It improves developers' confidence deploying UA enabled products and also enhances interoperability.

8 System modelling based on companion specification

Presented here is the discussion about possible I&C System Modelling (see Acknowledgement), which covers operations as well as security aspects. Plant level, process engineering and high-level I&C aspects can be described for e.g., by using AutomationML. With this model, an opportunity from combining AutomationML and OPC-UA is the ability to communicate and operationalize AutomationML by means of OPC-UA [OP17]. It is possible to simplify the creation of OPC-UA information models based on existing AutomationML data [IE16a]. This can be realized by a so-called OPC-UA companion specification due to analogies between AutomationML and the OPC-UA information model. The companion specification for AutomationML consists of an object model including many specific semantics which can be used online with multiple involved parties by OPC-UA, making an online version of the AutomationML model possible - AutomationML models can be exchanged via OPC-UA – and including OPC-UA data management, online communication functionality, multi-user support, access methods, security, etc. This is especially important for re-engineering and maintenance use cases where the AutomationML model evolves over time [Mp16]. The present AutomationML model can be managed by OPC-UA and makes an up-to-date description of the system as-is possible.

Conclusion

As industry standards evolve and strengthen those with wide adoption and proven interoperability will continue down the road of enterprise integration while others will fade into obscurity. OPC-UA fulfils the requirements of advanced digital industry and industrial networks which must meet ever-increasing demands. It also provides convergent, end-to-end, secured networks that are flexibly scalable, dynamically adaptable, and able to accommodate large numbers of I&C system components, with the fastest possible response times. Further, we saw by an example, how expensive and sophisticated hardware and software can be replaced by variety of functionalities from OPC-UA. Additionally, SIPLUG®, already available in the nuclear market, takes advantages of OPC-UA as an ease of integration and reliability.

New generation I&C system in NPP will certainly include COTS component in order to meet ever increasing competitive market. Therefore, system modelling is

essential to describe system architecture while OPC-UA and COTS are in use. Extension of existing modelling of I&C system with a selection of COTS, protocols (OPC-UA) and standards is the part of future work. The key is choosing well-established, complementary protocols like OPC-UA that offer the best interoperability options.

Bibliography

[IE15b] IEC 62541-2 OPC Unified Architecture – Part 2: Security Model.

[IE16a] IEC 62451-1 OPC Unified Architecture – Part 1: Overview and Concepts.

[Vw17] Venesa, W. et.al.: Interoperability and Security Challenges of Industrie 4.0, GI, Chemnitz, Germany, 2017.

[OP17] OPC Foundation: Unified Architecture: Interoperability for Industrie 4.0 and the Internet of Things,opcfoundation.org/wp-content/uploads/2016/05/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN-v5.pdf, accessed: 22/07/2017.

[Rc16] Robert, C. et.al.: Proposal for a Public Reference Architecture for Vulnerability Testing in Nuclear Power Plants, IAEA International Conference on Nuclear Security: Commitments and Actions, Vienna, 2016.

[Yg16] Yuan, G. et.al.: Cybersecurity Modelling for Nuclear Facilities: Interactions between System Specifications and Security Controls, IAEA International Conference on Nuclear Security: Commitments and Actions, Vienna, 2016.

[Kw16] Karl, W. et.al.: Nuclear Safety and Risk based Cybersecurity Testing, 47th Annual Meeting on Nuclear Technology, Hamburg, 2016.

[Mp16] Mithil, P., et.al.: Cybersecurity during Plant Operation, 42ª SNE annual meeting, Santander, 2016.

[KD15] Karl, W.; Y. Ding, Safety and Cybersecurity Aspects in the Safety I&C Design for Nuclear Power Plants, Shanghai, 2015.

[Kw15] Karl, W. et.al: I&C Modeling for Cybersecurity Analyses, 1st TÜV Rheinland China Symposium – Functional Safety in Nuclear and Industrial Applications, Shanghai, October 2015.

[IE06] IEC 60880:2006, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.

[BM16] BMWi: IT-Sicherheit für die Industrie 4.0 - Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten - Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, 2016.

[IE11] IEC 61513:2011, Nuclear power plants - Instrumentation and control important to safety - General requirements for systems

[IE16] IEC 62859:2016, Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity

[IE10] IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," in IEEE Std 7-4.3.2-2010 I (Revision of EEE Std 7-4.3.2-2003) , vol., no., pp.1-82, Aug. 2 2010.

[IE13] IEC 62443-3-3, 2013, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.

[IE10] IEC 61508-4:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems

Welches Veränderungspotenzial weist die Blockchain-Technologie für die Branche Logistik auf?

Eine fallstudienbasierte Untersuchung

Stefan Tönnissen[1] und Frank Teuteberg[2]

Abstract: Der Blockchain wird häufig das disruptive Potenzial zugesprochen, bestehende Geschäftsmodelle zu verändern und vorhandene Intermediäre überflüssig zu machen. Seit dem Start des Bitcoins hat sich die Blockchain-Technologie verbreitet und etabliert, so dass heute zahlreiche Anwendungen auf Basis dieser Technologie entstanden sind. In der Branche Logistik werden mit einem möglichen Einsatz dieser Technologie zahlreiche Vorteile wie z.B. die Erhöhung der Transparenz oder eine real time Verarbeitung in Verbindung gebracht. Weitgehend unklar ist bisher jedoch, ob diese Technologie zu einer Disruption der Geschäftsmodelle in der Branche Logistik führen könnte. Für die Beantwortung dieser Frage führen wir eine fallstudienbasierte Untersuchung von realen Fallstudien aus der Branche Logistik durch. Hierzu wenden wir ein Framework an, in dem wesentliche Merkmale einer disruptiven Innovation verbunden mit einer Analyse der Dimensionen eines Geschäftsmodells untersucht werden. Ein Ergebnis ist, dass die bisherigen auf der Blockchain-Technologie basierenden Anwendungen ein (bisher noch) vergleichsweise geringes Veränderungspotenzial innerhalb der Logistik aufweisen.

Keywords: Blockchain, Logistik, Disruptive Innovation, Erhaltene Innovation, Fallstudie.

1 Einleitung

Die Bundesvereinigung Logistik hat in ihrer Studie „Trends und Strategien in Logistik und Supply Chain Management“ 2017 die hohe Relevanz der Digitalisierung hervorgehoben. Demnach bleiben für die Supply Chain die wichtigsten Herausforderungen die Digitalisierung der Geschäftsprozesse bei gleichzeitiger Erhöhung der Transparenz. Des Weiteren wird in der Studie betont, dass die Blockchain eine disruptive Technologie ist mit dem Potential, bei einer ausreichenden technologischen Reife die Konzepte der Logistik grundlegend zu verändern [Ke17]. Diese bereits seit der Einführung der Bitcoins im Jahre 2009 vorhandene Technologie hat mittlerweile einen Reifegrad erreicht, der sie für viele Anwendungsfelder in der Praxis einsatzfähig macht. Die Blockchain wird in der aktuellen Literatur häufig als disruptive Technologie bezeichnet [Sw15], [No17], [Th17], [HPM17], mit dem Potenzial, etablierte Geschäftsprozesse zu zerstören [WC13], bisher bekannte Entwicklungsabläufe zu

[1] Universität Osnabrück, Unternehmensrechnung und Wirtschaftsinformatik, Katharinenstr. 1, 49069 Osnabrück, Deutschland, stoennissen@uni-osnabrueck.de
[2] Universität Osnabrück, Unternehmensrechnung und Wirtschaftsinformatik, Katharinenstr. 1, 49069 Deutschland, frank.teuteberg@uni-osnabrueck.de

unterbrechen, die Handlungsmöglichkeiten in Unternehmen abrupt zu verschieben [Kr17] sowie Geschäftsmodelle radikal zu verändern [DP17]. Martin Kolbe als CIO von Kühne + Nagel schreibt der Blockchain das Potenzial zu, die Supply Chains digitaler und effizienter zu machen und darüber hinaus die Entstehung von kollaborativen Geschäftsnetzwerken zu ermöglichen [Ko17]. Chavanne et al. (2017) bescheinigen der Blockchain das Potential, die bestehenden Lieferketten „entrümpeln“ zu können. Die Supply Chain Community sieht aktuell ein ernstes Interesse an der Blockchain-Technologie [Ma17]. Unklar ist bisher jedoch, wie groß das Veränderungspotenzial der Blockchain-basierten Anwendungen für die Branche Logistik wirklich ist und welche strategische Reaktion für die Marktteilnehmer die richtige ist.

In diesem Beitrag wird anhand von realen Fallstudien untersucht, zu welchen neuen (disruptiven) Geschäftsmodellen bzw. zu welchen Veränderungen bestehender Geschäftsmodelle die Blockchain-Technologie bisher in der Logistik geführt hat und welche Auswirkungen dies auf die jeweilige Branchenlogik haben könnte.

2 Grundlagen

2.1 Blockchain-Technologie

Die Blockchain-Technologie enthält zahlreiche Eigenschaften die geeignet sind, die Geschäftsmodelle und Geschäftsprozesse in der Logistik zu verändern. Hierzu zählt die Aneinanderreihung (Verkettung) von Daten, die zu einzelnen Blöcken zusammengefasst und auf allen Rechnern der Nutzer abgelegt werden [Sw15]. Diese Aneinanderreihung von Daten zu Blöcken ergibt eine sequentielle Abfolge, die wie eine Kette den Verlauf von Transaktionen widerspiegelt. Die Aufnahme eines neuen Datensatzes in die Blockchain erfordert den Durchlauf eines sog. Konsensmechanismus, der über das Netzwerk aller Teilnehmer läuft. Ein bekannter Konsensmechanismus ist der Proof-of-work, in dem die Miner in einem Blockchain-Netzwerk vor Aufnahme eines Datensatzes den Nachweis über den Aufwand zur Lösung eines mathematischen Algorithmus erbringen müssen [Sw15]. Zusätzlich zu den Daten enthält jeder Block einen Zeitstempel sowie den Hashwert des vorherigen Blocks. Die Datenblöcke sind mit Hilfe von kryptografischen Verfahren vor nachträglichen Veränderungen gesichert, so dass mit der Zeit eine lückenlose Kette von verbundenen Datenblöcken entsteht [No17]. Für die Nutzung einer Blockchain sind die beiden Arten „permissioned blockchain“ sowie „permissionless blockchain“ zu unterscheiden. Eine „permissionless blockchain“ ist eine öffentliche Blockchain ohne Zugangsbeschränkung, wie z.B. Bitcoin. Ein jeder Mensch auf der Welt kann mit Hilfe einer Software an dieser Blockchain teilnehmen. Dagegen wird in einer „permissioned blockchain“ die Möglichkeit zur Beteiligung restriktiv gehandhabt, in dem eine Zugangsberechtigung erforderlich ist. Diese Zugangsberechtigung wird durch einen Dritten vorgenommen [CR17].

2.2 Geschäftsmodelle

„Ein Geschäftsmodell beschreibt die Grundlogik, wie eine Organisation Werte schafft“ [BR11] und bildet die Geschäftslogik eines bestimmten Unternehmens oder einer Organisation ab [OPT05]. Es sind häufig vereinfachte Abbildungen der Realität mit der Beschreibung der wertschöpfenden Aktivitäten eines Unternehmens [Ve14]. Geschäftsmodelle bilden zum einen das Bindeglied zwischen den Geschäftstätigkeiten eines Unternehmens und der zugrundeliegenden Informationstechnologie, als auch zum anderen das Bindeglied zwischen der Strategie eines Unternehmens und den Geschäftsprozessen ab [Ve14]. In den letzten Jahren hat die Innovation von Geschäftsmodellen aufgrund der Vernetzung und Digitalisierung von (Service-)Prozessen und Dingen (Internet der Dinge, Industrie 4.0) zunehmende Aufmerksamkeit erlangt. Die digitale Transformation bezeichnet in diesem Zusammenhang eine Veränderung von Geschäftsmodellen verursacht durch neue Technologien [SR17]. Auf der Grundlage dieser Daten können neue datenzentrierte Geschäftsmodelle auf Basis der Blockchain-Technologie entstehen. Diese IT-basierten Geschäftsmodelle werden unterschieden in die Varianten Lizenzgeschäft, Lizenz plus Service sowie das Projektgeschäft [HJP10]. Das Lizenzgeschäft zielt auf eine große Kundengruppe als Massengeschäft ab mit einer Beschränkung der wesentlichen Eigenschaften des Produktes. Die unterschiedlichen Anforderungen der zahlreichen Kunden sollten hierbei über flexible Anpassungen des Produktes möglich sein. [HJP10]. In der Variante Lizenz plus Service wird ein Produkt, das nicht flexibel durch die Kunden konfigurierbar ist, mit einer Anpassungsdienstleistung durch den Hersteller angeboten. Hier wird also ein Standardprodukt individuell angepasst. Im Projektgeschäft wird das Produkt kundenindividuell im Rahmen eines Projektes entwickelt [HJP10]. Digitale Geschäftsmodelle sind nach Veit et al. (2014) „…überwiegend in Medien-, Handels-, Finanzdienstleistungs- sowie Logistikindustrien zu finden“. Diese digitalen Geschäftsmodelle auf Basis der Blockchain-Technologie können nach Rückeshäuser et al. (2017) in fünf verschiedenen Typen eingeteilt werden. Zunächst gibt es den Infrastrukturanbieter, dessen Angebot eine Infrastruktur in der Form einer Blockchain ist, ohne dass der Kunde jedoch weitere Funktionen dieser Infrastruktur nutzen könnte. Das hierbei übliche Vergütungsmodell ist ein Abonnement oder Miete des beanspruchten Speicherplatzes. Wird dem Kunden neben der Infrastruktur die Möglichkeit zur selbständigen Anpassung der Software angeboten, so spricht man von einem Plattformanbieter. Dieser erzielt seine Vergütung über ein Lizenzmodell oder einer Account-basierten Lösung sowie über eine Beratungsleistung. Für eine Integration der Infrastruktur in die Systemlandschaft des Kunden wird neben der reinen Infrastruktur auch die Implementierung angeboten. Neben einem Account- oder lizenzbasierten Vergütungsmodell wird ebenfalls eine Vergütung durch die entsprechende Beratung erzielt. Bei dem Angebot einer vollständigen Applikation wird von einem Applikationsanbieter gesprochen. Diese vollständige Applikation erlaubt es dem Kunden jedoch nicht, eigene Anpassungen vorzunehmen. Neben den Lizenzen und der Beratung sind hierbei vielfältige Vergütungsmodelle denkbar. Zu Letzt gibt es den Anbieter

komplementärer Services oder Produkte, der häufig als Informationsservice auftritt. Die Vergütung erfolgt über Revenue-Sharing bei Gemeinnützigkeit, sonst über Lizenzen und vergüteten Beratungsleistungen [RBM17].

Nach Stähler (2008) setzt sich ein Geschäftsmodell aus einem Nutzenversprechen, einer Architektur der Wertschöpfung und eines Ertragsmodells zusammen. Mit dem Nutzenversprechen geht eine Beantwortung der Frage einher, welchen Nutzen die Kunden aus einer Geschäftsbeziehung ziehen könnten. Die Architektur der Wertschöpfung folgt anschließend der Frage, wie der zuvor definierte Nutzen für den Kunden generiert wird. Zuletzt gilt die Frage zu beantworten, wie das Unternehmen mit dem Geschäftsmodell einen Ertrag generieren bzw. Geld verdienen will [St18]. Die Blockchain-Technologie hat das Potenzial, bestehende Geschäftsmodelle zu verändern, dies bedeutet, dass mindestens eine der drei Geschäftsmodell-Dimensionen nach Stähler (2008) durch die Einführung einer Blockchain-basierten Anwendung in der Logistik verändert wird.

Die der Blockchain zuvor zugeschriebene Disruption der Geschäftsmodelle ist ein Merkmal einer technologischen Innovation. Diese kann unterteilt werden in eine disruptive Innovation mit einer leistungsbezogenen Weiterentwicklung, sowie in eine erhaltene Innovation, bei der eine Verbesserung einer etablierten Technologie im Vordergrund steht. Sowohl disruptive als auch erhaltene Innovationen können inkrementeller oder radikaler Natur sein [We14]. Für eine Unterscheidung zwischen einer disruptiven technologischen Innovation und einer erhaltenen technologischen Innovation werden in Anlehnung an Albeck [Al16], Bower und Christensen [BC95], Druehl und Schmidt [DS08] und Govindarajan und Kopalle [GK06] die Merkmale Kunden, Produkt, Unternehmen, Performance, Preis, Markt, Gewinn, Veränderung und Kenntnisse herangezogen. Erhaltene Innovationen verbessern die bestehenden Produkte oder Leistungsangebote von bestehenden Unternehmen und zielen in den bestehenden Märkten auf die bekannten High-end Kunden ab [DS08]. Diese High-end Kunden sind bereit, für die verbesserten Leistungsmerkmale des bestehenden Produktes einen höheren Preis zu bezahlen und dem anbietenden Unternehmen damit einen höheren Gewinn zu ermöglichen [CR03]. In der erhaltenen Innovation werden die bestehenden Produkte oder Leistungen schrittweise in den traditionellen Funktionen verbessert [CR03]. Damit fällt es dem Kunden leichter, einen Überblick über die angebotenen Funktionen zu behalten. In den disruptiven Innovationen hingegen stehen deutlich verbesserte oder neue Produkte auf neuen Märkten im Fokus der anbietenden Unternehmen [CR03]. Aufgrund des andersartigen Leistungsversprechens des neuen Produktes verbunden mit einem geringeren Leistungsumfang als bestehende Produkte wird dieses Produkt zunächst zu einem niedrigen Preis an Low-end Kunden angeboten [BC95]. Die High-end Kunden sind nicht gewillt, das neue Produkt mit ihren bestehenden und bekannten Anwendungen zu nutzen [BC95].

Merkmale	Disruptive Innovation	Erhaltene Innovation
Kunden	Low-end Kunden	High-end Kunden
Produkt	Neues Produkt	Bestehendes Produkt
Unternehmen	Neue Unternehmen	Bestehende Unternehmen
Performance	Niedrige Performance	Hohe Performance
Preis	Niedriger Preis	Hoher Preis
Markt	Neue Märkte	Bestehende Märkte
Gewinn	Zunächst niedrige Gewinne	Hoch, Zahlungsbereitschaft der High-end Kunden
Veränderung	Eher radikal mit neuen Leistungen	Inkrementell, schrittweise Verbesserung
Kenntnisse	Kunden fehlt der Überblick über die Funktionen	Kunden haben einen guten Überblick über die Funktionen

Tab. 1: Merkmale für eine Disruption [Al16], [BC95], [DS08], [GK06].

2.3 Logistik und deren Branchenlogik

Mit der Logistik ist zunächst ein Dienst gemeint, der sich darum kümmert, dass „die richtige Ware zur richtigen Zeit am richtigen Ort“ zur Verfügung steht [De17]. Diese eher historische Auslegung des Begriffes greift jedoch heute zu kurz, da sich die Logistik „zu einem wesentlichen Treiber des digitalen und gesellschaftlichen Wandels entwickelt“ hat [De17]. Mit der heutigen Logistik werden alle unternehmensinternen und unternehmensübergreifenden Güter- und Informationsflüsse geplant, gesteuert und durchgeführt [De17]. Die Intralogistik als unternehmensinterne Logistik bezieht die innerbetrieblichen Material- sowie Informationsflüsse ein. Aufgrund einer häufig vorhandenen räumlichen und zeitlichen Verteilung von Produktion, Beschaffung, Lagerhaltung und Vertrieb sind logistische Dienstleister wie z.B. Spediteure, Transportunternehmen, Lagerunternehmen etc. in den logistischen Prozessen zwischen Versender und Empfänger eingebunden [De17]. Eine weitere Aufgabe der Logistik ist

daher das Management der Zusammenarbeit zwischen den am Prozess beteiligten Akteuren. Hierbei sind strukturelle Muster durch Aggregationen von mehreren Akteuren sowohl durch horizontale als auch vertikale Kooperationen entstanden [De17]. Zur Logistikbranche gehören üblicherweise zunächst die Spediteure, Transport- und Verkehrsunternehmen. Daneben treten Logistikserviceprovider auf, die sich um das Management einer kompletten Supply Chain kümmern [Wk17].

3 Fallstudien

Für die Beantwortung unserer Forschungsfrage führen wir eine qualitative Forschung durch die Analyse von Fallstudien durch. Die Fallstudienforschung ist in der qualitativen Forschung im Bereich von soziotechnischen Informations- und Kommunikationssystemen weit verbreitet [Re13] und kann Einsichten liefern, die mit anderen Methoden nicht erreicht werden könnten [Ro02]. Mit der Fallstudienforschung werden empirische Untersuchungen an realen Phänomenen im wirklichen Leben durchgeführt [RSC15], [Re13], anstatt in einem Labor oder Experiment [Ro02], [EG07]. Die wesentlichen Stärken der Fallstudienforschung sind, dass informationssystem-relevante Phänomene in ihrer natürlichen Umgebung studiert werden und aus dieser Sicht der Praxis neue Theorien entwickelt sowie bestehende Theorien erweitert werden können [Re13].

Für die Sicherstellung einer höheren Aussagekraft unserer Forschungsergebnisse führen wir eine multiple Fallstudie durch, da mit der Zunahme der Anzahl der Fälle die Ergebnisse robuster werden [Ro02] sowie eine stärkere Basis für den Aufbau von Theorien gebildet wird [Yi94]. Für die Theoriebildung aus der Fallstudienforschung ist die Auswahl der Fallstudien eine bedeutende Herausforderung [EG07]. Jedoch ist zunächst zu berücksichtigen, dass die Auswahl von Fallstudien auch von pragmatischen und logistischen Gründen geleitet wird [SG08]. Die Durchführung einer multiplen Fallstudie wirft ebenfalls die Frage nach der richtigen Anzahl der Fälle auf. Für Rowley (2002) sind 6-10 Fallstudien typisch.

Wir haben eine Suche über Google mit dem Suchstring: („blockchain and logistic" OR "blockchain and „Supply Chain“) and ("case study" or "Use case") für den Zeitraum 01.01.2017 - 31.12.2017 durchgeführt und 7060 Treffer erhalten. Anhand unserer Annahme, dass die Ergebnisse der ersten Seiten die Relevanz aufgrund der Suchalgorithmen von Google widerspiegeln [Go17], haben wir anhand der Titel und Kurztexte eine Analyse der Ergebnisse vorgenommen. Wir haben die Fallstudien dahingehend untersucht, ob anhand der Angaben im Titel oder Kurztext ein Beitrag zu unserer Forschungsfrage zu erwarten ist [RSC15]. Des Weiteren haben wir bei der Auswahl der Fallstudien auf eine breite Auswahl geachtet, um eine hohe Variation der Fälle zu erhalten [RSC15]. Eine weitere Voraussetzung an die Fallstudien ist, dass sie die Konzeptphase bereits hinter sich gelassen haben sollten und entweder als Prototyp im Testeinsatz oder sich im produktiven Einsatz befinden. Damit stellen wir eine empirische Untersuchung an realen Phänomen sicher [RSC15]. Unser Ergebnis der Falllstudien

Auswahl sind 10 Fallstudien aus den Bereichen Logistik und Supply Chain Management, Lebensmittelhandel und -transport, Einzelhandel allgemein, Einzelhandel für Pharmazie sowie Einzelhandel für Diamanten im Besonderen.

3.1 Beschreibung der Fallstudien[3]

Ocean Fright [1] ist eine Anwendung für die Digitalisierung und Automatisierung von internationalen Container Transporten über den Seeweg [Pe17]. Die IBM hat in Kooperation mit MAERSK einen Prototyp entwickelt. Die Anwendung **Agri-digital** [2] verbindet Warenlieferungen mit Zahlungsvorgängen und bietet eine hohe Transparenz über Lieferketten [Ag17]. Die Anwendung befindet sich zum Abschluss einen Prototyp, der sich bereits im Piloteinsatz befindet. Mit **Agri-food** [3] befindet sich eine Anwendung im proof-of-concept Piloten, die mit Hilfe von RFID und der Blockchain ein Rückverfolgungssystem über die gesamte Lieferkette bietet. Mit **Animal product** [4] gelingt die Identifizierung von tierischen Produkten mit einer lückenlosen Lieferkette und der Rückverfolgungsmöglichkeit [MBP17]. Das Unternehmen Provenance hat das Konzept in einer Blockchain Anwendung umgesetzt. Mit **Cognizant Retail** [5] bietet das Unternehmen Cognizant eine blockchain-basierte Anwendung für den typischen Einzelhandel an [WHC17]. Mit **OpenBazaar** [6] ist ein elektronischer Marktplatz für den Handel mit Waren und Services auf Grundlage einer Blockchain produktiv [Op17]. **Origin Tracking** [7] ist eine Anwendung, die als Hauptbuch für die Lebensmittelverfolgung fungiert und eine Integration in bestehende IT-Systeme anbietet [Pe17]. Die Anwendung wird von origintrail angeboten und befindet sich bei Walmart im produktiven Einsatz. Der Konzern Imperial setzt **CargoChain** [8] innerhalb des Konzerns als produktive Lösung zur Digitalisierung des Transportmanagements ein [Im17]. Für LifeCrypter [9] hingegen gibt es bisher nur einen Prototyp. **LifeCrypter** ist eine Anwendung zur Erfassung der Lieferketten für pharmazeutische Produkte [SS17]. In der produktiven Anwendung **Everledger** [10] für ein Supply Chain Tracking und Tracing von Diamanten sind bis heute über eine Millionen Diamanten registriert [Ba16].

3.2 Methodisches Vorgehen

Für die Beantwortung unserer Forschungsfrage, wie groß das Veränderungspotenzial der Blockchain-Technologie auf die Branche Logistik ist, haben wir ein Framework entwickelt, das zunächst anhand von neun Merkmalen nach Albeck (2016), Bower et al. (1995) sowie Govindarajan et al. (2006) die Fallstudien für eine erhaltene Innovation oder disruptive Innovation analysiert. Hierzu haben wir unsere Falllstudien systematisch auf die in Tabelle 1 dargestellten Merkmale hin untersucht. Beispielsweise haben wir hinsichtlich des Merkmals Kunden geprüft, ob Bestandskunden aus den bisherigen Geschäftsbeziehungen des Unternehmens angesprochen wurden, oder ob der Fokus primäre auf Neukunden liegt. Sollten die uns vorliegenden Informationen diesbezüglich

[3] Eine Übersicht der Fallstudien und deren Quellen im Internet finden Sie unter https://tinyurl.com/ybgsmlot

nicht aufschlussreich genug sein, so haben wir als Indiz bei einer permissioned Blockchain angenommen, dass damit zunächst Bestandskunden angesprochen wurden. Im Anschluss daran haben wir eine Untersuchung der Veränderungen der Fallstudien auf die Dimensionen der Geschäftsmodelle nach Gassmann et al. (2013) sowie Stähler (2008) vorgenommen. Beispielsweise gilt es bei dem Nutzenversprechen herauszufinden, was dem Kunden mit der neuen blockchain-basierten Anwendung angeboten wird [GS16].

Anhand dieser beiden Ergebnisse wird eine Gesamtwürdigung vorgenommen und eine Einschätzung hinsichtlich des Veränderungspotenzials aufgezeigt. Das Ertragsmodell von Gassmann et al. (2013) haben wir anhand der Geschäftsmodelle und deren Vergütungen von Rückeshäuser et al. (2017) feiner aufgegliedert, und die Fallstudie hinsichtlich der detaillierteren Aufgliederung bewertet.

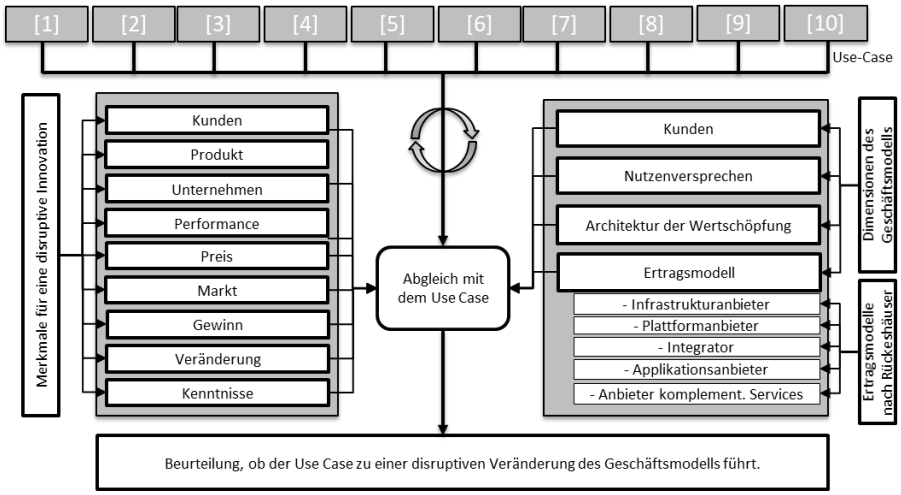

Abb. 1: Framework zur Untersuchung der Falllstudien.

Die für die Evaluierung durch das Framework notwendigen Daten haben wir anhand von Geschäftsberichten, Whitepapers, journalistischen Beiträgen, Blog-Einträgen sowie Homepages der Anbieter ermittelt. Bei der Auswahl der Fallstudien haben wir neben den in Kapitel 3 beschriebenen Aspekten auch darauf geachtet, dass wir zum einen mit dem Kontext der Fallstudie fachlich vertraut sind und zum anderen, dass zu den Fallstudien ausreichende Informationen für eine sinnvolle Evaluierung vorliegen [NVM13].

4 Ergebnis

4.1 Merkmale für eine disruptive Innovation[4]

Mit dem Merkmal Kunde untersuchen wir, ob die Blockchain-basierte Anwendung den Fokus auf die bestehenden Kunden des anbietenden Unternehmens setzt, oder ob neue Kunden angesprochen werden sollen. Sollten die bestehenden Kunden die Zielgruppe für die neue Anwendung sein, so ist eher eine erhaltene Innovation anzunehmen [Al16]. Bei einer Ausrichtung hin zu neuen Kunden ist ein disruptives Potential erkennbar, da die Markstrukturen verändert werden. Unsere Auswertung der Fallstudien zeigt eine Ausrichtung hin zu den bestehenden High-end Kunden, die anhand von vorhandenen Vertriebsstrukturen gezielt angesprochen werden können. Mit dem Merkmal Kunden eng verbunden ist das Merkmal Markt, denn eine Ausrichtung auf bestehende Kunden führt zu einer Ausrichtung auf bestehenden Märkten. Somit zeichnet sich die erhaltene Innovation durch eine Bearbeitung von bekannten Märkten aus, während eine Ansprache von neuen Kunden im Rahmen einer disruptiven Innovation ebenfalls mit neuen Märkten verbunden sein kann.

Das Merkmal Produkt haben wir daraufhin untersucht, ob die Blockchain-basierte Anwendung eher eine Anpassung bzw. Weiterentwicklung einer bereits vorhandenen Anwendung ist, wie z.B. bei Agridigital, oder ob eine neue Anwendung bzw. IT-Lösung entwickelt wurde. Die Weiterentwicklung einer bestehenden Anwendung ist der erhaltenen Innovation zuzuordnen, da der bestehende Leistungsumfang angepasst wird, während eine Neuentwicklung auf Basis einer neuen Technologie eher einen disruptiven Charakter aufweist.

Die umfangreichen Erfahrungen eines etablierten Unternehmens mit den bestehenden Märkten und Kundenanforderungen führt häufig zur Entwicklung von erhaltenen Innovationen [Al16]. Eine disruptive Innovation zeigt sich hingegen bei Startups bzw. neu am Markt auftretenden Unternehmen. Diese bieten Produkte mit zunächst einer geringeren Performance im Vergleich zu den bereits am Markt als wichtig empfundenen Leistungen zu einem geringeren Preis an [UA05]. Die am Markt bereits etablierten Produkte und deren Weiterentwicklung auf Basis einer erhaltenen Innovation weisen in der Regel höhere Preise aus, da zu dem bereits bestehenden Leistungsversprechen neue Funktionen hinzugekommen sind. Dadurch erwirtschaften erhaltene Innovationen in der Regel höhere Gewinne als disruptive Innovationen.

Eine disruptive Innovation mit neuen Funktionen führt häufig zu einer hohen Veränderung in den Geschäftsprozessen der Kunden, während eine erhaltene Innovation mit einer Weiterentwicklung der bestehenden Produkte eine eher geringe Veränderung nach sich zieht. Die Kenntnisse des Kunden über die neuen Funktionen sind demnach bei einer disruptiven Innovation eher geringer als bei einer erhaltenen Innovation.

[4] Die Ergebnisse der Merkmale zu den Fallstudien finden Sie hier: https://tinyurl.com/y7shlxew

4.2 Veränderungen in den Dimensionen der Geschäftsmodelle

Die Analyse der Fallstudien hinsichtlich der Dimensionen des Geschäftsmodells nach Gassmann und Sutter (2016) haben wir zunächst für das Nutzenversprechen sowie das Ertragsmodell durchgeführt. Die Analyse der Dimension Kunde ist zuvor in Kapitel 4.1 erläutert worden.

***Ocean Fright*:** Diese blockchain-basierte Anwendung hat die Wertversprechen, die Kosten der Papier- und Dokumentenverwaltung drastisch reduzieren sowie die Transparenz über den Transportstatus deutlich erhöhen zu können. Der Typ des Blockchain-basierten Geschäftsmodells ist *Integrator*, da neben der Bereitstellung der Blockchain auch eine standardisierte Schnittstelle zur Anbindung der legacy-Systeme bereitgestellt wird [Pe17]. ***Agridigital*:** Diese blockchain-basierte Anwendung hat die Wertversprechen, zunächst dem Getreideerzeuger eine Prozesssicherheit für den Zahlungsvorgang nach erfolgter Lieferung zu geben als auch einen beschleunigten Zahlungsvorgang durch eine Kryptowährung „Agricoin". Des Weiteren wird ein lückenloser Nachweis der Lieferkette über die Blockchain für eine Rückverfolgbarkeitsprüfung möglich sein. Der Typ des Blockchain-basierten Geschäftsmodells ist Applikationsanbieter, da neben der Blockchain eine voll funktionsfähige Anwendung angeboten wird [Ag17]. ***Agri-food*:** Das Wertversprechen dieser Lösung ist eine geschlossene, verifizierte und transparente Lieferkette, die Daten in Echtzeit verarbeitet und somit jederzeit Auskunftsfähig über den aktuellen Status ist. Der Typ des Blockchain-basierten Geschäftsmodells ist Infrastrukturanbieter, da lediglich eine offene Blockchain bereitgestellt wird [Ti16]. ***Animal product*:** Das Wertversprechen dieser blockchain-basierten Anwendung ist neben der Schaffung von Transparenz und der Möglichkeit einer lückenlosen Rückverfolgung von tierischen Produkten entlang der Lieferketten, auch die Prozessbeschleunigung innerhalb der Lieferketten. Der Typ des Blockchain-basierten Geschäftsmodells ist Plattformanbieter, da neben der reinen Blockchain auch eine Benutzerverwaltung angeboten wird [MBP17]. ***Cognizant Retail*:** Das Wertversprechen ist zum einen die Erhöhung der Transparenz der Lieferkette aber auch die Reduzierung von Kosten durch den Verzicht auf redundante Systeme sowie Effizienzgewinne durch Verkürzung der Transaktionszeiten. Der Typ des Blockchain-basierten Geschäftsmodells ist Infrastrukturanbieter, da lediglich eine offene Blockchain bereitgestellt wird [WHC17]. ***OpenBazaar*:** Das Wertversprechen von OpenBazaar ist zum einen der kostenlose Handel von Gütern und Services ohne Marktplatzgebühren, zum anderen der Verzicht auf das Sammeln von Kundendaten sowie der Verzicht auf eine Zensur. Der Typ des Blockchain-basierten Geschäftsmodells ist Applikationsanbieter, da eine peer-to-peer basierte Anwendung zur Verfügung gestellt wird. ***Origin Tracking*:** Das Wertversprechen der Anwendung ist die Integration in bestehende IT-Systeme bei einer gleichzeitigen Zunahme der Transparenz der Lebensmittelketten und damit einer Rückverfolgbarkeit. Der Typ des Blockchain-basierten Geschäftsmodells ist Integrator, da neben der Bereitstellung der Blockchain auch eine standardisierte Schnittstelle zur Anbindung der legacy-Systeme bereitgestellt wird [Pe17], [PL17]. ***CargoChain*:** Das Wertversprechen besteht aufgrund der digital vorhandenen Daten in der

Reaktionsgeschwindigkeit verbunden mit einer hohen Automatisierung sowie einem Exception-Handling basierend auf Workflows. Die geschlossene Blockchain wird hierbei mit den verschiedenen vorhandenen IT-Systemen verzahnt. Der Typ des Blockchain-basierten Geschäftsmodells ist Applikationsanbieter, da neben der Blockchain weitere Funktionen des Logistik Prozesses unterstützt werden [IM17]. ***LifeCrypter***: Das Wertversprechen ist sowohl die notwendige Transparenz als auch Rückverfolgbarkeit der Lieferkette, verbunden mit der Generierung eines höheren Vertrauens in Daten. Der Typ des Blockchain-basierten Geschäftsmodells ist Plattformanbieter, da neben der Blockchain auch konfigurierbare Smart Contracts zur Automatisierung von Prozessen angeboten werden [SS17]. ***Everledger*:** Das Wertversprechen der Anwendung ist die Transparenz über die Herkunft und den Transaktionen eines Diamanten innerhalb eines Lebenszyklus eines Diamanten. Der Typ des Blockchain-basierten Geschäftsmodells ist Applikationsanbieter, da neben der Blockchain eine Funktion für Endkunden zum Ausdruck von Diamantenzertifikaten bereitgestellt wird [Ba16].

Für die Dimension der Architektur der Wertschöpfung haben wir in einer Cross-Case Analyse (siehe Kapitel 4.3) die Wertversprechen der Fallstudien analysiert und die Eigenschaften der Blockchain-Technologie, die die Grundlage für dieses Wertversprechen liefern, hervorgehoben.

4.3 Dimension Wertversprechen / Nutzenversprechen

Basierend auf den Ergebnissen der within-case Analyse präsentieren wir die Ergebnisse einer Cross-Case Analyse, die Bezug nimmt auf das Leistungskonzept (Value Proposition) als Wertversprechen für Kunden [BR11]. Unsere Analyse hat zunächst sechs verschiedene Wertversprechen in den 10 Fallstudien ergeben. Die häufigsten Gemeinsamkeiten bestehen in Transparenzerhöhung, Rückverfolgbarkeit sowie Prozesseffizienz. Das Wertversprechen der Transparenzerhöhung basiert auf den Eigenschaften der Blockchain-Technologie Unveränderlichkeit der Daten, Verarbeitung der Daten in Echtzeit, permanente Verfügbarkeit der Daten sowie der chronologischen Reihenfolge der Daten. Das nächst relevante Wertversprechen ist die Rückverfolgbarkeit, die anhand der gleichen Eigenschaften wie bei der Transparenzerhöhung erzeugt wird plus dem Peer-to-Peer Netzwerk und Open Source. Die dann folgende Prozesseffizienz geht einher mit der Verarbeitung der Daten in Echtzeit, permanente Verfügbarkeit der Daten sowie den Smart Contracts für die Automatisierung von Prozessschritten.

Blockchain-basierte Anwendung **Wertversprechen**	**Ocean Fright**	**Agridigital**	**Agri-food**	**Animal product**	**Cognizant Retail**	**OpenBazaar**	**Origin Tracking**	**CargoChain**	**LifeCrypter**	**Everledger**
Kostenreduktion	X				X	X				
Transparenzerhöhung	X		X	X	X		X	X	X	X
Prozesssicherheit		X								
Prozesseffizienz		X		X	X			X		
Rückverfolgbarkeit		X		X			X		X	X
Echtzeitverarbeitung			X					X		

Tab. 2: Wertversprechen der blockchain-basierten Anwendungen.

4.4 Gesamtwürdigung anhand der Ergebnisse

Die wertschöpfenden Aktivitäten von Unternehmen zielen auf einen Kunden ab, der damit im Mittelpunkt des Interesses steht. Das disruptive Potential einer blockchain-basierten Anwendung zeigt sich demzufolge auch in der Veränderung der Kundenstruktur des Unternehmens. Unsere Analyse des Merkmals Kunde zeigt hinsichtlich einer disruptiven Innovation bei sieben von zehn Fallstudien weiterhin den typischen High-end Kunden, anstatt den bei einer disruptiven Innovation üblichen Low-end Kunden. Die Einbindung dieser High-end Kunden in eine permissoned Blockchain in neun von zehn Fällen zeigt einen deutlichen Bezug zu einer Anbindung von Bestandskunden. Diese Bestandskunden werden demzufolge in acht von zehn Fällen von bestehenden Unternehmen in bereits bestehenden Geschäftsbeziehungen mit der neuen blockchain-basierten Anwendung angesprochen, eine typische Ausprägung einer erhaltenen Innovation. Hervorzuheben ist jedoch für das Merkmal Produkt, dass in sechs Fallstudien entweder vollständig neue Produkte oder grundlegend veränderte Produkte angeboten werden. Diese Merkmalsausprägung spricht eher für eine disruptive Innovation, als für eine erhaltene Innovation. Jedoch ist die Bewertung des Merkmals Produkt im Zusammenhang mit den Merkmalen Kunde und Unternehmen vorzunehmen, denn die Ansprache eines bestehenden Kunden von einem bestehenden Unternehmen zeigt deutlich eine erhaltene Innovation, auch wenn die bestehenden Produkte grundlegend überarbeitet oder neu entwickelt werden.

Hinsichtlich der Untersuchung der Dimensionen ist die Transparenzerhöhung ein wesentliches Element im Nutzenversprechen. Diese Transparenzerhöhung basiert im Wesentlichen auf den Eigenschaften der Blockchain-Technologie wie zuvor in Kapitel 4.3 aufgeführt. Jedoch konnten wir zuvor bei den Merkmalen konstatieren, dass ein neues oder angepasstes Produkt nicht unweigerlich zu einer disruptiven Innovation führt, wenn ein bestehendes Unternehmen das Produkt an bestehende Kunde vermarktet. Demzufolge ist eine technologische Innovation als Grundlage für ein Nutzenversprechen in diesem Fall keine disruptive Innovation, sondern eher eine erhaltene Innovation.

5 Limitationen, Zusammenfassung und weitere Forschungen

Aus methodischen Gründen führten wir unsere Untersuchungen nur anhand von 10 Fallstudien durch. Daher wird die Validität unserer Ergebnisse unzweifelhaft von der Analyse von weiteren Fallstudien aus der Logistik profitieren. Unsere Forschung hat jedoch die Einschränkung, dass die von uns analysierten Fallstudien bald „veraltet“ und durch neue Anwendungen ersetzt sein werden.

Das Veränderungspotenzial der Blockchain-Technologie ist innerhalb der Branche Logistik sehr gering, da die blockchain-basierten Anwendungen unserer zehn Fallstudien hauptsächlich auf Bestandskunden in einem oberen und profitablen Marktsegment zielen. Eine disruptive Innovation entsteht jedoch nach der Lehre von Christensen et al. (2016) entweder in neuen Märkten oder in den unteren Marktsegmenten von bestehenden Märkten. Für die Unternehmenspraxis ist die korrekte Einordnung der Innovation eines Wettbewerbers deshalb relevant, da die strategischen Ansätze zur Reaktion bei einer disruptiven Innovation andere sind als bei einer erhaltenen Innovation [CRM16]. Für die Branche Logistik zeigt sich aktuell eine erhaltene Innovation, die von bestehenden Marktteilnehmern auf bestehende Kunden in bestehenden Märkten abzielt. Jedoch ist zu bedenken, dass dies eine Momentaufnahme ist und eine disruptive Innovation ein Prozess ist, der sich über einen längeren Zeitraum erstrecken könnte [WC13]. Der Erfolg einer disruptiven Innovation hängt darüber hinaus von der Geschwindigkeit ab, mit der sich die zugrundeliegende Blockchain-Technologie verbessert [CRM16]. Die Blockchain-Technologie bietet anhand ihrer technologischen Architektur zahlreiche Möglichkeiten für die Veränderung von bestehenden Prozessen und Geschäftsmodellen der Logistik. Die Studie „Logistikbranche in der Zwickmühle“ von Roland Berger weist aufgrund des zunehmenden Kostendrucks der Branche auf die Notwendigkeit zu digitalen Geschäftsmodellen hin [MT16]. Die Studie ermittelt für die Zukunft der Branche die vier Geschäftsmodelle Buchungs- und Optimierungsplattformen, Frachtführer und Terminalbetreiber, Supply-Chain Spezialisten sowie Service Provider. Diese Service Provider nutzen die Informationstechnologie und bieten darauf aufbauend Lösungen für die Sammlung und systematische Auswertung großer Datenmengen sowie weiterer Dienstleistungen an. Die Service Provider sind damit das Kernstück der digitalen Logistik [MT16]. Der Prozess der disruptiven Innovation in Zusammenhang mit der Blockchain verbunden mit den zunehmenden digitalen Geschäftsmodellen in der Logistik bietet Raum

für weitere Forschungen in Richtung der Veränderung von Geschäftsmodellen als auch der strategischen Ansätze zur Reaktion auf diese Entwicklungen.

Literaturverzeichnis

[Ag17] Agridigital, CBH Group: Solving For Supply Chain Inefficiencies And Risks With Blockchain In Agriculture, 2017, Pilot Report, availabel at: http://www.agridigital.io/blockchain#pilot-report, Stand: 30.04.2018.

[Al16] Albeck, W.; Geschäftsmodellinnovationen für das mittlere Marktsegment - Eine empirische Untersuchung deutschsprachiger Maschinenbauunternehmen in China. Springer Fachmedien Wiesbaden.

[Ba16] Badzar, A.: Blockchain for securing sustainable transport contracts and supply chain transparency. An explorative study of blockchain technology in logistics, Lund University 2016, http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8880383&fileOId=8880390, Stand: 30.04.2018.

[BR11] Bieger, T., Reinhold, S.: Das wertbasierte Geschäftsmodell – Ein aktualisierter Strukturierungsansatz, In: T. Bieger et al. (Hrsg.), Innovative Geschäftsmodelle, Springer-Verlag Berlin Heidelberg 2011.

[BC95] Bower, J., Christensen, C. M.: Disruptive Technologies: Catching the waves. Harvard Business Review 1995.

[CR17] Chakravorty, A.; Rong, C.; Ushare: user controlled sozial media based on blockchain. IMCOM `17, January 05-07, 2017, Beppu, Japan.

[Ch17] Chavanne, Y.; Pires, T.; Die Blockchain entrümpelt die Supply Chain, 2017. http://www.netzwoche.ch/news/2017-09-01/die-blockchain-entruempelt-die-supply-chain, Stand: 30.04.2018.

[CRM16] Christensen, C.M.; Raynor, M.; McDonal, R.: Was ist disruptive Innovation. Harvard Business manager, Januar 2016, Seite 64-75.

[CR03] Christensen, C.M.; Raynor, M. (2003): The Innovator's Solution: Creating and Sustaining Successful Growth. Boston, Harvard Business School Press.

[De17] Delfmann, W.; Kersten, W.; Stölzle, W.; ten Hompel, M.; Schmidt, T.; Logistik als Wissenschaft – zentrale Forschungsfragen in Zeiten der vierten industriellen Revolution. Positionspapier des Wissenschaftlichen Beirats der Bundesvereinigung Logistik (BVL) 2017.

[De10] Delfmann, W.; Dangelmaier, W.; Günthner, W. A.; Klaus, P.; Overmeyer, L.; Rothengatter, W.; Weber, J.; Zentes, J.; Positionspapier zum Grundverständnis der Logistik als wissenschaftliche Disziplin. Arbeitsgruppe des Wissenschaftlichen Beirats der Bundesvereinigung Logistik (BVL) e.V.

[DP17] Demont, A., Paulus-Rohmer, D.: Industrie 4.0-Geschäftsmodelle systematisch entwickeln. Eine strategiegeleitete Vorgehensweise für den Maschinen- und

Anlagenbau, in: Schallmo, D. (Hrsg.): Digitale Transformation von Geschäftsmodellen. Grundlagen, Instrumente und Best Practices. SpringerGabler 2017.

[DS08] Druehl, C.; Schmidt, G. (2008): A Strategy for Opening a New Market and Encroaching on he Lower End of the Existing Market. In: Production and Operations Management. 17 (1), S. 44–60.

[EG07] Eisenhardt, K. M.; Graebner, M. E.: Theory Building from Cases: Opportunities and Challenges, Academy of Management Journal. Vol. 50, No. 1, pp. 25-32.

[GFC13] Gassmann, O.; Frankenberger, K.; Csik, M.: Geschäftsmodelle entwickeln. 55 innovative Konzepte mit dem St. Galler Business Model Navigator, 2013, 2. Auflage, Carl Hanser Verlag München.

[GS16] Gassmann, O.; Sutter, P.: Digitale Transformation im Unternehmen gestalten. Geschäftsmodell, Erfolgsfaktoren, Handlungsempfehlungen, Fallstudien. 2016 Carl Hanser Verlag München.

[Go17] Google Inc.: How Search works, http://www.google.com/intl/ALL/search/howsearchworks/, Stand: 30.04.2018.

[GK06] Govindarajan, V., Kopalle, P. K.: The Usefulness of Measuring Disruptiveness of Innovations Ex Post in Making Ex Ante Predictions. The Journal of Product Innovation Management. Volume 23, Issue 1, January 2006, Pages 12–18.

[He08] Hensel, M., Wirsam, J.: Diffusion von Innovationen. Das Beispiel Voice over IP. Gabler Edition Wissenschaft, 2008.

[HJP10] Herzwurm, G., Jesse, S., Pietsch, W.: Geschäftsmodelle und Wertschöpfungsketten im Cloud Computing. Informatik 2010: Service Science - Neue Perspektiven für die Informatik, Beiträge der 40. Jahrestagung der Gesellschaft für Informatik e.V. (GI), Band 1, 27.09. - 1.10.2010, Leipzig.

[HPM17] Holotiuk, F.; Pisani, F.; Moormann, J.: The Impact of Blockchain Technology on Business Models in the Payments Industry, in Leimeister, J.M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, S. 912-926.

[Im17] IMPERIAL Logistics International B.V. & Co. KG: CARGOCHAIN 2.0, https://github.com/domschiener/cargochain, Stand: 30.04.2018.

[Ke17] Kersten, W.; Seiter, M.; See, B. v.; Hackius, N.; Maurer, T.: Chancen der digitalen Transformation. Trends und Strategien in Logistik und Supply Chain Management. Hamburg 2017: DVV Media Group GmbH.

[Ko17] Kolbe, M.: Kühne + Nagel testet Blockchain in der Logistik, 2017. https://www.cio.de/a/kuehne-nagel-testet-blockchain-in-der-logistik,3572699. Stand: 30.04.2018.

[Kr17] Kreutzer, R.: Treiber und Hintergründe der digitalen Transformation, in: Schallmo, D. (Hrsg.): Digitale Transformation von Geschäftsmodellen. Grundlagen, Instrumente und Best Practices. SpringerGabler 2017.

[MBP17] Marinello, F.; Boscaro, D.; Pezzuolo, A.: Development of a traceability system for the animal product supply chain based on Blockchain Technology. 8th European Conference on Precision Livestock Farming ECPLF 2017, At Nantes, Volume: 1.

[MT16] Marwyk van, K.; Treppte, S.: 2016 logistics study on digital business models. 2016. https://www.rolandberger.com/de/press/Logistikbranche-in-der-Zwickmühle-–-zwischen-dem-Druck-der-Digitalisierung-und-d-2.html, Stand: 30.04.2018.

[NVM13] Nickerson, R. C.; Varshney, U.; Muntermann, J.: A method for taxonomy development and its application in information systems, European Journal of Information Systems 2013, 22 (3), pp. 336-359.

[No17] Nofer, M., Gomber, P., Hinz, O., Schierech, D.: Blockchain. Business & Information Systems Engineering 2/2017.

[Ma17] O`Marah, K.: Blockchain For Supply Chain: Enormous Potential Down The Road, 2017. https://www.forbes.com/sites/kevinomarah/2017/03/09/blockchain-for-supply-chain-enormous-potential-down-the-road/#5b235c193db5. Stand: 30.04.2018.

[Op17] OpenBazaar: What is OpenBazaar? http://docs.openbazaar.org/, Stand 30.04.2018.

[OPT05] Osterwalder, A., Pigneur, Y., Tucci, C. L.: Clarifying Business Models: Origins, Present, and Future of the Concept. Communications of the Association for Information Systems, Volume 15, Article May 2005.

[PL17] Popper, N.; Lohr, S.: Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?“, https://www.nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html, Stand: 30.04.2018.

[Pe17] Petersen, M.: Blockchain in Logistics and Supply Chain: Trick or Treat?, International Conference of Logistics in Hamburg, 2017, DOI: 10.15480/882.1444.

[Re13] Recker, J.: Scientific Research in Information Systems. A Beginner`s Guide, Springer-Verlag Berlin. 2013.

[Ro03] Rogers, E. M.: Diffusion of Innovations. Third Edition. New York. The Free Press, 2003

[RSC15] Rose, S.; Spinks, N.; Canhoto A. I.: Management Research. Applying the principles, Routledge Taylor & Francis Group. 2015.

[Ro02] Rowley, J.: Using Case Studies in Research. Management Research News, Volume 25 Number 1 2002.

[RBM17] Rückeshäuser, N.; Brenig, C., Müller, G.: Blockchains als Grundlage digitaler Geschäftsmodelle. DuD Datenschutz und Datensicherheit. 8.2017.

[SG08] Seawright, J. and Gerring, J.: Case-Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options, Sage Journals, Volume: 61 issue: 2, 2008, pp. 294-308.

[SR17] Schallmo, D., Rusnjak, A.: Roadmap zur Digitalen Transformation von Geschäftsmodellen, in: Schallmo, D. (Hrsg.): Digitale Transformation von Geschäftsmodellen. Grundlagen, Instrumente und Best Practices. SpringerGabler 2017.

[SS17] Schöner, M. M.; Sandner, P.: Blockchain Technology in the Pharmaceutical Industry, FSBC Working Paper 2017, http://explore-ip.com/2017_Blockchain-Technology-in-the-Pharmaceutical-Industry.pdf, Stand: 30.04.2018.

[St18] Stähler, P.: Definition Geschäftsmodellinnovation. http://staehler.info/definitionen/geschaeftsmodellinnovation.htm, Stand: 30.04.2018.

[Sw15] Swan, M.: Blockchain, Blueprint for a new economy. O`Reilly USA 2015.

[Th17] Thiele, C.-L.: Zwischen Disruption und Spekulation: Virtuelle Währungen und Blockchain-Technologie. https://www.bundesbank.de/Redaktion/DE/Reden/2016/2016_12_07_thiele.html, Stand: 30.04.2018.

[Ti16] Tian, F.: An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology, 13th International Conference on Service Systems and Service Management (ICSSSM) 2016, Kunming, China.

[UA05] Utterback, J.; Acee, H.: Disruptive technologies: an expanded view. International Journal of Innovation Management 2005, S. 1–17. 09, 1 (2005).

[Ve14] Veit, D.; Clemons, E.; Benlian, A.; Buxmann, P.; Hess, T.; Kundisch, D.; Leimeister, J. M.; Loos, P. & Spann, M.: Geschäftsmodelle - Eine Forschungsagenda für die Wirtschaftsinformatik. In: WIRTSCHAFTSINFORMATIK - Research Notes, Ausgabe/Number: 1, Erscheinungsjahr/Year: 2014. Seiten/Pages: 55-64.

[We14] Weitert, C.: Wettbewerbsimplikationen technologischen Wandels - Eine simulationsbasierte Untersuchung der Anpassungsfähigkeit von Unternehmen. Springer Fachmedien Wiesbaden 2014.

[WHC17] Weldon, R.; Herridge, M.; Cohen, J.: Retail: Opening the Doors to Blockchain, https://www.cognizant.com/whitepapers/retail-opening-the-doors-to-blockchain-codex2879.pdf, Stand: 30.04.2018.

[WC13] Wessel, M., Christensen, C. M.: So überleben Sie disruptive Innovationen. Harvard Business Manager, Februar 2013, Seite 21-31.

[Wk17] WKO: Logistik: Struktur, Zukunft und Trends der Branche. Neue und ganzheitliche Logistikkonzepte sind gefragt. https://www.wko.at/service/aussenwirtschaft/logistik-branche-struktur-zukunft-trends.html, Stand: 30.04.2018.

[Yi94] Yin, R. K.: Case Study Research. Design and Methods, 2nd Edition, Sage Publications, 1994.

Security Aspects of Hardware Virtualization Technologies for Industrial Automation and Control Systems

Asmaa Tellabi[1], Ludger Peters[2], Christoph Ruland[3], Karl Waedt[4]

Abstract: Virtualization is a technology that is strongly driven by the information technology industry and has started being applied in the process industry. Virtualization might be used in the process automation, where process engineering departments control the process application software. In this paper, an architecture will be presented that is potentially applicable for Industrial Automation and Control Systems (IACS) of Industry 4.0 but also for Safety Instrumentation & Control (I&C) and Operational I&C for power plants. The focus of this paper will be on a firm control of outgoing and incoming access to/from the transmission system, which is presumed as a Time Sensitive Network (TSN). XtratuM is deployed as an example of hypervisor joined with the security extensions offered by Arm v7 and newer Arm processors with "Trustzone" support, and extended by a Trusted Platform Module (TPM).We present also security issues surrounding virtualization environments.

Keywords: Virtualization, IACS, XtratuM, TPM, hardware security, ARM, Trustzone.

1 Introduction

Virtualization builds a simulated, or virtual, computing environment similar to a physical environment. In the Industry 4.0 scope virtualization is deployed at different levels, up to digital twins, which are complete virtualized versions of plants or factories. In this paper we address the virtualization of computer-generated versions of hardware, operating systems (OS), storage devices, and more. This enables organizations to divide a single physical computer or server into multiple virtual machines (VM). Each VM can then interact independently and run different OS or applications while sharing single host machine´s resources of [KMP11]. This simulated environment is named a VM, which is a software implementation of an entity that executes programs like the ones in a real hardware based machine. Delivering fault tolerance, complete monitoring and simplified management is the key for a successful adoption of virtualization in the industrial sector. Today, the embedded market is slowly getting prepared to exploit the financial benefits of this favorable technology. Most of the current developments on virtualization are targeting desktop systems. Thus, shifting these results to embedded

[1] University of Siegen, Faculty of Science and Engineering, Chair for Data Communication Systems, Hölderlinstraße 3, Siegen, 57068, asmaa.tellabi@student.uni-siegen.de
[2] Hochschule Zittau/ Görlitz, Department Electrical Engineering and Computer Science, Theodor-Körner-Allee 16, Zittau, 02763,ludger.peters@framatome.com
[3] University of Siegen, Faculty of Science and Engineering, Chair for Data Communication Systems, Hölderlinstraße 3, Siegen, 57068, christoph.ruland@student.uni-siegen.de
[4] Framatome GmbH, Henri-Dunant-Str. 50, Erlangen, 91058, karl.waedt@framatome.com

systems is not an easy task. As virtualization technologies are dynamically growing, with numerous competing technologies developed, the perfect solution or a winner technology does not exist yet. Security levels required for an embedded device vary dramatically based on the device´s function [IC18]. Virtualization techniques and virtualized architectures present a supplementary layer of execution, together with their own administrator role, which necessitates proper management and security protection. A security solution for embedded devices must guarantee that the device firmware has not been altered; it should ensure security of the data stored by the device, secure communication and protect the device from malicious actions [IC18]. This layer is made up of multiple dissimilar components, each with a role in the virtualization process, each introducing a potential target for malicious attacks [EN18].

The remainder of this paper is organized as follows. Section 2 gives background information on virtualization concepts including security aspects of virtualization environments. Section 3 explains the proposed architecture and components. We conclude the paper in Section 4.

2 Hardware Virtualization

As a common model used on server systems, it offers two main advantages: first, a better resource utilization of a physical machine is achieved and second, a stronger separation between software modules, therefore avoiding a full system breach in case a single component is compromised [EN18]. On the other hand, to employ the virtualization model proficiently, hardware support is required. Virtualization has received huge popularity thanks to its financial benefits and further characteristics like availability, scalability, and improved performance [ST18].

The virtualization paradigm is connected to emulation and simulation´s concepts, which employ dissimilar methods. Emulation is a method in which a system is running as if it were a different system. OSs, APIs, and processes are emulated on a machine for which they were not created. The emulator reproduces the particular behaviour of physical hardware, meaning it runs a copy of software by emulating the hardware for which the software was already created. On the contrary, Simulation simulates the behaviour of a specific system. Its purpose is to reach similar results as an emulator, but necessitates modifying part of the program to be simulated. Virtualization offers methods for resources and devices to be used without taking into consideration their position and physical layout [EN18].

2.1 Hardware virtualization classification

Hardware Virtualization technologies are categorized following their level of hardware emulation. There is a difference between methods that offer full hardware emulation and others that offer hardware virtualization as follows [EN18]:

- **Full hardware emulation** permits running a guest OS in a diverse host architecture. It entirely emulates features of a software system or device on a hardware platform with a different instruction set, e.g. QEMU.

- **Hardware virtualization** allows a software system or device to be executed on a hardware platform with similar instruction set. In general, there is not a distinction between hardware virtualization and emulation, as long as hardware emulators can be deployed for device virtualization. Hardware virtualization is itself categorized into three categories as follows:

- **Full virtualization** capable of ensuring virtualization of x86 systems through hardware´s simulation. The guest OS is totally isolated from the hardware, the access to it is arbitrated by the virtualization layer or the virtual machine monitor. The guest OS running is unchanged without the need of hardware or OS support. A combination of binary translation of kernel code and direct execution of user-level code can be the basis of full virtualization. Full virtualization delivers a highest separation and security, but it reduces performance and adds extra overhead, e.g. VirtualBox. There are two types of full virtualization. B*are metal* virtualization or *native virtualization*, the hypervisor runs directly on the hardware without a host OS. The second form is known as *hosted virtualization*, where the hypervisor runs on top of the host OS; which can be almost any common operating system e.g.Windows [KMP11].

- **Para virtualization** provides a lightweight virtualization method where the hypervisor exposes hyper calls that can be called by a modified guest OS. Hyper calls deploy virtualized system calls and call the hypervisor's services. They can be invoked by a modified guest OS using defined APIs. On the other hand, para virtualization offers improved performance and less overhead than full virtualization, at the price of necessitating modifications to the guest OS. Examples of solution providing para virtualization contain Xen, KVM/QEMU.

- **Hardware-assisted virtualization** Intel Virtualization Technology (VT-x) and AMD's AMD-V were presented on 2000s and delivers a new execution mode that permits virtual machine monitors to be executed in a new privileged mode. By offering hardware extensions to the guest OS, it delivers improved performance and decreases unnecessary modifications required by paravirtualization. Examples of solutions are VirtualBox, Xen.

2.2 Related work

- **ACROSS (ARTEMIS CROSS-Domain Architecture)**: the goal of this project was to design a cross-domain architecture for embedded Multi-Processor Systems-on-a-Chip (MPSoC) and to implement its initial version in an FPGA.

To make system´s development easier, a library of middleware services was implemented to deliver basic services which were used in different application domains, e.g. diagnosis, and security [TR18].

- **ARAMiS (Automotive, Railway and Avionics Multicore Systems)**: its aim was to support a suitable development of multicore systems using virtualization in the domains of automotive, avionics and railway, especially for safety related systems. In this project concerns related to time requirements, performance, reliability, availability; security and energy efficiency were addressed [AR18].

- **CERTAINTY (Certification of Real Time Applications designed for mixed criticality)**: related to the certification process for mixed-critical systems (MCS) including functions dependent on different security levels. The project was based on mixed-criticality methods, with strong separation and high levels of certification. Application domains were related to fields that must adhere to real-time and safety-critical requirements [CE18].

- **IMA-SP (Integrated Modular Avionics for Space):** the European Space Agency (ESA) started this project in 2011 in order to analyze IMA architectures´ applicability to space applications. The project´s objective was to outline requirements of temporal and spatial partitioning systems (TSP) in the space domain, via a defined hardware [ES18].

- **MCC (Mixed Criticality Embedded Systems on Many Core Platforms)** its objective was to implement multi-core platforms, to develop verification procedures dedicated to MCS, to analyze theoretical bounds of the developed schemes, and to develop necessary run-time controls to manage communication sharing between the criticality levels [CO18].

- **MultiPARTES (Multi-cores Partitioning for Trusted Embedded Systems)** this project´s results were related to developing tools and solutions for creating trusted embedded systems with mixed criticality modules on multicore platforms. Their approach was to develop an open-source multicore-platform based on virtualization layer using the hypervisor XtratuM [HI18].

- **parMERASA (Multi-Core Execution of Parallelized Hard Real-Time Applications Supporting Analyzability):** The goal was to make multi-core processors use in the development of real-time systems easier. Measuring the worst case execution time of an activity is a challenge in multi-core architectures [PA18].

- **RECOMP (Reduced Certification Costs Using Trusted Multi-core Platforms)**: this project´s goal was the implementation of MCS on multi-core architectures, where safety applications meet standards´ requirements, without affecting any of the efficiency and design cost characteristics of less critical modules. The project has implemented multiple mechanisms dedicated to

virtualization and safe core-to-core communication for different safety levels with diverse hardware and development costs [RE18].

- **vIrtical (SW/HW extensions for heterogeneous multi-core platforms):** Its aim was to raise functionality, reliability and security of embedded devices following a maintainable cost, and power consumption. The project is based on virtualization; it provided a virtualization concept dedicated to embedded devices, also related to flexibility and security concepts [VI18].

- **OVERSEE (Open vehicular secure platform)** provided an open vehicular IT platform which focused on security and dependability mechanisms. As a result, separate systems and cabling are more and more important [OV18].

- **DREAMS (Distributed Real-time Architecture for Mixed Criticality System**: provided a domain-independent architecture, joining mixed criticality modules with networked multi-core chips and security, safety and real-time features that can guarantee data and system integrity [DR18].

2.3 Hardware virtualization threats

Hardware virtualization environments have similar security issues as the ones found in computing environments that might compromise OS, communication protocols, and applications. In this section we will discuss security threats surrounding virtualization [EN18].

- **Gaining unauthorized access to protected information**

Confidential information may be exposed by mistake or attained by unauthorized entities, by bypassing security controls that are in place. Confidential information disclosure to unauthorized entities can be either unintentionally, e.g. human errors, or intentionally. Confidential data can be object of interception, for example while data are in transit an attacker can eavesdrop or sniff over a network in order to capture data.

- **Intentionally attempting to mislead other entities**

An unauthorized entity gains access to a system by pretending to be an authorized entity through: masquerading, e.g. spoofing, falsifying data to mislead an authorized entity, e.g. reply attacks, to execute actions that will negatively impact the system, e.g. social engineering attacks. As an illustration, at the virtual network level, when connecting all available virtual networks, concerns of role separation and policy conflicts may rise, facilitating identity fraud.

- **Causing failure or degradation of systems, negatively affecting the services they provide**

This threat may happen, either directly by making system components or

communication channels unavailable, or by modifying system operations through system functions´ alteration in order to send compromised data, or interrupting system´s operations.

- **An unauthorized entity that may gain unauthorized control over a system**

Usurpation is defined as the misappropriation of identity through service, functionality, or data theft, or action´s misuse, which causes a system component to execute an important action to system´s security. In virtualized environments, privilege escalation´s impact is more dangerous than in a physical environment as administrator privileges´ hierarchical structure is different.

3 Architecture of a virtualized hardware platform

Nonetheless, with the propagation of digital safety and control systems, along with the existing association between safety systems and other systems, cyber security has grown into an important constituent in the general protection of nuclear I&C safety systems. Therefore, to serve these different digital components, cyber security should be contained within the global security program.

3.1 Components

- **XtratuM**

XtratuM is a bare–metal hypervisor or Type 1; it uses paravirtualization where sensitive instructions are replaced by hyper calls to provide a fully working virtualization environment. In case of porting an OS, only the Hardware Abstraction Layer (HAL) of the OS has to be matched to the hyper calls, it has to be executed in supervisor processor mode in order to virtualize the CPU, the memory, interrupts, and other peripherals. This hypervisor is specially developed to meet the requirements of safety–critical environments [FE18].

XtratuM delivers ARINC 653 scheduling policy, partition management, inter-partition communications, health monitoring, log files, traces, and multiple services so it can be easily adapted to the ARINC standard. It provides a strong temporal isolation via its cyclic scheduler, a strong spatial isolation through the execution of the partitions in processor user mode.

- **Arm Tustzone**

This technology is implemented into any ARM Cortex-A, Cortex-M23 and Cortex M33 family processor [ARM18]. It works by giving the processor an additional supplementary "secure state", which permits a secure execution of application’s code and isolates the security–relevant information from non–secure operations. Partitioning

divides the execution environment into a secure and a non–secure world. The partitioning can also be used to establish an individual environment with an open count of partitions. It also allows restricting the access to the different HW-resources like the memory or the peripherals. The TrustZone works by visualizing a single physical core as dual virtual cores to offer two completely isolated execution environments. For the realization, an additional bit, the Non–Secure Bit, is used to identify in which world the code is executed.

- **Trusted Platform Module (TPM)**

A TPM is a computer chip capable of securely storing a platform´s authentication credentials, e.g. of a laptop. These credentials might contain passwords, certificates, or encryption keys. Generally, a TPM is set up on the motherboard of a computer, and the communication is ensured with the rest of the system through the hardware bus. It is presented as a cryptographic coprocessor embedded on almost every commercial PCs and also servers. Before TPMs became well known, security coprocessors such as smart cards were used by few applications for cryptographic keys storage in order to recognize users and keys for encrypting data at rest [WD15]. An example of use cases can be the storage of platform´s measurements, which verifies that the platform is trustworthy.

- **Time Sensitive Networks (TSN)**

TSN is the IEEE 802.1Q defined standard technology to deliver deterministic messaging on standard Ethernet. TSN technology is centrally managed it provides guarantees of delivery and reduced jitter by means of time scheduling for real-time applications that necessitate determinism. TSN is an Ethernet standard that was created in order to allow deterministic communication on standard Ethernet. Before the IEEE 802.1 TSN standards, standard Ethernet didn't have a Layer 2 with deterministic capability [CI18]. One of TSN objectives is to handle real-time communication with reduced latency which relies on Ethernet technology. Since real-time capabilities are almost not available, standard Ethernet cannot be implemented on applications with hard real-time requirements [MA16].

3.2 Concept

Partitions´ functionalities can be based on TELEPERM® XS (TXS). It is Framatome's I&C system platform for safety I&C for nuclear power plants. It includes all the essential hardware and software components, together with the software tools obligatory for engineering, testing and commissioning, operation and troubleshooting in line with the most stringent software development requirements [To IEC 60880:2006]. TELEPERM® XS is used for deploying numerous types of I&C systems in a nuclear power plant. The essential constituents of this single core architecture are based on the TXS approach:

- **Hypervisor:** XtratuM is responsible of providing virtualization services to

partitions. It is executed in supervisor processor mode and virtualizes the CPU, memory, interrupts and some defined peripherals [FE18].

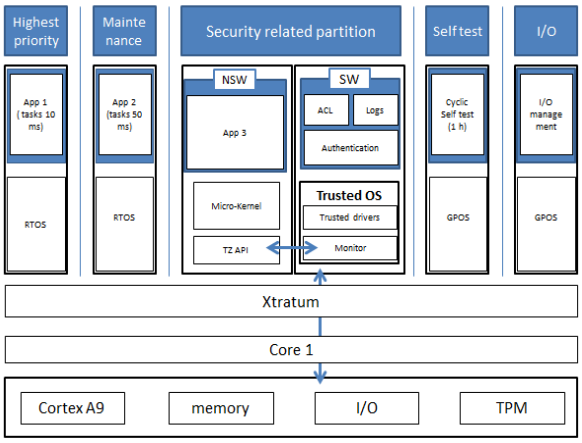

Fig.1:Single core architecture

- **Partitions:** are divided by a firewall. Each partition contains a specific task that represents a functionality as originally offered by TXS, and also divided by criticality level. Real time operating systems (RTOS) are used for time critical partitions, in our case we choose RTEMS.

- **Highest priority partition:** this partition contains tasks that have to be executed cyclically e.g. after every-50 ms. This partition runs on top of a RTOS. Tab.1 shows some details about this partition.

Partition	Description
Execution time	10 ms
Security relevant	Yes
OS	uses XAL
Functions	responsible of security relevant control operations

Tab. 1: Software information about highest priority partition.

- **Maintenance partition:** it contains the application that ensures the maintenance of each part in the system that has already sent a request to the server for maintenance.

- **Security related partition:** this partition implements the Trust Zone security extensions. In this partition two worlds exist, the secure world (SW) and the non-secure world (NSW). The SW includes applications for authentication,

Access control (ACL), and an application for logs. The authentication application uses the trusted platform module for cryptographic keys generation. The access control application manages the access of applications in the NSW following the roles of each user. TPM drivers have to be secured so they are contained in the SW.

- **Self-test partition:** which contains a cyclic test that is executed for example at least once per hour in order to check whether the functionalities are still accessible or there is a hardware problem that needs to be fixed (preventive maintenance). It runs on top of a general purpose operating system (GPOS).
- **I\O partition:** this partition is reserved for the management of I\O devices. It runs on top of a GPOS.

3.3 Inter-partition communication

The first option is to use shared memory by each partition, where sending partitions are allowed to write on it. A queuing channel is used to connect the NSW and the SW, and also an Inter-Partition Virtual Interrupt (IPVI) to connect SW to NSW. These three writing partitions can access all shared memory regions: Security related partition (NSW), the self–test partition, which sends messages to the other partitions every hour, the I/O management partition.

The second option, which is used for this system, is to use sampling channels. In this case, only two channels are used, with an IPVI for the connection between SW and NSW.

- **Channel 0:** Source: Highest Priority, Destination: Security Related–Partition (NSW) and I/O Management.
- **Channel 1:** Source: Maintenance, Destination: Security–Related Partition (NSW) and I/O Management.
- **Channel 2:** Source: Self-Test, Destination: All other partitions except for Security–Related Partition (SW).

3.4 Benefits of using a single-core architecture

The popularity of multi-core architectures in the electronic market has led to a constant move from single-core to multi-core designs even in safety-critical fields, like avionics and automotive. The implementation of mixed-critical applications on multicores is still a challenge because of the inter core interferences on shared platform resources that can have an undesirable effect on real time applications´ execution time [Al15].

- **Temporal effects of resource sharing in single core systems**

Sequential execution secures the isolation between different partitions, meaning that single applications competing for same hardware resources can be avoided. This partitioning is called Time Division Multiple Access (TDMA) with exceptions. This can cause temporal effects like Direct Memory Access (DMA) transfers, where different partitions compete for the memory bus at the same time. This can be avoided by replacing the DMA with a CPU controlled memory access scenario. Therefore security relevant aspects within a single core processor are well defined and are easier to handle [Al15].

- **Temporal effects of resource sharing in multicore systems**

In case single core architecture is replaced by multi–core architecture, the isolation between partitions cannot be secured through the sequential execution of applications. In this case several applications with different security levels run in parallel. Therefore these applications are competing for different system resources. This access needs to be handled by the implemented hypervisor [CI18].

- **System bus**

Components inside the system bus vary depending on the hardware vendor. In general, it includes the connection between CPU cores, the memory bus, shared caches and other devices. This connection has a highly varied access pattern, which should be well managed [CI18].

- **The memory, memory bus and controller**

Every program needs memory to execute its instructions. In case of multi–core processor environments and parallel executions of applications, several inferences between cores and the memory might occur and can cause additional timing delays.

- **The cache**

Located near the core, the cache is a fast storage for frequently used data. It is organized in multilayer hierarchies, where the L1 cache is always located on the core itself. The shared main memory is located on the cache. There are two main concerns; the first one is a bottleneck, where multiple CPU cores access the same cache memory at the same time. The second one is the overwriting of a section in shared memory by another core [CI18].

- **Logical units, pipeline stages**

On high performance MPSoC, the implementation of hyper threading where one physical core is executing two tasks at the same time can cause timing and memory access problems. Therefore this function is not implemented in ARM systems.

- **Addressable devices**

Devices, e.g. I/O-devices, interrupt/DMA controller, in MCS have to be secured they can be accessed only by authorized applications. This can be achieved by a locking mechanism in a single core environment which can be by prioritizing the access.

Conclusion

Virtual environments introduce new threats, risks, challenges, and also new assets and components. As a result, new technologies are required to deliver operative countermeasures and raise the trustworthiness of such environments. To be precise, delivered security tools have to adhere to virtualization properties and not to only be adapted to current techniques. Virtualization modules should definitely fit in with such tools via open interfaces and APIs. This paper presented a new architecture for IACS systems, which uses hardware virtualization and other security features. Based on automation principals used for nuclear power plants, this proposed new architecture uses benefits offered by virtualization. Hardware virtualization allows running multiple OSs and applications at the same time, but isolated from each other, on one physical host hardware. In the future, we intend to implement a demonstration of this architecture on a FPGA based board and test the improved security posture.

Bibliography

[KMP11] Karen, S.; Murugiah, S.; Paul, H.: Guide to Security for Full Virtualization Technologies. NIST Special Publ., vol. 800, 2011.

[IC18] Icon Labs: Security Requirements for Embedded Devices – What is Really Needed?, www.iconlabs.com, accessed: 02/07/2018.

[EN18] ENISA: Security aspects of virtualization, www.enisa.europa.eu, accessed: 10/05/2018.

[ST18] Stratus: Virtualization in industrial plants, www.stratus.com, accessed: 5/05/2018.

[TR18] TRIMIS: Transport Research and Innovation Monitoring and Information System, www.trimis.ec.europa.eu, accessed: 20/06/2018.

[AR18] ARAMIS: Automotive Railway Avionics Multicore Systems, www.projekt-aramis.de, accessed: 20/08/2018.

[CE18] CERTAINTY: Certification of Real Time Applications designed for mixed criticality, www.certainty-project.eu, accessed: 20/08/2018.

[ES18] ESA: European Space Agency, www.esa.int, accessed: 20/08/2018.

[CO18] CORDIS: Community Research and Development Information Service, www.cordis.europa.eu, accessed: 20/08/2018.

[HI18] HIPEAC, European Network on High Performance and Embedded Architecture and Compilation, www.hipeac.net, accessed: 20/08/2018.

[PA18] PARMERASA: WHAT IS parMERASA ABOUT?, www.parmerasa.eu, accessed: 20/08/2018.

[RE18] RECOMP: Reduced Certification Costs Using Trusted Multi-Core Platforms, www.fortiss.org, accessed: 20/08/2018.

[VI18] VIRTICAL: SW/HW extensions for virtualized heterogeneous multicore platforms, www.hipeac.net, accessed: 20/08/2018.

[OV18] OVERSEE Consortium: Open Vehicular Secure Platform, www.oversee-project.com, accessed: 20/08/2018.

[DR18] DREAMS: Distributed REal-time Architecture for Mixed Criticality Systems, http://dreams-project.eu, accessed: 20/08/2018.

[FE18] Fentiss: Fent Innovative Software Solutions, www.fentiss.com/xtratum, accessed: 20/08/2018.

[ARM18] ARM: ARM Security Technology - Building a Secure System using TrustZone Technology. Tech. Rep., 2009.

[WD15] Will, A.; David, C.: A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security. Apress, 2015.

[CI18] CISCO: Time-Sensitive Networking: A Technical Introduction, www.cisco.com, accessed: 20/08/2018.

[MA16] Morteza, F.; Alois, K.: An Ontology-based Plug-and-Play Approach for In-Vehicle Time-Sensitive Networking (TSN), Conference (IEMCON), 2016 IEEE 7th Annual, 2016.

[Al15] A. Alonso; et.al ,: Safety Concept for a Mixed Criticality On-Board Software System .IFAC-PapersOnLine, Volume 48, Issue 10, Pages 240-245, ISSN 2405-8963, 2015.

[CI18] CISTER: Multicore in real-time systems: Temporal isolation challenges due to shared resources, www.cister.isep.ipp.pt, accessed: 01/06/2018.

Security, safety and availability triad in a real-world industrial environment and resulting challenges

Michael Köpferl[1], Heiko Niedermayer[2], Georg Carle[3]

Abstract: Nowadays, machines in production environments are in some way or the other connected to the Internet as this is required for modern Industry 4.0 use cases. Yet, automation environments, also called Operational Technology (OT) and traditional IT environments are different. There are differences in requirements resulting in different objectives and development. While IT environments were connected to networks and the Internet traditionally, OT environments used to be stand-alone and therefore were not reachable through networks for both benign and malicious access. Disconnectedness resulted into lower security awareness for OT environments while at the same time paying special attention on availability and safety. This publication analyzes interdependencies of these goals and carves out problems resulting from this triad of Security, Availability and Safety.

Keywords: Operational Technology; Availability; Safety; Security

1 Introduction

While IT environments were connected to networks and the Internet traditionally, automation environments with production machines, also called Operational Technology (OT), used to be stand-alone. This, however, changed, at the latest as part of the Industry 4.0 age. Modern use cases require connectivity, e.g. production and maintenance optimization as well as gathering machine statistics for big data projects. Connectivity of machines to SCADA systems and other central infrastructure, external stakeholders like suppliers, customers, and others allows information exchange, both benign and malicious. Therefore, new attack vectors are created by connecting machines to networks that were not designed for this purpose which results in security risks[Ba18].

OT historically focused on maximizing availability of production machines to allow production to achieve highest possible output and reach safety requirements to reduce or eliminate the risk of injuries or environmental threats. Security, however, was neglected as attacks were only possible locally in a disconnected environment and physical barriers were sufficient to prevent those. By connecting machines to the Internet, these threats hit the

[1] Giesecke+Devrient GmbH, Security, Prinzregentenstr. 159, 81677 München, Germany michael.koepferl@gi-de.com / michael.koepferl@tum.de
[2] Technische Universität München, Boltzmannstraße 3, 85748 Garching, Germany niedermayer@net.in.tum.de
[3] Technische Universität München, Boltzmannstraße 3, 85748 Garching, Germany carle@net.in.tum.de

surface again and it appears that the OT world is not prepared as its protection approaches barely exceed rudimentary implementation of network-based security products like firewalls, data diodes, or similar products. These, however, are not able to provide a sufficient level of security as connectivity is still possible in some way, which also includes malicious communication and therefore attacks.

OT environments and their people and processes usually focus on two goals: safety and availability. Security as a goal is missing. Our contribution is as follows: First, we look at relevant definitions from both automation and security point of view to subsequently elaborate on their differences. Second, we analyze observed problems within a real-world industrial environment for interdependencies of objectives.

2 Definitions in standards and understandings of stakeholders

2.1 Automation point of view

We stated that the core objectives of the automation world are Safety and Availability. Therefore, we explain these from this point of view in the following:

Safety within an OT environment is defined as “freedom from unacceptable risk to the outside from the functional and physical units considered” according to the IEC61508 series[IE10]: “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”. Especially for automation environments, there is the term *functional safety*, which is defined as “part of the overall safety that depends on functional and physical units operating correctly in response to their inputs”.

For *availability*, there are several definitions. We here refer to the one found within the IEC62443-3-3 [IE13], as it is most relevant to industrial environments. It focuses on timely and reliable accessibility to information and functionality of automation systems. In section 2.4, we will compare this definition to the one introduced in the subsequent section and elaborate on differences.

Although standards like IEC62443 include confidentiality and integrity as topics, we have not seen in-depth awareness or let alone proactive implementation of expected and necessary level of security. We will analyze selected topics in the next chapter.

2.2 Security point of view

Availability, Confidentiality and Integrity are relevant objectives from a security point of view. Therefore, we analyze the definition of these goals from a security perspective in the following. The largely accepted international standard ISO/IEC 27000:2018(E)[IS18]:

"Information technology — Security techniques — Information security management systems — Overview and vocabulary" defines these terms as follows:

Availability is the "property of being accessible and usable on demand by an authorized entity". This means that valid users and processes need to be able to access required information. We described possible faults and errors as well as threats relevant to industrial environments within the last section.

Confidentiality is the "property that information is not made available or disclosed to unauthorized individuals, entities, or processes".

Integrity is the "property of accuracy and completeness" of information.

Information Security deals with the "preservation of confidentiality, integrity, and availability of information". Other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. Besides the main security objectives, which are most relevant, we also include: *Reliability* is defined as the "property of consistent intended behavior and results". *Non-Repudiation* is defined as the "ability to prove the occurrence of a claimed event or action and its originating entities". We will look at these properties when analyzing integrity as there are overlappings and interdependencies among risks and protective approaches.

2.3 Differences in availability definitions

We have seen that availability is a common goal and objective both from an automation and security point of view. However, definitions differ:

We can see that IEC62443 is more specific on the target of the definition, as it explicitly includes *functionality*, which is historically the core requirement of a machine. In so far, the information security perspective is incomplete and essential aspects may get ignored. Also, the IEC62443 definition explicitly includes *timely and reliable* accessibility, while the information security perspective is more vague as it only requires *on demand* accessibility. The ISO27000 definition, however, explicitly refers to accessibility of information to an *authorized entity*, which can be seen as a security aspect neglected by the automation world. As a short sidenote, the academic world also has a variety of definitions for availability-related goals and metrics, e.g. [St10].

2.4 Differences in the understanding of availability

Although standards provide definitions for availability, we recognize that there is no widely-accepted unique definition. Instead, each target group has their own perception and standards that sometimes do not take into account all possible influences or can be understood differently depending on the reader as they lack necessary precision and completeness.

From faults and outages that we experienced, from analysis of maintenance contacts between an industrial company and its suppliers as well as internal discussions with employees we find many different views on what availability means and what the respective stakeholders try to optimize and possibly neglect. The following table breaks these different definitions down systematically.

Type of availability	Perspective of	Definition/Goals
functional/technical	Supplier, maintenance staff	reduce outages to a minimum replace/repair broken parts[4] asap
data/information	IT	has to be accessible permanently[5] replace broken storage components, recover backed-up files
availability under attack	Security, partly IT	prevent data breaches prevent deletion / encryption malicious configuration changes

Together, all of these availability requirements form what is defined in IEC62443 and ISO27001. To make the operator use the machine successfully, all goals have to be fulfilled to prevent outages. However, all stakeholders have to be aware of the sum of these goals and perform their tasks to achieve the availability objective.

3 Examples of observed interdependencies of objectives

Based on aforementioned definitions, in subsequent sections we provide some examples of threats that are possible within industrial environments to show their impact on security, availability and safety.

3.1 Functional safety threatened by insufficient security

There are machines that can pose a threat to humans or the environment when something goes wrong. Regulation requires that these machines have a safety-off-functionality which can be used to immediately turn off dangerous parts (e.g. rotating, laser, heat, ...). Additionally, there are requirements to automatically turn off a machine or parts of it in case safety barriers are triggered. Both of these are defined in ISO13849:2015 as “safety functions”. Specialized safety components have to be implemented and tested as protective measures to achieve risk reduction.

While this seems to have no relation to the IT security of the factory at first, we have to consider that the signals for the safety-off signal have to travel through networked systems. In real production environments, we have seen cases where the signal travels through components (e.g. normal PLCs[6] which do not fulfill safety requirements of ISO13849.

Most of the time, these devices are directly connected to the internal machine network or at least to the HMI[7] device that is used to control the machine. Important from a security point of view is that this functionality is then physically accessible by any operator without any layer of security. Therefore, an attacker that managed to gain access to any of these components via network or direct access can reconfigure the PLC and exchange the implemented functionality triggered by the safety-off button with malicious code. Therefore, the safety-off functionality could be removed or exchanged by another (maybe even worse) action leading to severe injuries or environmental damages.

We are not the only ones to notice that. `https://www.controleng.com/single-article/machine-safety-iso-13849-1-status-interlock-switch-safety/b7973a7bc320b3ba7efea25c74cc3d15.html` reports on this. Thus, providing another example to our observations that unsuitable technology is used to achieve functional safety.

3.2 The machine is black box yet each component is security-relevant

Security of IT systems depends on security of each individual part of it, both hardware and software. Therefore, a system can be seen as one piece with a purpose (e.g. a multi-tier web application offering a defined service to the user) or as the individual pieces necessary to fulfill this service. Equivalently, a machine can be seen as a single system from a black-box perspective or by looking at it's individual components from a white-box view. There are different viewpoints by the stakeholders described in chapter 2.4. Accordingly, there are similar groups of stakeholders which viewpoints of a machine differ:

- *business leaders and commercial personnel* tend to see a machine as one big item with a purpose to produce specific goods
- user/operator: single machine with different parts (components) which together fulfill a certain purpose if the entirety of all components is functional
- *technicians*:
  - *electrical*: electrical wires, i.e. each part that (directly) consumes electrical energy counts
  - *mechanical*: mechanical components (e.g. cylinders, ...) which can break
  - *IT*: networked devices or network addresses or network cables and logical connections as far as known (not necessarily a strict one-to-one mapping)

[6] programmable logic controller
[7] Human Machine Interface

The above refers to the customer's point of view. The suppliers' personnel perspective is similar, but usually more specialized.

However, the security perspective of a machine has to be from a white-box view: every component that can be hacked/tampered with is considered critical. In a machine, there are usually no non-critical components for the machines availability like backup or maintenance components. Manufacturers only build in things that are relevant to be able to run the machine. And if there are any, these can still pose a threat to other components or other machines like any other networked device as they can be used as "jump hosts" to attack critical components. Additionally, directly interconnected devices or separate networks within a machine are often hidden from IT because they are under full control of the supplier or other technicians. These, however, still are part of the network as they are usually connected to a dual-homed device and therefore can be used for attacks.

Another interesting fact: within IT environments, there is usually a direct relationship of a requirement to a service offered in the network. Within OT environments, however, the core requirement is production of goods, while offered services in the network mostly have a supporting functionality. Therefore, unknown services can be existent on the network, which can facilitate an attack, although they are not necessary for operation or unknown at all.

As a consequence, due to lacking detailed information about a machine, security teams often only gain a black-box view. Their actually interest is different. They would need to have a white-box understanding and they would like to have access to all components and conduct individual security assessments (penetration tests). Usually, this would break warranties and contracts between manufacturers and the factory. In order to determine the necessary protection for the machine, the security team needs to gain detailed knowledge in some way. This includes functionality, manufacturer, type, firmware / operating system and installed software and its respective version(s) of all components within a machine. This knowledge can then be stored in an asset inventory. The inventory then serves as a basis for vulnerability and patch management.

From a technical perspective, there are multiple approaches to identify assets:

- the *manual approach* is a lot of work, which cannot be handled with only limited resources usually
- active and passive *network scans*, which could lead to availability and even safety impacts if errors occur during implementation of necessary components or scans
- evaluation of *machine documentation*, which can be incomplete or not understandable and usually is a lot of work due to different formats that cannot be parsed automatically

The approach used to identify assets therefore dictates the amount of work necessary while greatly influencing the completeness, level of detail and reliability of the result.

As industrial networks are usually very heterogeneous due to reasons described in section 3.3, the preparation and conduction of these steps is very time-consuming and therefore often not conducted at all or with reduced level of detail and care, resulting in limited information and, thus, overseen security risks[Ba18].

3.3 Insecure components that have to be used

Vendors of industrial automation technology often require the customer of a machine to use only specific, approved network components, for example switches. Within the observed environment, they justify this requirement as it is the only way to make sure that the machine works as intended considering "real-time" requirements of the machine's components that communicate across the network. They state that otherwise availability and safety of the machine could be impacted and cannot be guaranteed. However, they often fail to provide evidence for their requirements (i.e. provide specification or requirements of the protocols using the network infrastructure) or use known non-real-time components for other "critical" machine functionality in the same segment of the network.

If the factory operates non-supplier supported components or versions, the supplier will point to these as root cause of the problem without further analysis. OT security would benefit a lot from common security standards for manufacturers to use in development of their products. But security of their hardware and software is not one of their core objectives, as their main focus is on availability and safety.

Now, what is the issue with those components? They can have severe security issues as e.g. seen with a type of Siemens controllers (`https://www.sec-consult.com/en/blog/advisories/authentication-bypass-cross-site-scripting-in-siemens-sicam-rtus-sm-2556/`). It is common that old hardware and software is used for which security patches are not provided. The manufacturer may also not provide patches. This can be the case when the product reached end-of-life or is unsupported by the respective manufacturer for another reason. In many cases, exchange of these components is almost impossible due to required supplier support or cost constraints.

Also, if the former issues are all not applicable, the level of security tends to decrease by the number of different types of assets in a network. This is a maintenance problem as patch availability and necessity for all the different components with their different versions needs to checked. Required amount of human resources to achieve this is often not available.

Due to these reasons, there is a trade-off between safety, availability and security due to network components that affects industrial environments as the supplier requires to use their own components for availability and safety reasons, which in turn adds security problems. However, these can have an impact on availability and security again.

3.4 Impact of installing security patches

As stated before, suppliers usually focus on availability of a machine from a functional and technical perspective only. Therefore, we observed that they do not support installation of security patches on individual components in most cases and do not guarantee and test compatibility of security patches with their application. This, however, is important to achieve availability from a security perspective, i.e. availability of a machine and its components during and after an attack.

A second issue is the required downtime for system patching, which in turn reduces availability of the machine. Each security weakness has a risk assigned (e.g. CVSS score). Sometimes, the risk relevant to the target environment cannot be estimated. As availability is graded higher by business needs, hidden risks grow over time, which again can have an impact on availability when a security incident causes an outage.

3.5 Remote access for maintenance and management

Allowing a supplier remote access to the machine at the customer site can reduce downtime in case of a fault because the supplier can help faster, which has a positive impact on availability. However, confidentiality of data/information on the machine can be negatively affected when allowing remote access. Remote access may also enable other kinds of attacks. There are different remote access technologies:

- *direct connection* on network layer to the machine network via VPN technology across network, telephone or mobile network links
- *"screen sharing"* of the machine user interface or a engineering device through customer-operated technology

It is recommendable to record these sessions (non-encrypted) for later accountability and non-repudiation. This helps to understand liability in case of errors and helps with integrity as malicious software on the supplier's device might be detected when it tries to change something on the machine. Screen sharing solutions tend to provide better security: Confidentiality can be achieved as no undetected insight or large-scale extraction of data from the machine is possible and the supplier only sees the data shown by the machine operator or internal support personnel. A limitation of this approach is that the personnel may not have the knowledge to fully understand actions by the supplier and might not observe the actions with full attention.

Suppliers usually depend on special maintenance software, which needs to be available and be able to connect to the machine's components for error analysis. This can be achieved either if the supplier is able to connect to the machine via VPN solutions or if the customer

has an engineering device on-site with the required software that is connected to the machine network.

4 Conclusions

We have discussed the objectives of availability, safety, and security within production environments. The understanding of these terms differs among the stakeholders involved in the process. We also provided some examples from our own experience in an OT environment.

We conclude that in a connected industrial world, availability and safety cannot be seen as silo topics without considering the influence of security objectives. Our selected examples provide evidence that threats exist that can cause significant harm to today's production machines and environments. This can result into extended production outages or environmental or personal threats, which possibly leads to major financial problems to a single organization, business branch or even countries in case of critical infrastructures.

Future research topics could be threats originating from advanced malware, which can negatively influence all security objectives and cause safety problems as well as analysis of system changes for hidden threats.

References

[Ba18] Barbara Filkins, Doug Wylie: The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns. Survey, Escal Institute of Advanced Technologies, North Bethesda, MD, US, July 2018.

[IE10] IEC61508:2010: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. Standard, International Electrotechnical Commission, Geneva, CH, 2010.

[IE13] IEC62443-3-3:2013: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. Standard, International Electrotechnical Commission, Geneva, CH, 2013.

[IS18] ISO27000:2018(E): Information technology – Security techniques – Information security management systems – Overview and vocabulary. Standard, International Organization for Standardization, Geneva, CH, 2018.

[St10] Sterbenz, James PG; Hutchison, David; Çetinkaya, Egemen K; Jabbar, Abdul; Rohrer, Justin P; Schöller, Marcus; Smith, Paul: Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks, 54(8):1245–1265, 2010.

Addressing Security gaps in Industries seeking to adopt I4.0

Venesa Watson[1,2], Xinxin Lou[1,3], Yuan Gao[4] and Karl Waedt[5]

Abstract: The security challenges associated with Industry 4.0 (I4.0) have been well-reported, but little differentiation is made between the security challenges as a result of I4.0 versus those that are existent in industries seeking to become I4.0-enabled. It is essential that security gaps within current infrastructures are sufficiently addressed beforehand, as addressing them post I4.0 becomes a complex undertaking. This task necessitates a better understanding of the characteristics– such as performance requirements and governing standards - of these pre-I4.0 architectures to devise suitable solutions. For instance, it is seen that the automation industry is generally still in the infancy stage of cybersecurity and is further limited by strict safety requirements. Expansion of the auditing/monitoring capabilities within the automation environment is put forward as a starting point in addressing its security gaps, whilst also providing support for the specific requirements of this environment. I4.0 technology offers additional support in this regard, to further improve the security posture of the interconnected environments and the I4.0 architecture by large.

Keywords: security challenges; I4.0; performance requirements; auditing/monitoring capabilities; automation industry.

1 Introduction

Industrie/Industry 4.0 (I4.0) is a concept used to describe the 4th industrial revolution, where different sectors leverage state-of-the-art technological developments to enable a smart, connected manufacturing environment [PR17] [WT17]. As expressed by [WT17] [VA17] [Bl17] [Ca18], I4.0 faces several challenges that must be sufficiently addressed before this architecture becomes a reality. Among these challenges is security, which is normally discussed from the perspective of security challenges introduced by the I4.0 reference architecture model (RAMI). Insofar, studies have focused on questioning how I4.0 will address these security issues, submitting proposals in this regard [WT17] [Bl17] [C018] [De16]. It is reasonable for the I4.0 architecture to assume responsibility for some security challenges. For instance, the I4.0 goal to interconnect environments of

[1] Framatome GmbH, Henri-Dunant-Str. 50, 91058 Erlangen, venesa.watson@framatome.com: xinxin.lou@framatome.com
[2] University of Siegen, Faculty of Science and Engineering, Chair for Data Communication Systems, Hölderlinstraße 3, Siegen, 57068, venesa.watson@uni-siegen.de
[3] Bielefeld University, Department of Computer Networks and Distributed Systems, Universitätsstraße 25, Bielefeld, 33615, xlou@techfak.uni-bielefeld.de
[4] Otto-von-Guericke-Universität Magdeburg, Department of Technical & Operational Information Systems (ITI), Universitätspl. 2, 39106 Magdeburg, yuan.gao@ovgu.de
[5] Framatome GmbH, ICPGOP, Henri-Dunant-Strasse 50, 91058 Erlangen, karl.waedt@framatome.com

different criticalities, alone, widens the attack surface mainly for high-criticality systems. However, it is not emphasized enough that some of these *so-called* I4.0 security challenges are issues already existent in industries looking to adopt I4.0, and as such, should be addressed before becoming a part of the I4.0 architecture.

Reports on cyber-attacks indicate that existing security gaps are equally common to small-to-medium enterprises (IT/Information Technology) and automation industry (OT/Operational Technology), however, for the latter, security has been commonly accepted as compensatory rather than integral [WB18a] [WL17]. In general, the objectives (DoS, data exfiltration, etc.) of these cyber-attacks are similar across the both environments. Where differences are observed is in the approach followed in addressing the uncovered security gaps/vulnerabilities, as the incident response process is influenced by the security objectives and safety requirements characteristic of the environments [WB18a] [WL17] [CD13] [VT14]. The result is that, in comparison, IT environments have more options as it relates to security mechanisms that can be deployed. Contributing factors include: (1) IT and OT have different priorities - CIA vs. AIC; (2) the real-time requirements in OT restricts extent of control deployment; and (3) some legacy OT protocols (example, DNP3) work mainly on layer 2, thus IT security controls (example, IP-based filtering) cannot be applied. Furthermore, cybersecurity is still a relatively new topic is some OT environments, where faults are more readily accepted as a routine service failure and not a consequence of malicious activities [C018]. Both OT and IT environments necessitate an improved security posture to enable a more secure foundation for the interconnected I4.0 architecture. This will require a more comprehensive risk analysis to assess the impact of attacks against IT and OT environments and to drive the development and implementation of effective solutions. There is particular focus on the automation industry in this regard, as industry-players combine their efforts to address cyber-security in the OT environment. Several writers have indicated monitoring/auditing as a significant security gap to address to provide more oversight on network activities for detecting malicious activities [C018] [De16]. As a data-driven platform, I4.0 has the capabilities of providing additional analysis of monitoring data to further strengthen the security posture of the interconnected environments. It is postulated that industry-players can unlock this advantage once they increase the monitoring/auditing capacity of their systems.

This paper considers security in a specific automation industry to better understand the traditional approaches, then provides proposals on how to address these in preparation for I4.0 readiness. The security overview of the automation industry is presented in section 2. Arguments and proposals for increased monitoring are explored in section 3. Section 4 discusses opportunities with I4.0 for further security support. The conclusion is presented in section 5.

2 Security in the Automation Industry

In this paper, automation industry is used interchangeable with critical infrastructure, with specific focus on nuclear power plants as context for this analysis. Critical infrastructure describes physical and organizational structures that are essential for the maintenance of vital services important to a nation's economy and society, such as healthcare, energy production and transportation services [FO17] [EC18]. As such, highest priority is given to the protection of these systems, to ensure their resilience against serious threats. In recent years, these protective measures have become a recurring theme due to the upsurge in cyber-attacks launched at critical infrastructures [Cy18]. Swift action has been taken to implement additional measures necessary to protect against further attacks, however, this response is limited by the real-time requirements of the critical systems that make up these infrastructures. Traditionally, availability is given such high precedence in critical infrastructures that controls for integrity and confidentiality are normally unviable, especially where safety is considered [IN16]. Automation industries adopt a pyramid-scheme, which is the common industrial hierarchical network structure, where at least three (3) levels are defined (Fig. 1) [Ma16] [CE16].

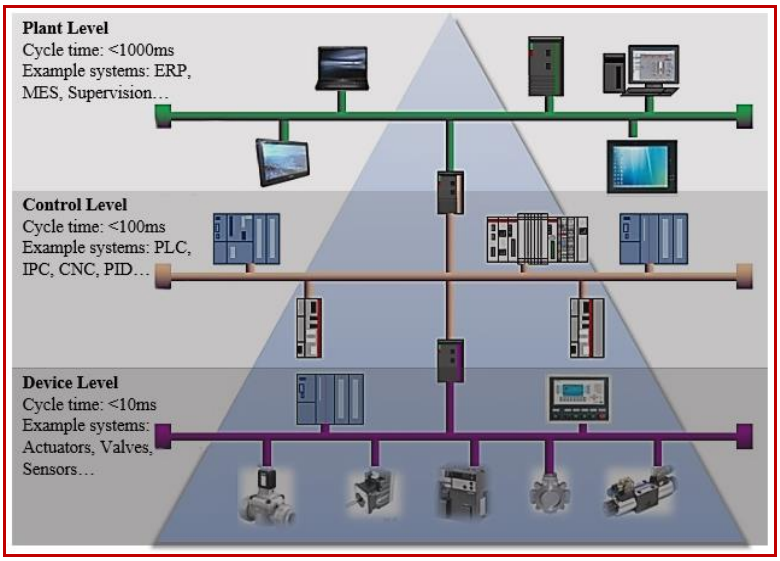

Fig. 1: Automation Pyramid [CE16]

The lowest levels are primarily concerned with the critical operations, where there is high speed transmission and modest data load that has a short life span [Ma16] [CE16]. In determining the controls that can be implemented, such factors must be considered. For instance, controls for confidentiality are unnecessary for data with a limited life span and is too intensive for time-critical applications. Integrity controls are also of concern due to the resource-intensive nature of cryptographic controls but can be nonetheless

demonstrated as useful for critical infrastructures. For instance, [Di11] exploited a Programmable Logic Controller (PLC) that is commonly used in automation industry, to demonstrate how the lack of integrity checks allowed an outsider to perform administrative-level commands. Even after additional security mechanisms were included in successive versions of this PLC, [Ma16] and [Mi17] again demonstrated that the system was still exploitable. The actions of the manufacturers and the subsequent successful attacks highlight the safety versus security paradox that is characteristic of some critical infrastructures - in that, security is both a risk and an asset to safety. The strict performance requirements of these infrastructures are normally dictated by highest safety requirements. This restricts the security mechanisms that can be implemented, as they can hinder safety. However, as demonstrated by the exploits of [Ma16] and [Mi17], limitations on security are also a safety risk. This safety versus security challenge must be sufficiently addressed to present a robust infrastructure for the I4.0 market.

2.1 Safety versus Security Paradox

Safety and security requirements for critical infrastructures are defined by national and international standards, for instance, HIPAA for healthcare and PCI DSS for the financial sector. As an example, this paper considers the nuclear power environment to describe an example of the safety versus security challenge. Therefore, standards from this environment, namely the IEC 62645 [IE16d] and IEC 62859 [IE16e] are referred.

IEC 62645, the top-level IEC cybersecurity standard for the nuclear domain, is concerned with cybersecurity requirements to reduce or eliminate the impact of an attack against digital Instrumentation & Control (I&C) systems. This standard makes recommendations for measures to prevent, detect and react to these attacks [IE16d]. In addressing security, IEC 62645 employs an approach based on the overall impact on plant safety, availability and equipment protection. The output of this approach is three security degrees, namely S3, S2 and S1 (highest severity) [IE16d] on top of baseline security requirements (BR). A nuclear I&C system is assigned a security degree based on the maximum consequences on the plant safety and performance following a successful cyber-attack on or involving that I&C system. When assessing the consequence of any cyber-attack, the impact on safety has greater importance than the impact on plant performance. Additionally, the I&C systems are to be considered from a functional perspective and assigned a security degree based on its most sensitive function - the one that results in the most severe impact, directly or indirectly, on plant safety and performance [IE16d] [WB18b]. IEC 61226 provides safety categories by which to classify these functions [IE05]. The assignment of the safety categories is based on the importance of the function in preventing DBE (design basis events) – that is, the group of design basis accidents and anticipated operational occurrences. Tab. 1 shows how the categorizations from both standards are related.

IEC 62645 Security Degrees and Criteria for Assignment	**IEC 61226 Safety Categories**
S1 - I&C programmable digital systems that process safety *category A* functions and those functions that could have the same impact on safety when maliciously manipulated.	**Category A** - the functions that play a principal role in the achievement or maintenance of NPP safety to prevent DBE from leading to unacceptable consequences
S2 - I&C programmable digital systems that process safety *category B* functions or those functions that could have the same impact on safety when maliciously manipulated.	**Category B** – the functions that play a complementary role to the category A functions in the achievement or maintenance of NPP safety, to prevent DBE from leading to unacceptable consequence
S3 - I&C programmable digital systems that, when attacked, cannot have a direct and immediate impact on plant safety or on the main nuclear process operation.	**Category C** - denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety

Tab. 1: IEC 62645 Security Degrees and IEC 61226 Safety Categories [IE16d] [IE05]

As observed with IEC 62645 and IEC 61226, safety has the highest priority in a nuclear infrastructure and is the determining factor for the application of security measures in this critical environment. The classification schemes indicate that stringent security measures are required for the most sensitive systems, however, what is not dictated is the appropriate measures that can be implemented. In a report published by the IAEA [IN16], the writers mentioned that "*while there are many elements that are common to safety and security, there are also challenges related to differences in approach and culture between the two disciplines*". As an example, [IN16] posits that the implementation of delay barriers for security reasons can serve to bar unauthorized personnel from certain areas or systems, but during safety or emergency situations, this security feature can limit rapid access to respond to the event. [IN16] goes on to highlight the need for a coordinated approach to nuclear safety and security to ensure they complement each other in a seamless and effective way. This cannot be achieved solely through the actions of nuclear industry partners and necessitates the commitment of security service providers to design controls suitable for the requirements of critical infrastructures. The safety & security interface is explicitly addressed by the new IEC 62859 [IE16e] on "*NPPs – I&C – Requirements for coordinating safety and cybersecurity*". This corresponds to some extent to the more general IEC TR 63069 on "*Industrial-process measurement, control and automation- Framework for functional safety and security*" developed by IEC TC65 WG20, currently targeted for publication in 2019. It is envisioned that this new standard will provide additional support in addressing safety and security to achieve a more robust infrastructure. But in the meantime, the next section describes how increased capacity for monitoring/auditing provides an avenue by which security in an automation industry can be addressed. The

overall aim is to highlight opportunities to reduce the safety versus security paradox to an excuse rather than a hindrance to ensuring highest security, and by extension, achieve increased I4.0 readiness.

3 Extending Monitoring/Auditing Capabilities

As gleaned from the analyses in [WB18a] [VT14] [Di11] and [Mi17], strict controls for confidentiality and integrity are essential for automation industries to realize the level of security required for I4.0. Confidentiality controls preserve privacy and ensures authenticity of systems and users, whilst integrity ensures trustworthy communication on the network. Security mechanisms for integrity and confidentiality include cryptographic controls (digital signatures, hashes, encryption, and so forth) that are commonly accepted as expensive, resource-intensive and possible hindrances to safety. However, considering that an attack against a critical infrastructure can result in serious consequences for life and environment, it is of utmost importance to deploy measures for highest security.

The study in [WB18a] lightly touched on the need for greater auditing in an automation industry. Here, the argument was based on a *so-called* cyber-prank exploit by which the monitoring system of an automation system was manipulated to indicate an error where there was none. This study postulated that an expansion of the already present forensic (auditing) capabilities is suitable to address this weakness. However, a more holistic approach is needed to quantify the need for further auditing capabilities. This necessitates a closer look into the current state of auditing within automation industries and the limitations that must be considered before these can be expanded. Fig. 1 depicts the typical automation pyramid network, which not only dictates the performance at each level but also influences the effectiveness of monitoring services. As indicated in [WB18a] and [C018], monitoring services do exist in OT environments; however, their scope of application is affected due to the segmentation of the networks [C018]. "*This means that sensors need to be placed at a number of different layers within the network in order to monitor activity*" [C018]. This is neither an easy or inexpensive undertaking; nevertheless, it may become necessary in light of the targeted attacks launched at critical infrastructures in recent years, especially where no appropriate isolation measures (like limitations to point-to-point network connections or physically unidirectional data diodes) can be enforced.

Expansion of the auditing capabilities is among the most viable solutions, as it does not require the introduction of intensive measures that are unfavourable for some critical environments. However, there are concerns as to how this expansion could affect network load. In that, the solution introduces additional network traffic that could cause unfavourable delays, possibly significant enough to affect safety. IEC 62645 [IE16d] and IEC 62859 [IE16e] find relevance here – as mentioned in previous sections, these standards dictate a security categorization approach wherein which users can sufficiently qualify and quantify risks based on their impact on safety. Essentially, expanding

auditing capacity does not translate to an unchecked security mechanism. Effective use of IEC 62645 and other industry-specific security standards can enable users to focus their efforts. That is, auditing capabilities should be introduced to network segments or systems following the risk analysis to validate these implementations. For example, as shown in [WB18a], the proposed forensics capabilities focused on network data that directly interacted with the vulnerable service, that is, the LEDs that formed a part of the monitoring system. It must also be noted that this is not a '*silver bullet*' solution, as the implementation of additional security controls in an environment in cybersecurity infancy will require change in behaviour. It must become routine for the data from these security controls to be reviewed instead of merely focusing on returning a system to normal operation following an event [C018] [De16]. Furthermore, as the I4.0 infrastructure moves away from the traditional pyramid structure [CE16] to a pillar structure [Gr17], this will remove the limitation with the scope of application as restricted by the segmentation of the automation pyramid. Also, I.40 will adopt a communication standard that categorizes traffic according to at least four (4) classes to differentiate between criticality [BR17] [IE16a]. This provides better control over network traffic in preventing high-critical traffic from being affected by less-critical traffic. In this sense, the increase of monitoring traffic on the network need not affect the performance requirements (e.g. timely delivery of high-critical traffic). Additional advantages with I4.0 technology are mentioned in the next section.

4 Security Opportunities with I4.0

I4.0 architectures are realized by the interconnection of different industries, and so will see different systems and protocols with varying functional requirements and criticality sharing a network. Challenges in achieving such architecture include security, interoperability, privacy and IT/OT convergence, which are addressed by the standards community. This has stimulated the development of technology that overcomes these I4.0 challenges to further its realization. Reports highlight time-sensitive Ethernet technology that can support critical networks and are ideal for I4.0. Examples include TTE (Time-Triggered Ethernet), AVTP (Audio/Video Transport Protocol), AFDX (Avionics Full Duplex Switched Ethernet) and OPC UA/TSN (Open Connectivity Unified Architecture over Time-Sensitive Networking), where the latter is earmarked as the forerunner for I4.0 [BR17] [IE16b] [AR09] [IE16a] [Ch15] [GE16].

Serial (or legacy) communication technology remains in popular use in some automation industries, as they are fit-for-purpose and simple to install and maintain. However, as seen with the introduction of Industrial Ethernet technology, such as Modbus TCP/IP and PROFINET, industry players are considering the implementation of more powerful technology (in terms of speed and scalability) that supports time-critical requirements [BR17] [GE16]. Ethernet, although a globally-accepted technology offering increased transmission speed, scalability and interoperability, does not support real-time communication. As such, manufacturers of Industrial Ethernet add extensions to support

this requirement, for example, as seen with PROFINET [Ve07] [PR18]. These Ethernet-based standards, namely TTE, AVTP, AFDX and OPC UA/TSN include extensions to provide a more reliable communication medium. Besides the services and mechanisms for traffic categorization, traffic-shaping, traffic-policing, time synchronization and bounded latency that these standards implement to support time-critical and mixed-criticality networks [BR17] [IE16b] [AR09] [IE16a] [Ch15] [GE16], the use of Ethernet also provides an opportunity for security in OT environments. This is a somewhat contradictory statement, given that Ethernet is not regarded as a secure technology. The emphasis however, is placed on the fact that Ethernet is compatible with a host of available security controls that have been so far unviable in OT. But it must be noted that these security controls are largely impractical for time-sensitive communication. Researchers, manufacturers, the standards community and other industry partners are developing and testing solutions in this regard [BR17]. For example, OPC UA/TSN resulted from this combination of competencies to demonstrate how the strengths of an Ethernet-based technology for real-time support (TSN) and a security and interoperability standard (OPC UA) can be pooled to bring about an I4.0-enabled platform [BR17]. Furthermore, AREVA (now, Framatome GmbH) has successfully demonstrated the applicability of OPC UA for monitoring systems in a nuclear environment [WT17]. An additional enabling-technology is seen with the establishment of lightweight MACs (message authentication codes) for resource-constrained infrastructures [IS16]. Available research demonstrates implementations of open and proprietary lightweight MAC schemes in Internet of Things (IoT) infrastructures, such as the smart grid, health systems and automotive networks [KT15] [FF11] [MS15]. Successful implementations were shown to satisfy the desirable security requirements of the target environment, whilst also preserving the performance requirements of the same [KT15] [FF11] [MS15]. Analysis of the performance and security of these schemes show the reduced resource/energy usage and resistance to different types of attacks, such as replay, data manipulation and spoofing. As IoT is an enabling technology for I4.0, it is reasonable to say that these demonstrations indicate that the use of cryptographic controls is possible in I4.0.

The cybersecurity foundation of I4.0 is provided by the IEC 62443-x-x series of standards. These assure that I4.0 relies on well proven concepts, even if not all standard parts of the IEC 62443 series are published yet. These are complemented by specific security standards like IEC TR 62541-2 [IE16c] on the OPC UA Security Model. In the nuclear IEC cybersecurity context, the new IEC 63096 on graded security controls for different lifecycles (platform development, engineering and integration, operation and maintenance) is providing streamlined recommendations on graded security controls based on both the IT security standards, like ISO/IEC 27002 [IS13] with its downstream standards as well as the applicable security controls from the IEC 62443 series.

A recent overview of further standards relevant in this context can be found in the Security Standards White Paper for Sino-German Industrie 4.0 / Intelligent Manufacturing, from April 2018 [SG18b]. The "*Intelligent Manufacturing*" is part the "*Manufactured in China 2025" program that corresponds to the German "Industrie*

4.0" [SG18a] [SG18b]. Accordingly, this overview also lists several Chinese OT related standards that are being developed at a faster pace as compare to the IEC standardization processes.

There are additional perceived and demonstrable opportunities that automation industries can obtain from these state-of-the-art technologies, but the implementation challenges are considerable, as additional testing is needed to establish proof-of-concept. Further, the replacement of legacy systems is not an entirely feasible or practical undertaking. One point of consideration for industry partners is placing these systems into dedicated security zones and using improved monitoring capabilities to detect malicious activities among these systems. Significant planning is needed to reap the benefits of extended monitoring capabilities, particularly to ensure that the collected data is within the realm of useful data for investigations and also that the data is actually used.

With the continued commitment and combined efforts of industry, standard bodies and vendors, foreseeable security challenges can be sufficiently addressed with meticulous planning.

5 Conclusion

As safety will always have the highest importance in critical environments like NPPs, it is vital to understand how safety and security intertwine, to define a complementary relationship. The I4.0 industrial revolution has driven technological advancement that provides opportunities to support improved safety-security balance, but industry partners need to extend the capabilities of their systems to realize these benefits. Monitoring/auditing capabilities have been highlighted as a worthwhile avenue in this regard, to provide additional insight on network activities so that malicious activities can be detected and investigated. With further security analysis of automation systems, the security posture of automation industries can be further assessed to direct the identification and implementation of additional mechanisms needed to achieve highest safety and security.

Acknowledgements

Some of the addressed cybersecurity related topics are being elaborated as part of AREVA GmbH's participation in the "SMARTEST" R&D (2015-2018) with German University partners, partially funded by German Ministry BMWi.

Bibliography

[Ez10] Ezgarani, O.: The Magic Format – Your Way to Pretty Books. Noah & Sons, 2010.

[AR09] Aeronautical Radio Inc (ARINC) Specification 664: aircraft data network, part 7 deterministic networks.

[Bl17] Bligh-Wall, S.: Industry 4.0: Security imperatives for IoT — converging networks, increasing risks, https://www.henrystewartpublications.com/sites/default/files/Bligh-Wall.pdf, accessed: 1/08/2018.

[BR17] B&R Automation. OPC UA TSN – field-tested, field-proven. https://www.br-automation.com/smc/e19f6c3e6ebdf58307c92f8a2f1a56b2cb6f3207.pdf, accessed: 1/08/2018.

[Ca18] Cabrera, E.: How the Industry 4.0 Era Will Change the Cybersecurity Landscape. https://blog.trendmicro.com/how-the-industry-4-0-era-will-change-the-cybersecurity-landscape/, accessed: 1/08/2018.

[CD13] Cheminod, M., Durante, L. and Valenzano, A.: Review of Security Issues in Industrial Networks. In: IEEE Transactions on Industrial Informatics 9 (1), pp. 277-293, 2013.

[CE16] Calvo, I., Etxeberria-Agiriano, I. Iñigo, M. A. and González-Nalda, P.: Key Vulnerabilities of Industrial Automation and Control Systems and Recommendations to Prevent Cyber-Attacks. In International Journal of Online Engineering (iJOE), pp. 9-16, 2016.

[Ch15] Chaudron, J: TTEthernet theory and concepts. http://etr2015.irisa.fr/images/presentations/TTEthernet_ETR_2015_Rennes.pdf, accessed: 1/08/2018.

[Co18] Cooke, A. Rising to the Industry 4.0 cybersecurity challenge. https://www.theengineer.co.uk/industry-4-0-cybersecurity/, accessed: 1/08/2018.

[Cy18] Cyberbit. Why more cyber attacks on critical infrastructure are expected. https://www.cyberbit.com/blog/ot-security/cyber-attacks-on-critical-infrastructure/, accessed: 1/08/2018.

[De16] Deloitte: Cyber Risks in Advanced Manufacturing. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf.

[Di17] Dillon Beresford: Exploiting Siemens Simatic S7 PLCs. https://media.blackhat.com/bh-us-11/Beresford/BH_US11_Beresford_S7_PLCs_WP.pdf, accessed: 1/08/2018.

[EC18] European Commission: Critical infrastructure. https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en, accessed: 1/08/2018.

[FF11] Fouda, M., Fadlullah, Z., Kato, N., Lu, R. and Shen, X.: Towards a light-weight message authentication mechanism tailored for Smart Grid communications. In: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1018-1023, 2011.

[FO17] Federal Office for Information Security: Recommendations for critical information infrastructure protection. https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html, accessed: 1/08/2018.

[GE16] GE Fanuc. TTEthernet – a powerful network solution for advanced integrated systems. https://bcourses.berkeley.edu/files/66071161/download?download_frd=1&verifier=wt3Ass5zlL3xWAIaWeTTBxZKQt2KKVeOChJzXh5r, accessed: 1/08/2018.

[Gr17] Greenfield, D.: Automation networks: from pyramid to pillar, https://www.automationworld.com/automation-networks-pyramid-pillar, accessed: 16/11/2017.

[IE05] IEC 61226 Nuclear power plants –instrumentation and control systems important to safety – classification of instrumentation and control functions.

[IE16a] IEEE 1722-2016: IEEE standard for a transport protocol for time-sensitive applications in bridged local area networks." December 16, 2016.

[IE16b] IEC TR 62451-1:2016 OPC unified architecture – part 1: overview and concepts.

[IE16c] IEC TR 62541-2:2016 OPC unified architecture - Part 2: Security Model

[IE16d] IEC 62645 Nuclear power plants - instrumentation and control systems - cybersecurity requirements

[IE16e] IEC 62859:2016 Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity

[IN16] International Nuclear Safety Group (INSAG). The interface between safety and security at nuclear power plants. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1472_web.pdf, accessed: 1/08/2018.

[IS13] ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls

[IS16] ISO/IEC 29192-1 Information technology -- Security techniques -- Lightweight cryptography -- Part 1: General

[KT15] Khemissa, H. and Tandjaoui, D.: A lightweight authentication scheme for e-health applications in the context of internet of things. In: 2015 Ninth International Conference on Next Generation Mobile Apps Services and Technologies (NGMAST), pp. 90-95, 2015.

[Ma16] Masood, R. Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives. https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/GW-CSPRI-2016-03+MASOOD+Rahat+Nuclear+Power+Plant+Cybersecurity_0.pdf, accessed: 1/08/2018.

[Mi17] Miru, G. The Siemens S7 Communication - Part 1 General Structure. http://gmiru.com/article/s7comm/, accessed: 1/08/2018.

[MS15] Mundhenk, P., Steinhorst, S., Lukasiewycz, M., Fahmy, S. and Chakraborty, S.: In: Lightweight authentication for secure automotive networks. In: Design, Automation & Test in Europe Conference & Exhibition, pp. 285-288, 2015.

[PR17] Pereira, A. C. and Romero, F.: A review of the meanings and the implications of the Industry 4.0 concept. In: Manufacturing Engineering Society International Conference (MESIC) 28-30 June, Spain, pp. 1206-1214, 2017.

[PR18] PROFIBUS & PROFINET International. Profinet industrial Ethernet for advance manufacturing. http://us.profinet.com/technology/profinet/, accessed: 1/08/2018.

[SG18a] Sino-German Industrie 4.0/Intelligent Manufacturing Standardisation Sub-Working Group. Alignment Report for Reference Architectural Model for Industrie 4.0/Intelligent Manufacturing System Architecture, https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/hm-2018-manufacturing.pdf?__blob=publicationFile&v=2, accessed: 1/08/2018.

[SG18b] Sino-German Industrie 4.0/Intelligent Manufacturing Standardisation Sub-Working Group. Security Standards White Paper for Sino-German Industrie 4.0/Intelligent Manufacturing, https://www.dke.de/resource/blob/1711300/9e7add87021790df6d2dc57312e05302/security-standards-white-paper-for-sino-german-industrie-40-data.pdf, accessed: 1/08/2018.

[SR18] Spenneberg, R., Bruggemann, M. and Schwarte, H.: PLC-Blaster: a worm living solely in the PLC. https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf, accessed: 1/08/2018.

[VA17] Vaidya, S., Ambad, P. and Bhosle, S.: Industry 4.0 – A Glimpse. In: 2nd International Conference on Materials Manufacturing and Design Engineering (ICDMM), 11-12 Dec, Aurangabad, India, pp. 233-238, 2017.

[Ve07] Verwer, A.: Overview and applications of PROFINET. https://pdfs.semanticscholar.org/presentation/d085/b744bcf11e88f99c76acd0cbee22c29de502.pdf, accessed: 1/08/2018.

[VT14] Vazan, P., Tanuska, P., Kebisek, M. and Duchovicova, S.: Safety of Industrial Networks. In: International Journal of Computer, Electrical, Automation, Control and Information Engineering, 8 (12), pp. 2117-2120, 2014

[WB18a] Watson, V., Bajramovic, E., Bejiga, M. and Waedt, K.: Designing Trustworthy Monitoring Systems - Forensic Readiness for Safety and Security. In: 12th International Conference on Reliability Maintainability and Safety (ICRMS), Shanghai, China, 2018. (not yet published).

[WB18b] Watson, V., Bajramovic, E., Lou, X. and Waedt, K. Example of graded and lifecycle phase-specific security controls for nuclear I&C and ES use cases. In: 26th International Conference on Nuclear Engineering (ICONE26), July 22-26, 2018. (not yet published).

[WL17] Watson, V., Lou, X. and Gao, Y.: A review of PROFIBUS protocol vulnerabilities - considerations for implementing authentication and authorization controls, In: 14th International Conference on Security and Cryptography (SECRYPT), Madrid, Spain, pp. 444-449, 2017.

[WT17] Watson, V., Tellabi, A., Sassmannshausen, J. and Lou, X.: Interoperability and Security Challenges of Industrie 4.0. In: GI INFORMATIK, 25-29 Sept, Chemnitz, Germany, pp. 973-986, 2017.