Investigation of Resource Constraints for the Automation of Industrial Security Risk Assessments

Marco Ehrlich*, Georg Lukas‡, Henning Trsek*, Jürgen Jasperneite* and Christian Diedrich†
*inIT - Institute Industrial IT, TH OWL, Lemgo, Germany
Email: {marco.ehrlich, juergen.jasperneite, henning.trsek}@th-owl.de
‡rt-solutions.de GmbH, Industrial Security, Cologne, Germany
Email: lukas@rt-solutions.de
†Institut für Automatisierungstechnik, Otto von Guericke University, Magdeburg, Germany
Email: christian.diedrich@ovgu.de

***Abstract*—The current static risk assessment processes and concepts do not match the increasing requirements with regard to flexibility within the industrial automation domain. The amount of manual tasks and needed efforts for risk assessments are too high in order to adequately cover the rising rate of system reconfigurations. Analysing the typical risk assessment processes from the IEC 62443 will show resource constraints with regard to time, bottlenecks, and the main cost drivers. If the most rewarding process steps can be identified and automated, the overall performance of risk assessments can be enhanced to keep up with the demanded flexibility.**

***Index Terms*—Automation, Security, Tool Market Analysis, Risk Assessment, IEC 62443**

I. Introduction

The ongoing Industrie 4.0 (I4.0) developments are enabling a disruptive paradigm change within the industrial automation domain leading to a more complex interconnection and the break-up of the traditional automation pyramid. In addition, the digitalization degree of the Operational Technology (OT) environments is steadily increasing by the rising adoption of Information Technology (IT) approaches [1]. Physical and virtual worlds will be brought together resulting in leading-edge Cyber-Physical Production Systems (CPPSs) that enable a holistic communication addressing the demands of globally distributed volatile and competitive markets, e.g. adaptable manufacturing with lot size one or customer-specific and intelligent products.

In this context, high-level specifications for future industrial systems foresee a hybrid landscape of communication networks containing pervasive wired and wireless (also often legacy or isolated) solutions intertwined. Simultaneously, improvements on the overall performance of heterogeneous networking infrastructures are required in a reliable, secure, and automated way [2]. Nevertheless, the current situation inside the OT domain differs from these described visions due to the architectures, which have been developed in a highly specialized manner, are often not networked, and are dedicated to particular applications with special requirements, such as determinism, a high availability, and long system lifetimes [3]. This prevalent heterogeneity results in increased efforts, time, and resources required for planning, installation, configuration, and maintenance of the underlying systems during their whole lifecycle. This highly dynamic mixture of systematic, organisational, and technological advances needs to be investigated from the viewpoints of safety (protection of humans, machines, and environment) as well as security (protection of machines from human attacks). Only thereby, a safe and secure operation of the upcoming modular CPPSs can be guaranteed. Therefore, safety and security are intrinsically obligatory factors for the overall success of I4.0 [4]. This work will focus on the aspects of industrial security, especially the intrinsically mandatory process of risk assessment for modular CPPSs as a basic foundation for security.

The proposed flexibility of future CPPSs results in various new attack vectors for the industrial automation domain with regard to security causing a predicted global loss of $6 trillion by 2021 [5]. Regularly reported incidents inside the OT domain are, e.g. cyber attacks, stolen passwords, data breaches, espionage, or ransomware. Prominent examples of attacks against industrial companies are Stuxnet (2010), BlackEnergy (2012), Havex (2014), NotPetya (2017), WannaCry (2018), LockerGoga (2019), and DarkSide (2021) [6]. These attacks result in huge financial and reputational losses for the victim companies. They evidently show the increasing gap between the speed of digitalisation with focus on flexibility and the required improvements in the area of security for the industrial automation domain [5].

The remainder of this work is organized as follows: The next Section II contains the current challenges, the motivation, and the problem statement of this work. In Section III the state of the art with regard to standardization activities for this domain, especially the IEC 62443, is shown. Afterwards, Section IV presents the required market analysis of tools which already support risk assessment steps. The focus of this work is introduced in Section V by specifying and discussing the evaluated results from the practical risk assessments following the IEC 62443-3-2 process. Section VI concludes this work and provides an outlook towards the future work.

II. Motivation

The introduced developments take place in a global environment where cyber attacks and critical information infrastructure breakdown were the most dangerous global technological

risks in 2020 becoming a common hazard for individuals, businesses, and society [7]. At least 70% of the businesses perceive the corresponding risks as high or moderate and include them into their overall risk profiles with corresponding strategic decisions [8]. For example in Germany mechanical and plant engineering is a key sector and the driving force behind the economy with Small and Medium-sized Enterprises (SMEs) being the largest industrial employers and one of the most innovative and leading industrial sectors [9]. Unfortunately, the application of security-related standards is hindered by a lack of expertise and resources exactly there and just 41% of the companies are able to apply at least one of the most common security standards, despite the fact that more than 80% of the companies know about the issues [9]. Security compliance takes up more than 30% of resources in smaller organizations [10]. Due to a recent case study this results in a drastic situation where 100% of companies have network connections into their OT environments with around 66% of direct connection to the public Internet, but 0% have the corresponding security standards and Incident Response (IR) mechanisms in place [11]–[13]. This also applies to the management of risks, which is a fundamental pillar of OT security. Around 75% have never conducted an OT risk assessment or just do not know about it [14]. In general, a huge variety of challenges arises which need to be solved in order to secure the upcoming developments within the I4.0. The following list shows an excerpt of the overall challenges evaluated by their importance for this work:

1) Supporting security with software tools for a higher degree of automation [15], [16]
2) Capturing and formalizing of expert knowledge from the industrial automation domain [16]–[18]
3) A dynamic threat and attacker landscape requiring flexible security approaches [15]
4) Guarantee completeness and correctness of the assessments with regard to risk management [19]
5) Coverage of all security objectives during the complete lifecycle of an asset [16], [17], [20]
6) Asset identification and management of available information, interfaces, and data models [15], [17], [18]

Taking the identified challenges and the current state of security within industrial companies into account, a huge amount of improvements is possible for the applied risk assessment processes. Every CPPS needs a continuous safety certification to be operated and to comply with all the regulative requirements imposed by present laws, e.g. according to the Machinery Directive 2006/42/EG for the European markets. This results in a need for safety risk assessments after every functional change of a CPPS. The corresponding security risk assessment is mandatory as well and its importance enhanced due to the surge of recent security incidents, publicly available vulnerabilities, the currently intensifying threat landscape, and the increasing extent of possible damage. Currently, every modified CPPS configuration has to be manually assessed by security domain experts. This imposes high efforts that lead to a trade-off between the dynamics of the adaptation of reconfigurable production processes and their security. This is due to the fact that today's relevant standards originally being designated for static systems need to be applied manually with a necessity for domain-knowledge in a consistent and iterative cyclic manner. In addition, there are extensive standardization activities with various stakeholders from different domains, which have their own distinctive best practices and guidelines. This results in a broad suite of standards, which is too complex to establish for the majority of companies and especially for SMEs with regard to costs, time, and general resources [21].

To support the vision of I4.0 with a sufficient level of security, it will be necessary to meet the needed security requirements and certifications in an automated way and to reduce the current static procedures and manual efforts as much as possible. Consequently, the modelling and integration of security with a focus on OT is required for future industrial systems. In addition, the resulting increase of the automation degree and usability will harden the industrial systems with higher availability and robustness. This includes benefits for all involved stakeholders, such as component manufacturers, system integrators, or asset owners, with their respective security responsibilities [22].

The overall aim of this work is to propose an evaluation methodology in order to investigate the required efforts and resources for the process of industrial risk assessment basically consisting of two main dimensions, namely the required competence and the available tool support. Three Research Questions (RQs) have been formulated to serve as a scoping framework for this work:

- RQ 1: What is the status of available tools for industrial risk assessments? (Market Analysis)
- RQ 2: What are the required skill levels to perform typical risk assessment tasks? (Knowledge Requirement)
- RQ 3: What are the most rewarding parts of risk assessments to be automated in the future? (Future Automation)

III. State of the Art

In order to meet the demanded security levels and to achieve the overall desired security objectives of availability, integrity, and confidentiality, globally security-related standards, best practices, and regulations are proposed [3]. Although there is never a 100% guarantee to build a secure system, these proposals try to provide frameworks for stakeholders in order to perform evaluations, audits, and hardening with their systems to be secure against the majority of attacks or at least to become unrewarding for possible adversaries. In general, these standards help organizations to describe the current and target states regarding security, identify and prioritize opportunities for improvement with, e.g. countermeasures, evaluate the corresponding processes, and communicate the findings towards all relevant stakeholders. Therefore, each specified system configuration has to be manually assessed by domain experts to see whether it fulfils the demanded security requirements or not [23].

The common rule of thumb for IT as well as for OT environments is to perform security-related activities in a continuous manner as stated inside, e.g. the ISO/IEC 27005 standard. This is described within the Plan, Do, Check and Act (PDCA) cycle and the corresponding Information Security Management Systems (ISMSs). These actions are generally used to raise awareness for security, to assign responsibilities and clarify processes, to incorporate the business management, and to maintain technical procedures for, e.g. risk management, incident handling, auditing, and training. For the OT domain the IEC 62443 family of standards is the most important framework for security-related topics. In addition, it offers the Defense-in-Depth strategy including a collection of activities to establish a secure development, production, and operation of, e.g. industrial assets. The IEC 62443 adopts various approaches from the IT domain for the OT environments. This includes ISMSs and the definition of a Security Program (SP) containing eight Security Program Elements (SPEs) for a continuous evaluation of all aspects of security in a continuous and integrated manner.

One of the basic pillars for all the above mentioned security-related activities is Risk Management (RM) covering social, technical, and organisational aspects which need to be integrated into company activities. Nevertheless, RM is currently mainly based on static and manual efforts, is not covered by automated tools, is often neglected in daily business, and generates additional costs for every company, but especially inside SMEs with smaller budgets and less resources. The general framework for RM within IT environments is described in the ISO/IEC 31000 standard, which specifies all required methods for a holistic RM application in organizations. Further references are the ISO/IEC 31010, NIST 800-82, NIST 800-30, or NIST 800-39. In contrast, the OT domain offers own processes to support industrial stakeholders with an approach to establish secure production plants and factories with regard to RM. The standards of choice here are the German VDI/VDE 2182, which is also referred to inside the IEC 62443-2-1, and on a more global scale the IEC 62443-3-2. Due to its popularity and distribution worldwide and its novelty, the IEC 62443-3-2 standard is chosen as a focus of this work.

The IEC 62443-3-2 standard specifies the security risk assessment procedure for system design within the industrial automation domain for Industrial Automation and Control Systems (IACSs). It can be used by organizations in order to assess risks and to apply countermeasures with regard to the defined seven categories of Foundational Requirements (FRs). The whole procedure is based on the application of zones (grouping of logical or physical assets sharing common security requirements) and conduits (logical grouping of communication channels sharing common security requirements) as a fundamental concept from the IEC 62443-1-1. In general, the standard describes how to frame the investigated system, to partition it into zones and conduits, to assess the corresponding risks, to establish target security levels (SL-T), and to document the results. The whole process consists of seven main Zone And Conduit Requirements (ZCRs) (1-7), each representing a high-level step needed for a holistic RM and being divided by a various amount of sub steps.

- ZCR 1: Identify the System under Consideration (SUC)
  1) Identify the SUC perimeter and access points
- ZCR 2: Initial cyber security risk assessment
  1) Perform initial cyber security risk assessment
- ZCR 3: Partition the SUC into zones and conduits
  1) Establish zones and conduits
  2) Separate business and IACS assets
  3) Separate safety related assets
  4) Separate temporarily connected devices
  5) Separate wireless devices
  6) Separate devices connected via external networks
- ZCR 4: Initial risk exceeds tolerable risk?
  1) Compare initial risk to tolerable risk
- ZCR 5: Perform a detailed cyber security risk assessment
  1) Identify threats
  2) Identify vulnerabilities
  3) Determine consequence and impact
  4) Determine unmitigated likelihood
  5) Determine unmitigated cyber security risk
  6) Determine SL-T
  7) Compare unmitigated risk with tolerable risk
  8) Identify and evaluate existing countermeasures
  9) Reevaluate likelihood and impact
  10) Determine residual risk
  11) Compare residual risk with tolerable risk
  12) Identify additional cyber security countermeasures
  13) Document and communicate results
- ZCR 6: Document cyber security requirements, assumptions, and constraints
  1) Cyber security requirements specification
  2) SUC description
  3) Zone and conduit drawings
  4) Zone and conduit characteristics
  5) Operating environment assumptions
  6) Threat environment
  7) Organizational security policies
  8) Tolerable risk
  9) Regulatory requirements
- ZCR 7: Asset owner approval
  1) Attain asset owner approval

For the complete contents of the IEC 62443-3-2, please refer to the reference itself. This section should just summarize the most important points in order to make the following evaluation more comprehensible.

IV. Tool Market Analysis

In addition to the summary of the necessary standardisation activities, a high-level market analysis of the available tools within the industrial RM domain was performed. The idea is to propose a categorisation of typical tools, which can be used as support for risk assessments, and to enhance these categories with the corresponding automation degree of the tool and the

covered risk assessment steps (ZCRs) from the IEC 62443-3-2 standard. The results are shown here in the following paragraphs consisting of five categories plus one sixth category for the research-based approaches. The evaluation of the tool-based automation degree is based on the taxonomy of Level of Autonomy (LOA) consisting of six levels and being inspired by the definitions from the automotive sector [24]. It is based on the two key dimensions with regard to the scope of the automated tasks and the role of the human operator. The taxonomy can also be interpreted as an indicator on how much creativity (equaling a certain unpredictability) is required and how easy tasks can be formalised and repeated in order to be automated. The following list describes the different levels in an abstract way. The presented tool examples in the following subsections are presented without any personal preference, supportive funding, or certain order.

- No autonomy, humans are in full control of the system without any assistance (LOA 0)
- Assistance with or control of subtasks, humans are always responsible, specifying set points (LOA 1)
- Occasional autonomy in certain situations, humans are always responsible, specifying intents (LOA 2)
- Limited autonomy in certain situations with alerting of issues, humans confirm act as a fallback (LOA 3)
- System in full control in certain situations, humans might supervise (LOA 4)
- Autonomous operation in all situations, humans may be completely absent (LOA 5)

1) Documentation: The definition of workplace-related dangers and the creation of the corresponding high-level reports are general tasks for nearly every responsible in all domains. With regard to industrial risk assessments this implies the documentation of the identification, analysis, and evaluation of risks in a comprehensible manner to be compliant with the requirements from the applicable standards. Nowadays the typical tools used for this task are the classical office software suits for writing texts, creating tables, and drawing figures. Various templates for these tasks are also freely available on the public Internet. The given tools are not able to assist the human operator with certain tasks resulting in no autonomy at all.

- ZCR Coverage: 5.13, 6.1-6.9 & 7.1
- LOA: 0

2) Checklists: This category of tools can be understood as an entry point to the topic of security for companies of every size and state of security. They contain standardised checklists in the form of a questionnaire mostly based on international standards which have to be answered by the user in order to give an estimation about the security level. The most famous one for the OT domain is the Cyber Security Evaluation Tool (CSET)[1]. Light and Right Security ICS (LARS ICS)[2] works in a similar way but lacks current updates and is still in a reworking phase by German authorities. Another example is the Microsoft ThreatModeler[3] which was originally designed for STRIDE-based RM inside IT environments and yet the implemented concepts could theoretically be adapted towards the OT domain. The presented tools can support the human operator with special subtasks, such as automatic questionnaire creation or result presentation.

- ZCR Coverage: 2.1, 6.9 & 7.1
- LOA: 1

3) Security Information and Event Management (SIEM): The tasks of tools from this category are generally designed to aid network administrators in computer security, intrusion detection, and incident prevention. This includes capabilities, such as collecting, analysing, presenting network- and security-related information, the integration of log files and sources, or triggering warnings about findings. There are a lot of commercial products in this domain, but also open source tools are available, e.g. the Open Source Security Information Management (OSSIM)[4] system, Enterprise Log Search and Archive (ELSA)[5], or Sguil[6]. By using SIEMs the human user is supported by automated log analyses and alerts within the specified scope representing the operator intents.

- ZCR Coverage: None
- LOA: 2

4) Passive Monitoring: OT monitoring tools passively supervising the whole network are well-suited for the requirements in industrial environments because typical assets there mostly react very sensitively to disturbances or changes to their normal communication patterns. Every direct interaction may disconnect assets or disable certain communication paths resulting in a system shutdown and consequently a loss of availability and productivity. These tools analyse various data sources, such as network traffic, asset information, or logs, and are able to detect anomalies in the regular patterns. Newer solutions are also able to match available vulnerability information with the detected assets and to create threat scenarios up to a certain degree. Typical vendors in this category are, e.g. Dragos[7], Forescout[8], or Nozomi[9]. The huge variety of analysis capabilities of passive OT monitoring tools are the most advanced ones for the industrial domain so far resulting in a limited autonomy for certain tasks, such as network scanning and alerting, but the human always needs to be there to act as a fallback.

- ZCR Coverage: 2.1, 5.2, 5.13 & 7.1
- LOA: 3

5) Active Scanner: Active scanning tools for network analysis are more widely spread within IT systems due to possible disturbances of the OT networks and assets. Nevertheless, active scanning under predefined circumstances and controlled

[1] www.ics-cert.us-cert.gov/assessments
[2] www.bsi.bund.de/de/themen/industrie_kritis/ics/tools/tools_node
[3] www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
[4] www.alienvault.com/products/ossim
[5] www.github.com/mcholste/elsa
[6] bammv.github.io/sguil/index
[7] https://www.dragos.com/platform/
[8] https://forescout.de/resources/eyeinspect-datenblatt
[9] https://www.nozominetworks.com/products/overview/

framework conditions can be beneficial to get an accurate and transparent overview because some types of information are not detectable via passing monitoring. A typical open-source example of such tools is the network scanner NMAP[10]. Especially interesting for the industrial domain are the active vulnerability scanners which can discover technical vulnerabilities of assets, e.g. Greenbone[11] or Nessus[12]. In addition, specialised tools for the task of penetration testing are also available, e.g. the open-source Metasploit[13]. These tools are typically used by domain experts after a high-level risk assessment and the necessary scoping in order to dig deeper into certain parts of a system. Therefore, this category requires a huge domain-specific know-how for the safe usage with operational systems and can only assist with certain subtasks while the responsibility is always lying at the human operator.

- ZCR Coverage: 1.1 & 6.2
- LOA: 1

6) Research Approaches: So far three reference sets of related work were identified. In [25]–[27] a security-related diagnosis approach is presented based on a self-developed categorization of industrial assets. Engineering artifacts specified in AutomationML (AML) enhanced with an Web Ontology Language (OWL) model are used to detect security flaws during the engineering phase. The authors of [28], [29] propose a method-agnostic thought model for risk assessments in order to cover the topic of security engineering focusing on the system design phase. In [30] an automated risk identification tool is developed to create attack graphs for systems during the engineering phase via an AML model to OWL ontology translation [31]. This is based on the modelling of asset and vulnerability information with the self-developed AMLsec enhancement as a knowledge base and the rule-based check (with Shapes Constraint Language (SHACL) and SPARQL Protocol and RDF Query Language (SPARQL)) of security requirements from the IEC 62443. The overall status shows a strong coverage of security-related topics within the lifecycle phases of development, design, and engineering. Currently, there are approaches missing which cover the operation lifecycle phase for asset owners. In addition, the general steps of risk analysis and risk evaluation (including the mitigation) are neither regarded at the moment. The identified research approaches are able to deliver occasional autonomy in certain situations, such as information collection from industrial assets or risk identification based on system models. Nevertheless, the human user is always responsible and specifies the set points for the developed tools.

- ZCR Coverage: 3.2-3.6 & 5.13
- LOA: 2

[10]https://nmap.org/
[11]https://community.greenbone.net/
[12]https://de.tenable.com/products/nessus
[13]https://www.metasploit.com/

V. Evaluation of Practical Assessments

A. Demonstrator Analysis

In order to find out about the specific characteristics of each risk assessment step, the corresponding process from the IEC 62443-3-2 standard has been used for three practical risk assessments of typical industrial demonstrators inside the SmartFactoryOWL[14], which is a research and transfer factory operated by Fraunhofer IOSB-INA and OWL University of Applied Sciences and Arts, in Lemgo, Germany. Each of the corresponding steps has varying requirements, such as cost, time, knowledge, experience, relation to stakeholders, or the dependence towards other steps. Therefore, the conducted practical risk assessments were used to determine the status quo with regard to a possible automation of certain steps of the process model.

The first inspected demonstrator was a developed and implemented system from the research project DEVEKOS[15], which inherits a novel skill-based engineering and communication scheme based on Open Platform Communications Unified Architecture (OPC UA) with real-time capabilities and vendor-independent functionalities. The system containing around 30 different controllers from six manufacturers produces fidget spinners providing a real-world example of an industrial production system. According to [32] it can be classified as a learning factory and following the ISA 88 classification it is a process cell. The second investigation was performed on an industry-grade towel folding machine produced by the company Kannegiesser provided via the ADIMA[16] research project. This machine contains only one controller and the communication architecture is provided by one vendor resulting in a much simpler system. It can be classified as an industrial development extent [32] and as an unit following the ISA 88 definition. The third assessment was performed on the Customizable Production System demonstrator within the AutoS²[17] project including a laser engraving process for figurines with the corresponding conveyor belts. This system consists of one process cell according to ISA 88 with one external interface to the Internet and includes three controllers from one common manufacturer. It can also be classified as a learning factory [32].

In order to be able to evaluate the difficulty and the needed experience of each step, the following categorisation named Level of Knowledge (LOK) was used by adapting it from the IEC 62443-3-3 OT standard and the corresponding Security Level (SL) specifications of typical attacker motivations and resource usage. Following the IEC 62443 standard SL 0 is chosen when there are no security measures at all. SL 1 delivers protection against casual or coincidental violation, SL 2 provides protection against intentional violation using simple

[14]https://smartfactory-owl.de
[15]https://www.devekos.org/projektdemonstrator
[16]https://www.init-owl.de/forschung/projekte/detail/adaptives-assistenzsystem-fuer-die-instandhaltung-intelligenter-maschinen-und-anlagen
[17]https://www.init-owl.de/forschung/projekte/detail/automatische-bewertung-und-ueberwachung-von-safety-security-eigenschaften-fuer-intelligente-technische-systeme

means, SL 3 gives protection against intentional violation using sophisticated means, and finally SL 4 is described by protection against intentional violation using sophisticated means with extended resources.

Every LOK ranging from zero to four can also be described by an average cost depending on the required skills and resources estimated from typical loans inside the consulting domain because most of the asset owners do not employ security experts and are dependant on external analysts. The LOK values for the respective ZCRs were defined based on the experiences made during the practical risk assessments and out of the discussions with domain experts and typical asset owners. The calculated costs (based on needed time and required LOK) are used to make the assessments comparable and to formulate the hypothesis for follow-up research activities.

- Junior Analyst (LOK 0): No specific requirements or security-related skills → 80€/hour
- Analyst (LOK 1): Simple means with minimum resources & basic security-related skills → 100€/hour
- Senior Analyst / Junior Security Analyst (LOK 2): Simple means with low resources & generic security-related skills → 120€/hour
- Security Analyst (LOK 3): Sophisticated means with moderate resources & OT specific skills → 150€/hour
- Senior Security Analyst (LOK 4): Sophisticated means with extended resources & OT specific skills → 200€/hour

B. Result Discussion

Each risk assessment step (represented by a ZCR from the IEC 62443-3-2) was performed on all three demonstrating systems accordingly in a fully manual way without any tool support from the presented categories. Table I shows the overall summary of the results acquired during this process. The ZCRs are listed with the corresponding tool coverage and the linked LOA from the previous sections. These values are used for the discussion later on. In addition, the experienced and estimated LOK values are presented and used to calculate the cost for each practical risk assessment based on the measured time required for the certain ZCR. The ZCR 2.1 shall be used here as an explanatory example requiring 13.0h during the risk assessment of the first system from the DEVEKOS project. This step can be further described with a LOA of 3 and a LOK of 4 representing a task for a typical senior security analyst with OT specific skills and extended resources assisted by available software tools, e.g. passive OT monitoring. The total cost for this ZCR at the inspected system are 2.600€, calculated with the measured 13.0h multiplied with 200€ per hour as a typical loan in Germany based on the LOK.

The further analysis of Table I shows six ZCRs which are mainly of interest due to the combination of a low LOA due to available tools, a high need on domain-specific know-how represented by the LOK value, and high resource requirements with regard to time. The following lists summarizes the prioritized six identified ZCRs together with their respective justification.

1) ZCR 5.1 ”Identify threats”
   - Low LOA available
   - High LOK necessary
   - High resource requirements
2) ZCR 3.1 ”Establish zones and conduits”
   - Low LOA available
   - High LOK necessary
   - Medium resource requirements
3) ZCR 5.6 ”Determine SL-T”
   - Low LOA available
   - Medium LOK necessary
   - Medium resource requirements
4) ZCR 2.1 ”Perform initial cyber security risk assessment”
   - Medium LOA available
   - High LOK necessary
   - High resource requirements
5) ZCR 7.1 ”Attain asset owner approval”
   - Medium LOA available
   - High LOK necessary
   - Medium resource requirements
6) ZCR 5.2 ”Identify vulnerabilities”
   - Medium LOA available
   - Medium LOK necessary
   - High resource requirements

In order to analyse the results in a more detailed way, Figure 1 shows the mean percentages of the identified ZCRs with regard to time from the three risk assessments at the different demonstrators. The focused six ZCRs represent 18.75% of the whole ZCR process (32 ZCRs in total) but make up for nearly half (44.6%) of the needed time within the conducted risk assessments. Figure 2 presents a similar picture based on the mean percentages with regard to costs. The six identified ZCRs make up for 46.6% of the related costs. This biased tendency supports the statement of having a few ZCRs functioning as bottlenecks which should be the focus for the upcoming research work in order to automate certain steps for industrial risk assessments.

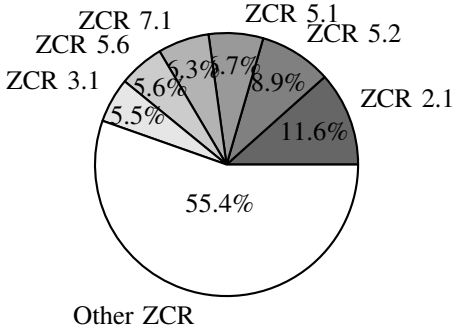

Fig. 1. Mean Percentages of the three Risk Assessments with regard to Time

In addition, the ZCR 2.1 should function as an example here again. The purpose of the initial cyber security risk assessment is to understand the worst-case scenarios present to the SUC

TABLE I
PRACTICAL EVALUATION RESULTS WITHIN THE SMARTFACTORYOWL FOR THE TIME AND COST REQUIREMENTS OF THE (1) DEVEKOS, (2) ADIMA, AND (3) AUTOS² PROJECTS

RM Step	Tool Category	LOA	LOK	(1) Time [h]	(1) Cost [€]	(2) Time [h]	(2) Cost [€]	(3) Time [h]	(3) Cost [€]
ZCR 1.1	5	1	2	6.0	720	1.0	120	4.5	540
ZCR 2.1	2 & **4**	3	4	13.0	2600	1.5	300	6.0	1200
ZCR 3.1	-	0	4	5.0	1000	1.5	300	2.0	400
ZCR 3.2	6	2	4	1.0	200	0.5	100	0.5	100
ZCR 3.3	6	2	4	1.0	200	0.5	100	0.5	100
ZCR 3.4	6	2	4	1.0	200	0.5	100	0.5	100
ZCR 3.5	6	2	4	1.0	200	0.5	100	0.5	100
ZCR 3.6	6	2	4	1.0	200	0.5	100	0.5	100
ZCR 4.1	6	2	3	2.0	300	2.0	300	1.0	150
ZCR 5.1	-	0	4	8.0	1600	1.5	300	2.0	400
ZCR 5.2	4	3	3	10.0	1500	2.0	300	3.0	450
ZCR 5.3	-	0	4	2.0	400	0.5	100	1.0	200
ZCR 5.4	-	0	4	2.0	400	0.5	100	1.0	200
ZCR 5.5	-	0	4	1.5	300	0.5	100	0.5	100
ZCR 5.6	-	0	3	5.0	750	1.0	150	3.0	450
ZCR 5.7	-	0	3	1.0	150	0.5	75	0.5	75
ZCR 5.8	-	0	4	2.0	400	1.0	200	2.0	400
ZCR 5.9	-	0	4	3.0	600	0.5	100	1.0	200
ZCR 5.10	-	0	4	2.0	400	0.5	100	1.0	200
ZCR 5.11	-	0	4	1.5	300	0.5	100	0.5	100
ZCR 5.12	-	0	4	3.0	600	1.0	200	2.0	400
ZCR 5.13	1, **4** & 6	3	2	2.0	240	0.5	60	1.0	120
ZCR 6.1	1	0	3	1.0	150	0.5	75	1.0	150
ZCR 6.2	1 & **5**	1	2	0.5	60	0.5	60	0.5	60
ZCR 6.3	1	0	4	0.5	100	0.5	100	0.5	100
ZCR 6.4	1	0	3	1.0	150	0.5	75	1.0	150
ZCR 6.5	1	0	3	0.5	75	0.5	75	0.5	75
ZCR 6.6	1	0	3	1.0	150	0.5	75	1.0	150
ZCR 6.7	1	0	3	0.5	75	0.5	75	0.5	75
ZCR 6.8	1	0	3	0.5	75	0.5	75	0.5	75
ZCR 6.9	1 & **2**	1	3	0.5	75	0.5	75	0.5	75
ZCR 7.1	1 & **2**	1	4	5.0	1000	1.0	200	4.0	800
Total amount:				**85.0**	**15170**	**24.5**	**4290**	**44.5**	**7795**

of the organization. Currently to the best of our knowledge, for components there are only tools available for the identification of technical vulnerabilities to support this step. The LOA equals 3 with regard to the tool category of passive monitoring and the needed LOK is set to 4 based on the task description and the corresponding requirements for analysts performing this typical risk assessment task. The measured time was the highest of the practical evaluation. These factors combined show many possibilities and promises of huge gains with regard to the potential automation of risk assessments. In addition, based on the results from Table I presented in the bullet point list before this summarizing hypothesis for the follow-up research activities of this work is formulated:

> *If security risk assessment processes inside the industrial manufacturing domain are automated, the required manual efforts are reduced by 20% in time and 50% in cost.*

In summary, the presented results of the three conducted practical risk assessments show a clear need for further specification of the IEC 62443-3-2 process and concepts in order to fulfil the increasing requirements with regard to modularity, flexibility, and automation. The initially defined

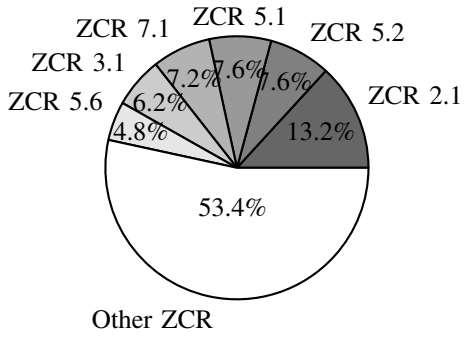

Fig. 2. Mean Percentages of the three Risk Assessments with regard to Costs

research questions were answered in the following ways. **RQ 1 (Market Analysis)** was addressed by the identification, analysis, and categorisation of available tools on the market. The evaluation revealed the coverage of ZCRs from the overall IEC 62443-3-2 process by the already present tools. The specification and assignment of the corresponding LOA values was used to further describe the status quo. The answer to **RQ 2 (Knowledge Requirement)** included the introduction and explanation of LOK values based on the already standardized methodology from the IEC 62443 used to describe the re-

sources and the motivation of possible attackers. The assigned skill levels were enhanced with typical loans for the related tasks and were used to calculate the corresponding costs. **RQ 3 (Future Automation)** was resolved by the identification of six ZCRs which have been characterised as the most rewarding ones for an automation within future research activities.

VI. Conclusion & Future Work

In this work we have investigated the topic of risk assessment automation within the industrial manufacturing domain. The main goal was to analyse and characterise the risk assessment process from the IEC 62443-3-2 with regard to the inherited resource constraints with regard to time and the related costs. The definition of the LOA and LOK metrics enabled us to assign quantitative values to the so far non-tangible characteristics of efforts and required skill levels. This was supported by an analysis and categorisation of the available tools on the market. This revealed five distinctive tool categories to be used further on and the corresponding related work from the research domain. In order to find out about the needed resources for typical risk assessments, three practical iterations have been conducted at different industrial demonstrators within the SmartFactoryOWL in Lemgo. This showed the current status quo and the current resource constraints due to manually required efforts. In the end, six ZCRs from the IEC 62443-3-2 process were identified as the main cost drivers for the current state of manual risk assessments and as the most rewarding steps to be automated in the upcoming research activities. Therefore, the future work includes the further analysis of the identified steps for improvement and the concept proposals on how to solve the related issues. This needs to be aligned in a compliant way with the present concepts from the IEC 62443 standard, such as the definition of SLs or an assignment of FRs. The formalisation of required know-how into practically applicable information models is required as well as the definition of the connected processes. In addition, the alignment and coupling with similar research questions from the safety domain will be addressed.

References

[1] M. Wollschlaeger, T. Sauter, and J. Jasperneite, *The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0*, IEEE Industrial Electronics Magazine, March, 2017.

[2] J. Jasperneite, T. Sauter, and M. Wollschlaeger, *Why We Need Automation Models: Handling Complexity in Industry 4.0 and the Internet of Things*, IEEE Industrial Electronics Magazine, March, 2020.

[3] M. Cheminod, L. Durante, and A. Valenzano, *Review of Security Issues in Industrial Networks*, IEEE Transactions on Industrial Informatics, Volume: 9, Issue: 1, 2013.

[4] M. Ehrlich, A. Bröring, D. Harder, T. Auhagen-Meyer, P. Kleen, L. Wisniewski, H. Trsek, and J. Jasperneite, *Alignment of safety and security risk assessments for modular production systems*, e&i Elektrotechnik und Informationstechnik, 2021.

[5] D. R. Coats, *Worldwide Threat Assessment of the US Intelligence Community*, Statement for the Record, 2018.

[6] A. Pattanayak and M. Kirkland, *Current Cyber Security Challenges in ICS*, IEEE International Conference on Industrial Internet (ICII), Seattle, USA, 2018.

[7] World Economic Forum, *The Global Risks Report*, 15th Edition, 2020.

[8] B. Filkins, *SANS 2019 State of OT/ICS Cybersecurity Survey*, SANS Institute Information Security Reading Room, 2019.

[9] S. Zimmermann et al., *Industrial Security in the Mechanical and Plant Engineering Industry - Results of the VDMA study and recommendations for action*, VDMA Competence Center Industrial Security, 2019.

[10] Ponemon Institute and Siemens, *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat*, Smart Energy International, Issue 5, 2019.

[11] Dragos Inc., *Year in Review: Lessons learned from the front lines of ICS cybersecurity*, Annual Report, 2019.

[12] Dragos Inc., *Year in Review: The ICS landscape and threat activity groups*, Annual Report, 2019.

[13] Dragos Inc., *Year in Review: ICS vulnerabilities*, Annual Report, 2019.

[14] TÜV Rheinland i-sec GmbH, *Industrial Security in 2019: A TÜV Rheinland Perspective*, Whitepaper, 2019.

[15] M. Eckhart, B. Brenner, A. Ekelhart, and E. Weippl, *Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges*, Journal of Internet Services and Information Security (JISIS), Volume: 9, Issue: 3, 2019.

[16] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, *Areview of cyber security risk assessment methods for SCADA systems*, Computers & Security, Issue: 56, 2016.

[17] G. Wangen and E. Snekkenes, *ATaxonomy of Challenges in Information Security Risk Management*, Proceeding of Norwegian Information Security Conference (NISK), Stavanger, Norway, 2013.

[18] E. Bergström, M. Lundgren, and Å. Ericson, *Revisiting information security risk management challenges: A practice perspective*, Information & Computer Security, 2019.

[19] M. Rocchetto, A. Ferrari, and V. Senni, *Challenges and Opportunities for Model-based Security Risk Assessment of Cyber-Physical Systems*, Springer Nature 2019, Resilience of Cyber-Physical Systems - Advanced Sciences and Technologies for Security Applications, 2019.

[20] U. P. D. Ani, H. He, and A. Tiwari, *Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective*, Journal of Cyber Security Technology, Volume 1, Issue 1, 2016.

[21] S. Obermeier, *Cyber Security Research Challenges - An Industry Perspective*, 23rd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Torino, Italy, 2018.

[22] C. Landwehr, D. Boneh, J. C. Mitchell, S. M. Bellovin, S. Landau, and M. E. Lesk, *Privacy and Cybersecurity: The Next 100 Years*, Proceedings of the IEEE, Volume: 100 , Issue: Special Centennial Issue, 2012.

[23] M. Ehrlich, M. Gergeleit, K. Simkin, and H. Trsek, *Automated Processing of Security Requirements and Controls for a common Industrie 4.0 Use Case*, International Conference on Networked Systems Workshop - Advanced Communication Networks for Industrial Applications, Garching, Germany, 2019.

[24] T. Gamer, B. Kloepper, and M. Hoernicke, *The way toward autonomy in industry - taxonomy, process framework, enablers, and implications*, 45th Annual Conference of the IEEE Industrial Electronics Society (IECON), Lisbon, Portugal, 2019.

[25] M. Glawe and A. Fay, *Wissensbasiertes Engineering automatisierter Anlagen unter Verwendung von AutomationML und OWL*, at – Automatisierungstechnik, Volume: 64, Issue: 3, 2016.

[26] C. Tebbe, K.-H. Niemann, and A. Fay, *Ontology and life cycle of knowledge for ICS security assessments*, 4th International Symposium for ICS & SCADA Cyber Security Research, Belfast, United Kingdom, 2016.

[27] C. Tebbe, M. Glawe, K.-H. Niemann, and A. Fay, *Informationsbedarf für automatische IT-Sicherheitsanalysen automatisierungstechnischer Anlagen*, at – Automatisierungstechnik, Volume: 65, Issue: 1, 2017.

[28] S. Fluchs and H. Rudolph, *Making OT security engineering an engineering discipline: A method-agnostic thought model and a data model*, atp, Transforming Automation, 2019.

[29] S. Fluchs, *On Modelling for Security Engineering as a Submodel of the Digital Twin*, Fluchsfriction Blog, 2021.

[30] M. Eckhart, A. Ekelhart, and E. Weippl, *Automated Security Risk Identification Using AutomationML-based Engineering Data*, IEEE Transactions on Dependable and Secure Computing, 2020.

[31] Y. Hua and B. Hein, *Interpreting OWL Complex Classes in AutomationML based on Bidirectional Translation*, 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, 2019.

[32] O. Cardin, *Classification of cyber-physical production systems applications: proposition of an analysis framework*, Computers in Industry, Volume 104, 2019.