ORIGINALARBEIT

Alignment of safety and security risk assessments for modular production systems

M. Ehrlich, A. Bröring, D. Harder, T. Auhagen-Meyer, P. Kleen, L. Wisniewski, H. Trsek, J. Jasperneite

In order to ensure the safety and security of industrial systems with regard to all life cycle phases from development through operation to disposal, specific regulatory and normative requirements are imposed. Due to the digitalization, interconnection, and constantly increasing complexity of manufacturing systems in the context of Industrie 4.0, the manual effort necessary to achieve the required safety and security is becoming ever greater and almost impossible to manage, especially for small and medium-sized enterprises. Therefore, this paper examines the existing challenges in this area in more detail and gives an outlook on the possible solutions to ensure safety and security much quicker and with less manual effort. The overall vision is a (partially) automated risk assessment of modular systems with respect to safety and security, including the alignment of the corresponding processes from both domains and the formalization of the information models needed.

Keywords: safety; security; alignment; automation; processes; models

Abgleich von Safety- und Security-Risikobeurteilungen für modulare Produktionssysteme.

Um Safety und Security von industriellen Systemen im Hinblick auf alle Lebenszyklusphasen von der Entwicklung über den Betrieb bis zur Entsorgung zu gewährleisten, werden bestimmte regulatorische und normative Anforderungen gestellt. Durch die Digitalisierung, Vernetzung und stetig steigende Komplexität von Fertigungssystemen im Kontext von Industrie 4.0 wird der manuelle Aufwand zur Sicherstellung der geforderten Safety und Security immer größer und vor allem für kleine und mittlere Unternehmen kaum noch bewältigbar. Daher untersucht dieser Artikel die bestehenden Probleme in diesem Bereich genauer und gibt einen Ausblick auf die möglichen Lösungen, um Safety und Security deutlich schneller und mit weniger manuellem Aufwand zu gewährleisten. Ziel ist eine (teil-) automatisierte Risikobeurteilung von modularen Systemen in Bezug auf Safety und Security, einschließlich des Abgleichs der entsprechenden Prozesse aus beiden Domänen und der Formalisierung der benötigten Informationsmodelle.

Schlüsselwörter: Safety; Security; Abgleich; Automatisierung; Prozesse; Modelle

Received June 11, 2021, accepted September 6, 2021

1. Introduction

When industrial systems are developed, constructed, and later placed on the market, they must comply with the general requirements of legal regulations and standards, but especially with regard to safety and security. In general, safety describes the protection of humans, machines, and the environment, whereas security aims at protecting the system components against human attacks. Typically, machine builders choose the process of a safety risk assessment to identify hazards and appropriate countermeasures to minimize the risks associated with the identified hazards to grant conformity for a machine with the applicable legislation. With the rise of Plug & Produce approaches in order to achieve goals, such as lot size one, sustainable production, customer-oriented on-demand production, or increased efficiency, one aspect has been not been considered so far, namely the associated repetition of the corresponding needed safety risk assessment [6]. Nevertheless, this is mandatory e.g. for the European markets according to the Machinery Directive 2006/42/EG. If an asset owner connects several modular production systems, he needs to take over the liability of the system integrator and must become aware of new emerging hazards due to the linkage and assess or minimize them accordingly. Modularity in this work includes the evaluation of technical measures, such as component-based changes, and excludes organisational measures, e.g. construction or policies. Traditionally, a safety risk assessment is carried out according to ISO 12100, which considers the general safety of machines.

Additionally, to safety, the increasing digitalization of industrial systems within the Industrie 4.0 developments and a generally growing threat landscape makes security considerations more important for industrial companies as ever before [8]. Therefore, governments, institutions, and organizations work globally on approaches, best practices, and standards for industrial security [1]. The various combinations of Plug & Produce systems change the scope of the security risk assessments for each machine by creating additional communication interfaces between assets resulting in possible threats. This leads to new vulnerabilities, creates additional attack vectors

Ehrlich, Marco, inIT – Institute Industrial IT, OWL University of Applied Sciences and Arts, Campusallee 6, 32657 Lemgo, Germany (E-mail: marco.ehrlich@th-owl.de); **Bröring, Andre,** inIT – Institute Industrial IT, OWL University of Applied Sciences and Arts, Lemgo, Germany; **Harder, Dimitri,** TÜV SÜD Product Service GmbH, Lemgo, Germany; **Auhagen-Meyer, Torben,** Phoenix Contact Electronics GmbH, Bad Pyrmont, Germany; **Kleen, Philip,** Fraunhofer IOSB-INA, Lemgo, Germany; **Wisniewski, Lukasz,** inIT – Institute Industrial IT, OWL University of Applied Sciences and Arts, Lemgo, Germany; **Trsek, Henning,** inIT – Institute Industrial IT, OWL University of Applied Sciences and Arts, Lemgo, Germany; **Jasperneite, Jürgen,** Fraunhofer IOSB-INA, Lemgo, Germany

for possible aggressors, and requires a new prioritization of the security objectives in general. Especially, in case that the security of a safety function is affected by a change of a modular production system, the security risk assessment is a mandatory step with regard to the definitions inside the IEC 61508 which require a consideration of a security risk assessment further referring to IEC 62443 security standard.

To enable safety and security in a modular system today, all possible variants and configurations are considered and evaluated manually, requiring that all modules, whose safety- and security-relevant properties are known, the procedure, and the results are documented by the responsible domain expert. This approach is only partially effective for modular systems following the ideas of the Plug & Produce paradigm change. Due to adaptive technologies configuring system characteristics and the demand for dynamic system architectures, it is currently not possible to estimate in advance which variants and configurations will be required in the future. In addition, a detailed analysis of the interdependence of safety and security processes is not yet provided. Only high-level comparisons and possibilities for an information exchange are currently discussed. A well-developed approach to combine safety and security assessments for the practical usage within industrial systems is still missing.

Therefore, a combined approach for the industrial risk assessment with regard to safety and security is required. To cover industrial systems with Plug & Produce capabilities and make them future-proof, this work discusses the advances of an integrated safety and security risk assessment process for the operation phase of modular systems inside the industrial automation domain. In addition, the relevant modelling of information for an automated safety and security risk assessment will be taken into account as well.

Section 2 describes the state of the art of safety and security risk assessments and the corresponding advantages and drawbacks. Further, in Sect. 3 an evaluation an alignment of safety and security is presented based on the analysis of a common process and the formalisation of necessary information. Section 4 concludes this work and presents future research directions.

2. State of the art

The risk assessment according to ISO 12100 starts at the very beginning of the development of a machine during the design phase and considers the hazards that can arise during the complete lifecycle. The aim is to identify all hazards and to minimise them following the risk assessment process. The process starts with the determination of the physical machine limits, such as size, weight, or materials, and continues with the identification of hazards in preparation for the risk assessment. Since ISO 12100 is a standard for the safety of machines and thus concerns the classic field of safety, the very first point of consideration, the limits of the machine, lacks a concept for the coverage of cyber physical machines due to an increased connectivity and additional interfaces.

After the risk assessment follows the risk evaluation. The risk evaluation aims to check whether the mitigation measures are effective. Risk reduction should be approached in three steps: The first step is the intrinsic safety design, which means that if a hazard that can be mitigated by design measures is identified, these should be used. If the mitigation measures are not sufficient, the possibility of a technical protection measure is considered in a second step by installing safety functions with safety components to further minimise the corresponding risks. In this step, the corresponding functional safety standards are used. These are ISO 13849-1, IEC 62061 where the risks are explicitly calculated with a risk graph and the safety function is designed according to the determined safety characteristic value (SIL or PL). The last step includes the implementation of warning signs on the machine itself, additional information within the corresponding manuals, and specific user training.

The general procedure to make IT systems secure is to continuously execute security-relevant activities like described in ISO/IEC 27001. This can be achieved by executing the Plan, Do, Check, Act (PDCA) cycle and building up an Information Security Management System (ISMS). The IEC 62443 for the industrial automation domain adopted most of these concepts and represents the most important reference for secure industrial systems. Further, in VDI/VDE 2182 an eight-step process is specified including (1) Identify assets, (2) Analyse threats, (3) Determine relevant security objectives, (4) Analyse and assess risks, (5) Identify individual measures and assess their effectiveness, (6) Select countermeasures, (7) Implement countermeasures and (8) Perform process audit. A more detailed overview can be found inside [1].

Authors in [2] describe the issues for interconnected, flexible, and self-optimizing production systems in respect of safety and security. After every modification of the production system during the operation phase, a new manual assessment is necessary. This results in the need for a conjunct consideration of safety and security in an automated assessment algorithm to ensure a safe, secure and efficient operation of the future industrial production systems.

One of the first technical reports for a harmonized framework of (functional) safety (IEC 61508) and security (IEC 62443) for industrial automation and control systems is the IEC TR 63069. It includes general term definitions for safety, security, and their combined risks. In addition, three guiding principles are provided, which includes the protection of safety implementations, the protection of security implementations, and the compatibility of implementations from both domains. The focus of this work is set on the risk assessment phase, which is also covered inside the IEC TR 63069. Nevertheless, only abstract differences are presented and a proposal for a high-level combination of safety and security is shown. A practical guidance for modular industrial systems is missing. That is where the ISA TR 84.00.09 might come into place. It should describe a completely coupled lifecycle for safety and security with example methodologies for each phase. Unfortunately, it is not yet publicly available and will have a focus on the process industry. Further conclusions from this work can be drawn as soon it has been published.

Another technical report is provided by the ISO TR 22100-4 which covers the general safety of machinery in relationship with the ISO 12100 standard and presents considerations for a safety and security interplay. Especially machine builders and system integrators are addressed here. It describes general similarities and differences between both domains with regard to aims and critical aspects, e.g. risk elements. In addition, a five-step procedure (Identify, Protect, Discover, React, and Restore) to secure systems is presented, and general advisories are given to increase the overall security in compliance to safety. The approaches provide a policy-like view on the interplay of safety and security. This work discusses the corresponding contents in order to pave the way for an integrated process for safety and security. Another standard to include into these considerations is the IEC TR 63074:2019 which shows possible effects of security risks to a safety-related control system from a technical perspective by providing countermeasure implementation guidance.

In addition, several surveys from the research and development domain are available which present combined approaches for safety and security [7]. They mostly contain overviews of generally available approaches for the representation and processing of distinctive domain knowledge. This includes the usage of, e.g. fault or attack trees, model-based engineering, Bayesian networks, distributed

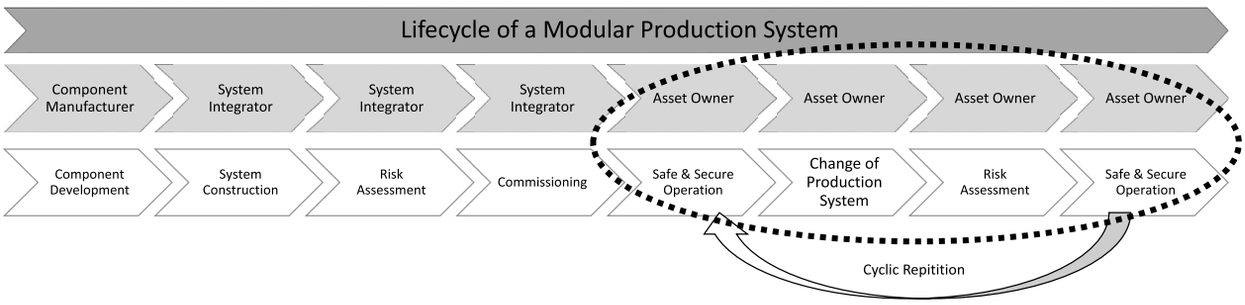


Fig. 1. Typical lifecycle of a modular production system showing the relevant stakeholders on top and the corresponding safety- and security-related activities below

ledger technologies, or Markov processes [12]. All these approaches represent value for the interplay of safety and security, but cannot be used for problems that are addressed by this work, which focuses on the alignment of a more detailed process to combine both domains based on a common process.

System Theoretic Process Analysis for safety and security (STPA-SafeSec) is a novel analysis methodology addressing the dependencies between security vulnerabilities and the overall system safety in a single framework. In [5], the overall approach is presented and evaluated against a power grid use case. It enables users to analyse specific cyber-physical systems with regard to safety and security, but is currently missing the possibility to quantify risks, which could resolved by introducing already existing quantification methods [7]. STPA-SafeSec contains two loops (system refinement and control analysis) aiming at the non-static nature of industrial systems and the internal complexity of modern systems with regard to technologies. It also provides a way to commonly investigate safety and security based on integrated definitions, such as constraints, hazardous scenarios, and hazard control actions. Additionally, an identification of the most critical system components is performed to propose mitigation strategies efficiently. STPA-SafeSec provides a well-designed approach to combine safety and security for cyber-physical systems, also specifying a process to follow during the practical implementation. Nevertheless, the approach of aligning safety and security specific characteristics to unified definitions increases the danger of loosing domain-relevant information which could be important for the overall assessment of a system. Therefore, this work tries to further describe the common information base for safety and security in order to make processes more efficient, but also taking into account the characteristics which represent an antagonism [12].

The FMVEA (Failure Mode, Vulnerabilities and Effects Analysis) [13] method extends the FMEA (Failure Mode and Effect Analysis) for safety analysis with an analysis for threat modes to cover information security as well. For each component of the considered system, the potential failure modes (safety) and threat modes (security) and the resulting effects are identified. Further, for each failure mode, a potential cause, and for each threat mode a potential vulnerability and threat agent as well as the probability of occurrence are identified. This process is repeated until all threat and failure modes for every component are examined and all cause-effect chains are known. This method describes a well-structured proceeding to examine the relevant attack possibilities and failure scenarios component-by-component to eliminate the corresponding causes. Nevertheless, according to the authors, this method is best suited for the early design phase and multi-stage attacks may be overlooked. Also, the overall process for an analysis including the information sources as well as mitigations and countermeasures are not part of this process.

The need for a combined process for safety and security is presented in [4] as well. In addition to the impact of security attacks on the safety of machinery, safety and security have similar objectives and scopes, namely trying to prevent undesirable emergences and making systems more resilient. Thus, the different methodologies to analyse safety and security should stay separate, but need to be aligned as much as possible in order to increase the efficiency of the corresponding analyses. A presented approach is to define a shared objective, define a shared scope, and then analyse risks from both perspectives [4]. However, no specified process is provided yet. Another mentioned supportive overlap are skills of safety and security engineers with the general thinking in risks and thinking about worst case scenarios in both domains leading to mutual understanding. To further integrate these two domains now, not only finding analogies in the lifecycles, but integrating the safety and security lifecycle is necessary to avoid them undermining each other [14]. The aim should be to create one concrete step-by-step execution process. Therefore, the necessary inputs and outputs for each step need to be identified to create a combined process for safety and security [4].

It is required to define commonalities and antagonisms of safety and security with regard to mandatory information, data sources, and process steps. This work will focus on the risk assessment (identification, analysis & evaluation) during the operation phase and the inherited information. In addition, the introduction of a common risk assessment process and the implementation of needed consequences are going to be analysed and discussed.

3. Proposed research framework

The following section will dive deeper into the analysis and discussion with regard to the two foundational pillars of this work: (1) Safety and security process alignment and (2) information modelling of safety- and security-relevant information, inputs, and outputs. Both will be investigated in order to pave the way for further developments. The focus is further described inside Fig. 1 showing a typical lifecycle of a modular production system within industrial environments and the corresponding stakeholder. The different phases include various activities with regard to safety and security. The goal here is to support the asset owner during the operation phase with a (semi-) automated risk assessment, e.g. after the exchange of components, the switching of modules, or the update of software applications.

3.1 Process alignment

As shown within the introduction and the state of the art sections, the two domains of safety and security are already well-covered and

Table 1. Alignment of safety and security within the ISO TR 22100-4

Characteristic	Safety	Security	Alignment
Goal	Avoid accidents and damage	Availability, Integrity & Confidentiality	Conditional Dependency
Conditions	Transparent, obvious, and well-known	(Mostly) not obvious and well-known	Antagonism
Flexibility	Rather static environment	Highly dynamic landscape	Independency
Countermeasures	Mainly machine builders	All involved stakeholder	Conditional Dependency

Table 2. Alignment of safety and security with regard to general characteristics

Characteristic	Safety	Security	Alignment
Purpose (in this work)	Risk Assessment: Risk Analysis Machinery Limits Hazard Identification Risk Estimation Risk Evaluation	Risk Assessment: Risk Identification Risk Analysis Risk Evaluation	Conditional Dependency
Approach	Deductive (general to specific)	Inductive (specific to general)	Antagonism
Aim	Normative conformity	High-priority actions	Conditional Dependency
Objective	Availability & Robustness	Availability, Integrity & Confidentiality Privacy	Conditional Dependency
Assessment Timing	Certain point in time before first usage and after every change	Any point in time during the whole lifecycle	Conditional Dependency
Cause	Accidental & Environmental	Deliberate (malicious intents)	Conditional Dependency
Priority	First, leading	Second, following	Conditional Dependency
Protection	Humans, Machines & Environment	Assets & Intellectual Property	Mutual Reinforcement

were moved into the focus of several working groups and initiatives on a global scale due to its importance. Nevertheless, there are various open questions to be clarified in order to integrate the processes from both domains which result in a typical "chicken or egg question" with regard to the initial motivation of the corresponding risk assessments: When do we need security from a safety point of view? When do we need safety from a security point of view? Which process is starting and leading? Which one is more important and has the bigger impact on the overall risk assessments in the end? Therefore, several proposals on different abstraction levels are already in work, such as the ISO TR 22100-4. Table 1 shows the current state of a possible alignment of both domains based on certain characteristics. The contents were enhanced by a statement with regard to a possible alignment of the presented characteristics based on the proposed scale inside in order to further proceed with the integration of safety in combination with security [9]:

- *Mutual reinforcement:* Fulfilment of safety requirements or safety measures contributes to security, or vice-versa, thereby enabling resource optimization and cost reduction.
- *Conditional dependency:* Fulfilment of safety requirements conditions security or vice-versa.
- *Antagonism:* When considered jointly, safety and security requirements or measures lead to conflicting situations.
- *Independency:* No interaction at all.

The following tables are showing the identified characteristics of the safety and security domain and a possible alignment as a main contribution of this work with focus on the risk assessments within the lifecycle phase of operation:

- Table 2 → General characteristics
- Table 3 → Information-related characteristics
- Table 4 → Quality-related characteristics

The contents of the previous tables shows additional characteristics (24 in total) for the alignment of safety and security, similar to the already provided starting point within the ISO TR 22100-4 documentation. With regard to our evaluation it can be stated that the majority of characteristics inherit a conditional dependency (12/24) between each other or sometimes even a mutual reinforce-

Table 3. Alignment of safety and security with regard to data-related characteristics

Characteristic	Safety	Security	Alignment
Start	Pre-defined checklists of, e.g. hazards	Dynamic collection of, e.g. vulnerabilities	Antagonism
Basis	Probabilistic & non-probabilistic statistical data of stochastic faults	Non-probabilistic experience-based data of previous incidents	Conditional Dependency
Input	System Information	System Information	Mutual
	Hazards	Threats & Vulnerabilities	Reinforcement
Output	Coverage of risks by safety measures for safe operation	Prioritisation of security risks for further implementation of countermeasures	Mutual Reinforcement
Failure Likelihood	Stochastic hardware faults from statistical data	Combination of non-statistical threats and system properties	Antagonism
Metrics	SIL / PL (IEC 61508 / EN 13849)	SL (IEC 62443)	Conditional Dependency

Table 4. Alignment of safety and security with regard to quality-related characteristics

Characteristic	Safety	Security	Alignment
Completeness	Standardized checklists covering all risks	"Low-hanging fruits" & "Crown jewels"	Antagonism
Multiplicity	New safety risk assessment after every modification	Continuous security risk assessment	Mutual Reinforcement
Stakeholder	Asset Owner = System Integrator	Asset Owner	Mutual Reinforcement
Legal	Mandatory fulfilment	Optional fulfilment, except for critical infrastructure	Conditional Dependency
Documentation	Obligated for later inspection	Not necessary, advised for internal risk management	Conditional Dependency
Culture	Maximal transparency towards authorities	Confidentiality about results	Antagonism

ment (5/24). Only some characteristics are evaluated as an antagonism (6/24) or independency (1/24). This clearly shows the further necessity for an aligned investigation of both domains and paves the way for various possibilities to combine efforts, reduce required resources, and increase the overall efficiency of industrial risk assessment processes. Future work will inspect the separate steps in a more detailed way to specify additional possibilities to align safety and security. Information which can be shared for both domains, such as the scoping or the machine limits, should be used and stored commonly in order to reduce technical efforts and enable a common usage. Domain-specific information need to be added and maintained separately. These requirements express the need for future-proof data storage possibilities and information modelling which will be discussed inside the next section.

3.2 Information modelling

The Asset Administration Shell (AAS) is the industrial implementation of a digital twin, the digital representation of an asset, proposed by the Plattform Industrie 4.0 from Germany. The goal is to specify a fully interoperable digital twin that enables a seamless and vendor independent exchange of information across companies during the whole lifecycle of the represented assets. The AAS structure is described in a technology-independent metamodel and consists of several submodels with smaller packets of data, such as construction data of a machine, process data from sensors, or a description of executed process steps. To exchange this information, a passive AAS can be shared as an AASX file, a package file format for the AAS. The re-active AAS makes the AAS data available via Application Programming Interfaces (APIs), whereas the pro-active AASs autonomously interact in peer-to-peer connections with other AASs using I4.0 language [10, 11]. Currently, a standardized submodel for safety or security is missing and was not aligned on yet. There are first ongoing works, such as shown in the reference [3]. Here, the structure of the submodel matches a security engineering process that can be used during the design phase of the system's life cycle. A process for the assessment of new threats, vulnerabilities, and modifications of the system that influence the security during the operating phase is still missing.

The whole development of the AAS environment is currently in progress and is vastly enhanced by the research domain. Therefore, all specifications and implementations are highly dynamic and adaptive. One of the first possibilities to model and implement submodels is the AASX package explorer. This is an open-source software tool

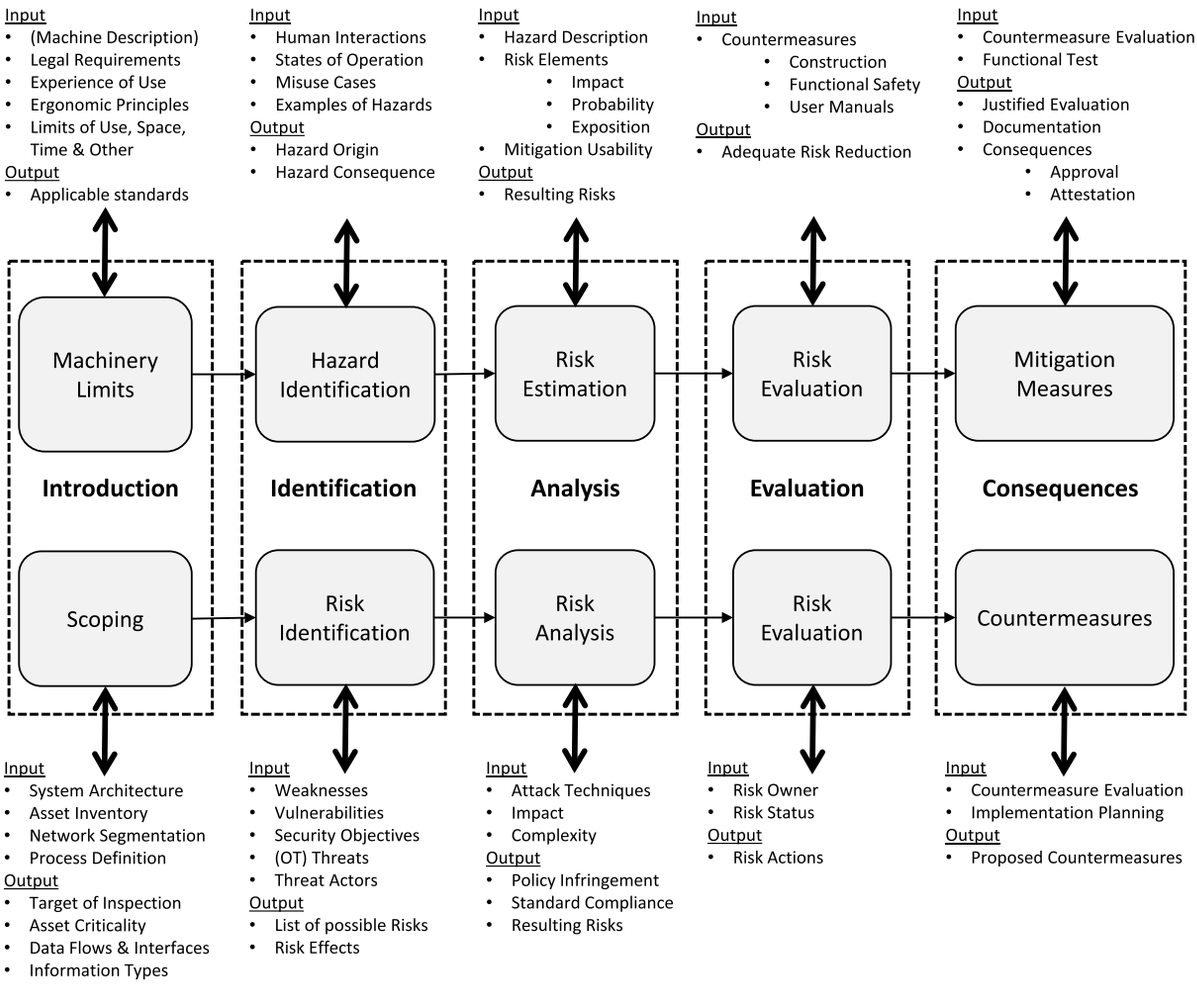


Fig. 2. Safety (top half) and security (bottom half) process analysis with possible inputs and outputs per risk assessment step for the industrial automation domain

which can be used to create, edit, and view AASX files.[1] Additionally, the AASX server is an implementation to make AASs accessible via HTTP REST, OPC UA, or MQTT for the data access and communication to other assets and IT systems.[2] Another Software Development Kit (SDK) including the metamodel of the AAS is BaSyx[3] and PyI40AAS[4] as a Python3 implementation of the AAS.

For the integration of safety and security into the digital twins of assets, e.g. with the AAS, it is mandatory to specify a common information structure like a standardized submodel. Following this structure, the information base, provided as a file (passive AAS) or via communication interfaces (re-active AAS), leads to the possibility to automate parts of the safety and security assessment process, such as risk identification, risk analysis, or risk evaluation. The current status of research and implementation does not show the need of autonomous interaction of an AAS (pro-active AAS) within this work. In order to utilize the mentioned concept of the AAS and to create the mentioned information structure, an investigation of the available information is required. Therefore, Fig. 2 shows an aligned version of the risk assessment steps with regard to their respective inputs and outputs. The top part represents a typical safety-related risk assessment and the bottom part represents a typical security-related risk assessment.

The contents within Fig. 2 make clear how diverse the information landscape for risk assessments currently is. The respective processes for safety (top half) and security (bottom half) share certain information inputs and outputs, but also require separate data from different sources. The current version only shows an abstract view on the information modelling to progress within this topic. Future work will include the detailed analysis of the available information and the data inputs/outputs for the corresponding risk assessment steps. This includes information sources, inherited characteristics, usable metrics, fixed categories or enumerations, and the definition of interfaces. Possible characteristics of knowledge in general are already listed here as an outlook for further discussion:

- Qualitative vs. quantitative (ordinality)
- Discrete vs. continuous (consistency)
- Factual vs. analytical (evaluation)
- Subjective vs. objective (perception)
- Explicit vs. implicit (articulability)
- Procedural vs. declarative (psychology)
- Collective vs. individual (holder)

[1] https://github.com/admin-shell-io/aasx-package-explorer.

[2] https://github.com/admin-shell-io/aasx-server.

[3] https://projects.eclipse.org/projects/technology.basyx.

[4] https://git.rwth-aachen.de/acplt/pyi40aas.

4. Conclusion

In this work, we have investigated the alignment and a possible automation of safety and security risk assessment processes within the industrial automation domain. The current style of risk assessments is not adaptive enough for the upcoming developments and requires a lot of manual efforts by domain experts which contradicts the foreseen flexibility of Industrie 4.0 applications, such as Plug & Produce or Self-X concepts. The results were achieved by analysing the state of the art and the related work within this topic in order to further motivate the necessity for a common taxonomy of both domains and an aligned process for the operation of machines. This twofold analysis and evaluation revealed additional characteristics to describe safety and security respectively and allowed us to assess the possibilities for an alignment of both worlds. In addition, an outlook to the common formalisation of safety and security information has been given to further support the developments with regard to the implementation of suitable digital twins and the corresponding submodels.

The approach, objectives, and required information were compared for machine safety and security. In addition, similarities, differences, and dependencies were identified. Since there are many similarities and supporting dependencies, further efforts should be made to assess the hazards and vulnerabilities of safety and security in an analysis process. It was shown how the approach of both safety and security domains can be processed in the same steps and phases. By proceeding together, dependencies can be better resolved and further utilized. A common process can more easily ensure that the safety and security of assets are covered adequately. Considering to develop one common framework for management to reliably ensure critical infrastructure protection and to resolve the "chicken or egg question". It should be investigated whether a joint approach also reduces the effort of the two assessments and thus increases cost-effectiveness.

In order to increase cost-effectiveness, the assessments processes must be (semi-) automated. Both domains can learn from each other. It should be considered to what extent the concept of a vulnerability database, such as the NIST NVD, can be used in the form of a hazard database in machine safety. Potentially, this would allow the emergence of new hazards in combinations of machines to be tested with less effort. Another idea is to use this kind of database for findings from accident reports and thus subsequently evaluate hazards in machines already in operation with the current state of knowledge. The next steps are to evaluate the cost-effectiveness of a common process and find an algorithm and information that can be used in both machine safety assessment and threat analysis. In the future, it will be attempted to create a common context regarding hazards, which can be classified by several experts as reasonable or correct. This so-called knowledge data system of safety and, in the future, also security, could be provided, e.g. by TÜV SÜD with the compliance software mCOM ONE.

Acknowledgements

This contribution was funded within the project AutoS^2 as part of the technology network it's OWL with support from the ministry of economic affairs, innovation, digitalization, and energy of the state of North Rhine-Westphalia, Germany.

Funding Note Open Access funding enabled and organized by Projekt DEAL.

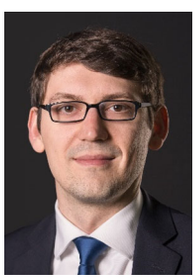
References

1. Ehrlich, M., et al. (2019): Survey of Security Standards for an automated Industrie 4.0 compatible Manufacturing. IECON, Lisbon, Portugal.
2. Ehrlich, M., et al. (2020): Automatische Bewertung und Überwachung von Safety Security Eigenschaften – Strukturierung und Ausblick. In Jahreskolloquium Kommunikation in der Automation.
3. Fluchs, S. (2021): On Modelling of Security Engineering a as a submodel of a Digital Twin. Blog Post.
4. Fluchs, S. (2021): OT security and safety: two perspectives, shared objective. In The ICS CyberSec – what next? Conference.
5. Friedberg, I., et al. (2017): STPA-SafeSec: safety and security analysis for cyber-physical systems. J. Inf. Secur. Appl., 34, 183–196.
6. Kleen, P., Flatt, H., Jasperneite, J. (2017): Erweiterung des "Secure Plug & Work" für Safety-kritische Systeme. In Automation – Leitkongress der Mess- und Automatisierungstechnik, Baden-Baden, Germany.
7. Lyu, X., Ding, Y., Yang, S. H. (2019): Safety and security risk assessment in cyber-physical systems. IET Cyber-Phys. Syst. Theory Appl.. https://doi.org/10.1049/iet-cps.2018.5068.
8. Pattanayak, A., Kirkland, M. (2018): Current cyber security challenges in ICS. In IEEE international conference on industrial Internet, Seattle, USA.
9. Pièrre-Cambacédès, L., Bouissou, M. (2010): Modeling safety and security interdependencies with BDMP (Boolean Logic Driven Markov Processes). In IEEE international conference on systems, man and cybernetics, Istanbul, Turkey.
10. Plattform Industrie 4.0 (2020): Details of the Asset Administration Shell: Part 1 – The exchange of Information between Partners in the Value Chain of Industrie 4.0. Federal Ministry for Economic Affairs and Energy.
11. Plattform Industrie 4.0 (2021): Asset Administration Shell Reading Guide. Federal Ministry for Economic Affairs and Energy.
12. Kriaa, S., et al. (2015): A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf., 139, 156–178.
13. Schmittner, C. et al. (2014): Security application of failure mode and effect analysis (FMEA). In Computer safety, reliability, and security.
14. Schulman, P. R. (2020): Safety and security: managerial tensions and synergies. In The coupling of safety and security.

Authors

Marco Ehrlich
received a Master of Science degree in Information Technology from the Ostwestfalen-Lippe (OWL) University of Applied Sciences and Arts in Lemgo, Germany, in 2017 as the year's best student. Since 2014 he is working as a research assistant in the working group Computer Networks of Prof. Jürgen Jasperneite at the inIT - Institute Industrial IT in Lemgo, currently starting as a PhD candidate. His research interests are focused on cyber security regarding network configuration and management, especially in the industrial automation domain.

Andre Bröring
received a Bachelor of Science degree in Electrical Engineering from the Ostwestfalen-Lippe (OWL) University of Applied Sciences and Arts in Lemgo, Germany, in 2019 and is currently finishing his master's program in Information Technology. Since 2020 he is working as a research assistant in the working group Computer Networks of Prof. Jürgen Jasperneite at the inIT – Institute Industrial IT in Lemgo. His research interests are focused on the Asset Administration Shell as well as communication technologies and cyber security in the industrial automation.



Dimitri Harder
received his Master of Science in Optimization and Simulation from Bielefeld University of Applied Sciences, Germany, in 2016. He worked for almost 3 years as a research assistant in the field of model-based process optimization for energy efficiency for calenders in the project management of Prof. Dirk Weidemann at ISyM - Institute for System Dynamics and Mechatronics. Since 2019, he has been working as a project manager in the field of modular certification. His interests focus on mathematical modelling and standardization of a Digital Twin Architecture for digitalized machine safety.

Torben Auhagen-Meyer
received a Master of Engineering degree in Sensor- and Automation Technology from the University of Applied Sciences and Arts in Hannover, Germany, in 2014. After a few years working in the automotive industry he is now working at Phoenix Contact Electronics GmbH developing components for functional safety.

Philip Kleen
completed his studies in electrical engineering and mechatronic systems at the Ostwestfalen-Lippe University of Applied Sciences and Arts in Lemgo in 2015, after a vocational training as an electronics technician for industrial engineering. Since 2015, he is working as a technical-scientific assistant in the research group Communication Systems and IIoT at Fraunhofer IOSB-INA. His research interests are focused on infrastructure of industrial communication as well as machinery safety (smartSafety) in the field of industrial automation, especially for adaptive, dynamic and modular production systems.

Lukasz Wisniewski
received a Master of Science degree in informatics from the Technical University Opole and PhD degree from the Otto von Guericke University in Magdeburg. Since 2014 he is Research Group Manager of the group Computer Networks at the inIT - Institute Industrial IT of the OWL University of Applied Sciences in Lemgo. His research interests are in the area of IoT, real-time communication protocols and heterogeneous communications systems.

Henning Trsek
received the degree in electrical engineering and information technology from the OWL University of Applied Sciences, Lemgo, Halmstad University, Sweden, and Aalborg University, Denmark, and received the Master's degree in that field in 2005. He received the Ph.D. degree in the area of wireless real-time communication from the Otto-von-Guericke-University Magdeburg, Magdeburg, Germany, in 2016. Afterward, he was employed at the inIT - Institute Industrial IT, Germany, with the responsibilities of a research group leader. His current research interests include the area of Smart Factories, Industrie 4.0 and Industrial Security. He was just announced as a professor for the topic of distributed automation systems at the OWL University of Applied Sciences in Lemgo and is also with rt-solutions.de as a Senior Consultant and responsible for the Industrial Security Department.

Jürgen Jasperneite
received a Dr.-Ing. degree in electrical engineering and information technology from the Otto-von-Guericke-University of Magdeburg, Germany, in 2002. He is a full professor of computer networks at the Ostwestfalen-Lippe (OWL) University of Applied Sciences and the founding director of the inIT - Institute Industrial IT as well as the Fraunhofer Anwendungszentrum Industrial Automation in Lemgo, Germany. He is one of the main initiators of the Centrum Industrial IT, which is Germany's first science-to-business center in the field of industrial automation. He initiated the SmartFactory-OWL, which is a research and demonstration factory for ICT-based automation technologies operated by Fraunhofer and the OWL University. His current research interests include distributed real-time systems, especially in the domain of intelligent automation.