DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

Towards an approach for assuring machinery safety in the IIoT-age

Ein Ansatz zur Gewährleistung der Maschinensicherheit im IIoT-Zeitalter

Tommi Kivelä
Markus Golder
Kai Furmans

Institute for Material Handling and Logistics (IFL)
Karlsruhe Institute of Technology (KIT)

The Industrial Internet of Things (IIoT) promises to bring benefits for all parties, from the machine manufacturers and system integrators to the end users, through data analytics and intelligent machines enabled by increased connectivity. The connectivity, however, brings along the possibility of unauthorised intrusions, causing disturbances in production or intralogistic systems, or in the worst scenario, acting as unintended or malicious triggers for safety hazards. In this work, we present an approach for safety and security co-assurance for machinery. Current safety and security standardisation for industrial control systems and for machinery is discussed, as well as safety and security co-assessment methodology. On this basis, an updated machine lifecycle model and an approach for safety and security risk co-assessment and risk reduction is described. Initial results based on the approach are discussed for a mixed-criticality controller device currently under development.

[Keywords: Machinery, Safety, Security, Assurance approach]

Das Industrial Internet of Things (IIoT) verspricht Vorteile für alle Beteiligten, von den Maschinenherstellern und Systemintegratoren bis hin zu den Endanwendern, durch Datenanalyse und intelligente Maschinen mit erhöhter Konnektivität. Die Konnektivität bringt jedoch die Möglichkeit des unbefugten Eindringens mit sich, wodurch Störungen in der Produktion oder in logistischen Systemen verursacht werden oder welches im schlimmsten Fall das unbeabsichtigte oder böswillige Auslösen von Sicherheitsrisiken bewirkt. In dieser Arbeit stellen wir einen Ansatz zur Sicherung von Maschinen, unter Berücksichtigung von Safety und Security, vor. Die aktuellen Sicherheitsnormen für industrielle Steuerungssysteme und für Maschinen werden ebenso erörtert wie die Methodik der Sicherheitsbeurteilung. Auf dieser Basis wird ein aktualisiertes Maschinenlebenszyklusmodell und ein Ansatz zur Bewertung und Reduzierung von Sicherheitsrisiken (Safety und Security) beschrieben. Erste Ergebnisse auf Basis des Ansatzes werden für eine in Entwicklung befindliche Mixed-Criticality-Steuerung diskutiert.

[Schlüsselwörter: Maschinen, Maschinensicherheit, Cybersicherheit, Gewährleistungsansatz]

1 INTRODUCTION

The Industrial Internet of Things (IIoT) promises to bring benefits for all parties, from the machine manufacturers and system integrators to the end users, through data analytics and intelligent machines enabled by increased connectivity. The connectivity, however, brings along the possibility of unauthorised intrusions, causing disturbances in production or intralogistic systems, or in the worst scenario, acting as unintended or malicious triggers for safety hazards. Apart from securing the related overlaying IT-systems, this raises new questions also for the safety assurance of machinery, when both the safety-related and non-safety-related parts of modern machinery control systems are increasingly designed with network connectivity directly built in.

A new mixed-criticality controller is developed in ZIM-Project FOLSA ("Future-oriented Logistics Safety Application"). The controller includes safety-related and non-safety-related subsystems, the first to support the implementation of safety-related functions, the second for standard control functionality and as well as for communication. The controller is targeted especially at material handling applications as a compact, embeddable and cost-efficient solution to enable safety and non-safety-related functions on the same platform, with secure IIoT-capabilities. The controller concept was previously published in [HKV+16].

In this work, we present an approach, developed during the FOLSA-project, for machinery safety assurance, where security is integrated into the machine lifecycle. The main focus is on an approach for the safety and security risk

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

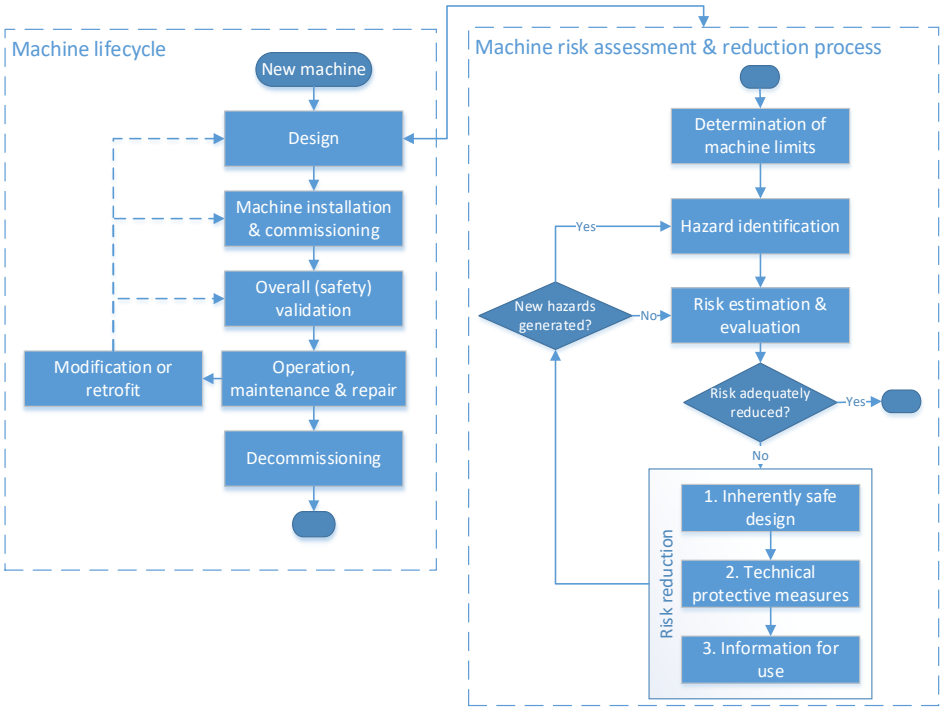

Figure 1. Machine lifecycle from a safety perspective, with risk assessment and reduction process according to [ISO12100].

co-assessment and the mapping of the assessed risk to technical risk reduction measures. The approach is based on current safety and security standards in combination with safety and security co-assessment methods suggested in literature.

The following text is structured as follows. In chapter 2, we summarise the current safety regulation for machinery and the role of security in the standards. We additionally introduce the IEC 62443-standard series [IEC62443-1-1] for security of industrial automation and control systems. A brief overview of existing safety- and security co-analysis methodology from literature is given in chapter 3, to provide a basis for the risk analysis approach. The approach for machinery safety and security co-assurance is presented in chapter 4, with ongoing work in ZIM-Project FOLSA, based on the approach, presented in chapter 5.

2 State of standardisation for safety and security in machinery

Machine products sold on the European market must adhere to the safety requirements originating from the Machinery Directive [EC06]. For machinery, this typically means following the guidelines of harmonized standards, beginning with risk assessment according to the type A standard ISO 12100 [ISO12100] followed by implementation of functional safety of the machine according to the generic type A standard-series IEC 61508 [IEC61508-1] or according to type B standards, such as ISO 13849 [ISO13849-1] or IEC 62061 [IEC62061]. Additionally, type C standards provide safety requirements for specific types of machinery.

A typical machine lifecycle model and the risk assessment and reduction process according to [ISO12100] is illustrated in Figure 1. When a new machine is being designed, the risks related to hazards arising from the machine are to be assessed and reduced to an acceptable level. The risk in the safety standardisation is considered to be the combination of the probability of occurrence of harm and the severity of that harm, harm being physical injury or damage to health, which might occur due to a hazard. The risk reduction can be achieved through inherently safe design, technical protective measures or lastly through information for use [ISO12100]. When using technical protective measures, they are designed according to the relevant functional safety standards, with additional information, such as the required rigor of implementation, defined in type C standards. After design the machine is taken into use and the overall safety is validated. During the machine lifetime, there might arise a need for modification or retrofitting the machine with newer technology, which can trigger a return to the relevant lifecycle phase.

In the next two sections, relevant functional safety standards and their requirements are discussed, as well as the guidance they provide towards the role of security in safety-related control systems. After, related standardization for security of industrial control systems is discussed in sections 2.3 and 2.4.

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

2.1 GENERIC AND MACHINERY-SPECIFIC FUNCTIONAL SAFETY STANDARDS

For the foreseeable future, the machinery sector will remain in a situation with two applicable functional safety standards, the ISO 13849 and the IEC 62061 (based on the generic IEC 61508). The two machinery standards set requirements for the development of safety-related control systems for machinery. In ISO 13849 the required risk reduction is achieved by implementing the safety functions fulfilling Performance Levels (PLs), built with architectures corresponding to categories, while the IEC 62061 uses Safety Integrity Levels (SILs), originating from the IEC 61508 series. Both the PLs and SILs are defined as limits for the probability of the dangerous failure of the safety function. In addition to the probabilistic definition, all the standards additionally require rigorous engineering processes to avoid systematic faults during development, with more measures required for higher PL or SIL. The standards provide guidelines for the development of safety-related parts of the control system to meet these requirements. While both standards can be used for development of safety-related control systems for machinery, the ISO 13849 is more hardware and structure oriented, whereas the IEC 62061 leans more towards complex programmable systems. [ISO13849-1], [IEC62061], [IEC61508-1]

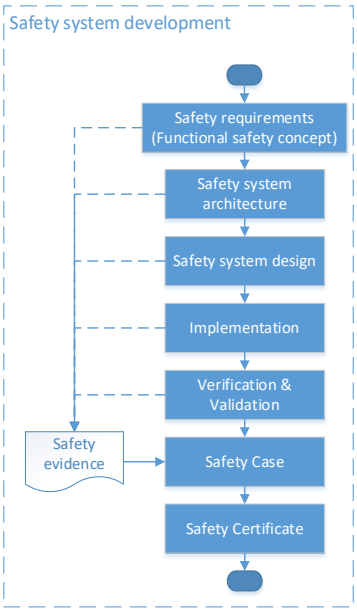

Figure 2. Typical safety system development steps

A typical safety system development process is shown in Figure 2, loosely based on the IEC 61508. Both the ISO 13849 and IEC 62061 base on the IEC 61508, thus the illustrated process applies for safety system development for machinery in general, regardless of the specific standard(s) being used. After the risk assessment, the safety requirements can be defined, with the safety functions the safety system should implement and e.g. their required PL or SIL. The safety system is gradually designed, starting from architecture through design to implementation, followed by verification and validation against the specifications provided in the earlier phases. Throughout the process, safety evidence is gathered, which in the end is combined in to a safety case, which can be presented to an assessor in order to obtain a safety certificate for the developed system. [IEC61508-1], [IEC61508-2], [IEC61508-3]

For safety-related embedded software, as being developed in the FOLSA-project, the IEC 62061 [IEC62061] requires following the requirements of IEC 61508-3 [IEC61508-3], while ISO 13489 has a similar requirement only if the components shall comply with required PL e [ISO13849-1]. Machinery manufacturers often need to comply with both the machinery standards during product development, due to varying customer and market requirements.

The development of safety-critical software according to IEC 61508-3 needs to follow a strict process, which can be modelled with the well-known V-model, where the artefacts used during the specification-phase are used as inputs to the next phase, for finer grained design, and to the verification phase. The whole software is validated against the software safety requirements specification. Once the software has been validated and integrated into the component or machine, the component or machine are typically certified by a third-party. If modifications to the software are needed (triggered by an authorised software modification request), a proper software modification procedure needs to be followed. The effect of the modification on the functional safety of the system needs to be analysed. Following the analysis, the development process shall return to a proper phase of the software lifecycle and all the latter steps are to be carried out. After a modification to a component, re-certification with the third-party is carried out [IEC61508-3]. This traditional model of software development for safety-critical systems poses problems for internet-connected devices, which need to be constantly updated to stay secure.

2.2 SAFETY AND SECURITY

With the ongoing trend of machines being interconnected and online, security will have a much larger role for the safety of machinery in the future. In neither of the current versions of the functional safety standards for machinery is security directly mentioned. The role of security in current and future safety standardisation from a machinery point of view is shortly discussed in this section.

The ISO 13849-1 mentions, in clause 4.6.4 (Software-based parameterization), related to maintaining the integrity of the parameterization data, that unauthorised modification of said data shall be prevented. Additionally, clause 4.6.3 Safety-related application software (SRASW), contains a requirement that access rights to modifications on the SRASW shall be controlled. Note, SRASW refers to a program created in a limited variability language (LVL),

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

which typically would mean e.g. a PLC-program (Programmable Logic Controller), as opposed to safety-related embedded software (SRESW) created in a full variability language (FVL), e.g. C or C++. [ISO13849-1]

The other machinery standard IEC 62061 has very similar requirements towards prevention of unauthorized modification of safety-related software parameters in clause 6.11.2 Software based parameterization. Additionally, the standard has a requirement in clause 6.10.2.6, that the software safety requirements specification shall specify a software-based safety-related control function (SRCF) to prevent unauthorized modification of the safety-related electrical control system (SRECS). [IEC62061]

While the machinery specific functional safety standards do not yet contain more regarding security issues than mentioned above, the current version of the industry agnostic standard, IEC 61508, has some requirements regarding security aspects. The requirements are more specifically in part 1: General requirements [IEC61508-1]. Under clause 1.2, there is a requirement for "malevolent and unauthorised actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant safety lifecycle phases". Furthermore, reference to IEC 62443 series [IEC62443-1-1] is given, among other security standards, with additional sections stating that the standard does not cover the precautions to the aforementioned unauthorized actions nor does it specify the means to meet the security requirements for a safety-related system. The requirement is repeated under clause 7.4.2.3, for hazard and risk analysis, stating that if security threats are identified during the analysis as being "reasonably foreseeable, then a security threats analysis should be carried out". Lastly, there is a mention in clause 7.5.2.2, referring back to the hazard and risk analysis, stating that "If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements". Both the previously mentioned clauses refer to IEC 62443 series for further guidance. [IEC61508-1]

To summarize the requirements from IEC 61508-1, the possible security threats are to be considered during the hazard and risk analysis for the particular safety-related system under development and if such threats exists, their effects should be analysed as a basis for finally specifying the security requirements for the system. In addition to the requirements in IEC 61508-1, there is a single mention regarding security in the normative annex D of IEC 61508-3 (Part 3: Software requirements). Clause D.2.4 states that details of any implemented security measures against listed threats and vulnerabilities shall be listed in the safety manual for a software element. [IEC61508-1], [IEC61508-3]

The Working Group 15 of the IEC Technical Commission 44 ("Safety of machinery - Electrotechnical aspects") is currently working on an upcoming standard IEC 63074, "Safety of machinery - Security aspects related to functional safety of safety-related control systems", which will, when published, provide guidance on safety and security for machinery, which is currently not sufficiently provided by the functional safety standards ISO 13849 or IEC 62061. [IEC63074]

2.3 THE IEC 62443

The IEC 62443 series, referred to by the IEC 61508-1, is a cybersecurity standard series for industrial automation control systems (IACS), based on existing, well-established, security standards for generic IT systems, such as the ISO IEC 27000 series: [ISO27000]. Other well-known security standards exist, like the Common Criteria ISO 15408 [ISO15408]. Utilising generic IT-security standards for industrial control systems is, however, difficult, since the risks, related to physical processes, and prioritised characteristics, typically e.g. availability versus confidentiality, differ significantly. Other security standards and guidelines also exist for industrial control systems, they are discussed in the section 2.4. The focus, however, in this work is on the IEC 62443, since it is the main security standard currently referred to by the safety standards.

The standard is developed by the International Society of Automation (ISA), but published by the IEC as an international standard. Currently, the IEC ISA 62443 series consist of 13 published or previously openly available draft standards [ISA99]. The standards are divided into 4 different groups: General (Parts 1-x), Policies & Procedures (Parts 2-x), System (Parts 3-x) and Component (Parts 4-x). In the terms of this standard series, a system is a whole IACS, thus for machinery, the process and component requirements defined in parts 4-1 [IEC62443-4-1] and 4-2 [IEC62443-4-2] are more relevant. The general parts of the standard series provide the basis for the latter parts, thus the discussion here focuses on the general and the component parts of the standard series.

The IEC ISA 62443-1-1 defines the 5 Security Levels (SLs) for the standard series: 0-4, with larger number indicating an increasing level of security. The SLs are defined based on how complex the threat is, against which defences are provided. The SLs are [IEC62443-1-1]:

- **SL 0:** No specific requirements or security protection necessary
- **SL 1:** Protection against casual or coincidental violation
- **SL 2:** Protection against intentional violation using simple means with low resources, generic skills and low motivation
- **SL 3:** Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

- **SL 4:** Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Another relevant concept for the discussion in this work are the foundational requirements (FRs), which are also defined in part 1-1 as follows [IEC62443-1-1]:

1. Identification and authentication control (IAC)
2. Use control (UC)
3. System integrity (SI)
4. Data confidentiality (DC)
5. Restricted data flow (RDF)
6. Timely response to events (TRE)
7. Resource availability (RA)

The IEC 62443-1-1 additionally describes a typical security lifecycle, for which the steps are shown in Figure 3. The lifecycle is rather similar to the safety lifecycle shown in Figure 1, with the risk assessment and reduction in the form of security-related countermeasures. However, one key difference is the cyclic nature of the security lifecycle. Maintaining security requires active effort, triggered by cyclic reviews or by security-related events. The standard additionally differs between the roles of product supplier, system integrator and asset owner. In the discussion about the dependencies between these different roles, the standard refers to the VDI VDE Guideline 2182 [VDI2182-1], which, along with the discussion about the dependencies will be discussed further in section 2.4. [IEC62443-1-1]

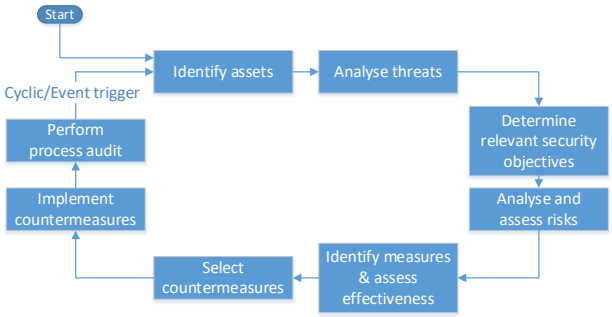

Figure 3. Security lifecycle according to [IEC62443-1-1].

The latter parts of the standard series derive more specific requirements from the foundational requirements. First system requirements, in part 3-3 [IEC62443-3-3], and then component requirements in part 4-2 [IEC62443-4-2]. Both parts 3-3 and 4-2 also map the requirements to the targeted security level, SL-T. The part 3-2 [IEC62443-3-2] gives suggestions for risk assessment to determine the target security level (SL-T) for a system, but not for a single component.

The determination of the SL-T is a matter of risk management. The risk is defined in IEC 62443-1-1 as "Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence" [IEC62443-1-1]. The part 3-2 discusses the process of risk assessment. The IACS under consideration is first divided into zones and conduits. Zones are a physical, logical/virtual or mixed groupings of assets. Information between entities inside a zone or between zones flows through conduits [IEC62443-1-1]. A risk assessment is performed for each zone and conduit. The process steps provided in the standard can be summarized as: identify threats and vulnerabilities, estimate the related unmitigated risk and thereafter the required SL-T. Risk matrices are introduced shortly in informative appendix B as a method for mapping the assessed unmitigated risk to a target security level. This mapping, however, is for each organisation to determine by themselves. After identifying and evaluating countermeasures based on this requirement, the risk should be re-evaluated. [IEC62443-3-2] The process roughly resembles the risk assessment process in ISO 12100, the main difference being the intentional nature of the risk source, which makes the estimation difficult.

The SL-T can also vary depending on the Foundational Requirement. Some FRs, such as the resource availability or system integrity, can be considered higher priority than, for example, data confidentiality. Leaking the machine operational data can be a minor business mishap compared to a safety-related function failing to operate when necessary. The part 1-1 defines the Security Level vector format for this reason, where the SL-T is defined as a vector, with different SL defined for each FR. [IEC62443-1-1]

In the part 4-1, “Secure product development life-cycle requirements” [IEC62443-4-1], a group of security management processes are defined, which the product or component manufacturer should implement. The requirements for the product development phase detailed in IEC 62443-4-1 very much resemble the safety system development phases shown in Figure 2, with the standard requiring:

- Security requirements specification: Including product security context, threat model and derived requirements
- System design according to security principles, guidelines and defence-in-depth
- Secure system implementation
- Security V&V
- Additionally, maintaining product security requires cyclic reviews with update and defect management processes

If a functional safety management is in place for a machinery manufacturer, it might be natural to include the security management into the same process framework. It is nonetheless clear, that the security aspects of a device require a more active involvement from development teams

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

during the device operation lifecycle than might have been required previously with safety devices, which might have only required service personnel for maintenance tasks.

While the part 4-1 focuses on the security management requirements, the part 4-2 provides the concrete technical security requirements for an IACS product or component. The standard lists specific component requirements (CRs) related to each FR, and additional requirements for software applications, or specific requirements for embedded, host or network devices. The Annex B provides a concrete mapping between product SL and the CRs, with an increasing amount of the CRs required as the component SL increases. [IEC62443-4-2]

The IEC 62443 could be considered as having a similar role for security of industrial control systems as the IEC 61508 currently has for functional safety, as a generic guideline. The industry-specific standards, like the ISO 13849 or IEC 62061 are there to adapt the generic standards for the needs and requirements of a specific industry. While machinery-specific guidelines for security, like [IEC63074] are in development, until they are published the IEC 62443 provides a good guideline for the security aspects of developing modern, interconnected machinery.

2.4 Other security standards and guidelines

In addition to the IEC 62443 series, other guidelines exist for securing industrial control systems. Here we provide a short look into two of them. First, the VDI/VDE 2182-series, where the first part, "IT-Security for industrial automation – General model" provides a general model for securing industrial automation systems, and the latter parts provide examples in utilizing the general model [VDI2182-1], also from the point of view of a machine manufacturer [VDI2182-2.2]. Secondly, we shortly look into the ICS-specific guidance provided in the NIST SP800-Series.

The VDI/VDE 2182-1 describes a procedure model, which can be used for IT-security for industrial automation. The procedure described is the same as the lifecycle model from IEC 62443-1-1, previously shown in Figure 3. The guideline additionally discusses the dependencies between different parties: the product vendors, integrators or machine manufacturers and plant management, or the end user. The activities of the different parties are considered in relation to one another – technical documentation flowing downstream from vendor towards end user, and requirements flowing upstream from the end user towards the product vendor. The model of the dependencies between the different parties, with each party going through the cyclical security lifecycle, be it for a specific component, machine or system, is shown in Figure 4. [VDI2182-1]

The suggested approach for the risk assessment in the guideline is, after asset identification to create a threat matrix, using a threat catalogue like [BSI18] as a basis. The risk is estimated semi-quantitatively, where the other parts of the guideline provide examples from the point of view of different parties, e.g. the part 2.1 for a PLC manufacturer or part 2.2 for a machine manufacturer [VDI2182-2.1], [VDI2182-2.2]. The part 1 suggests using countermeasure catalogues to identify possible countermeasures for the threats, but no direct suggestions are provided. [VDI2182-1]

The threat catalogues by BSI ([BSI18]) and the procedure provided in [VDI2182-1] give a comprehensive basis for assessing organisational, systems and technical threats, but might be difficult to use for a machine manufacturer.

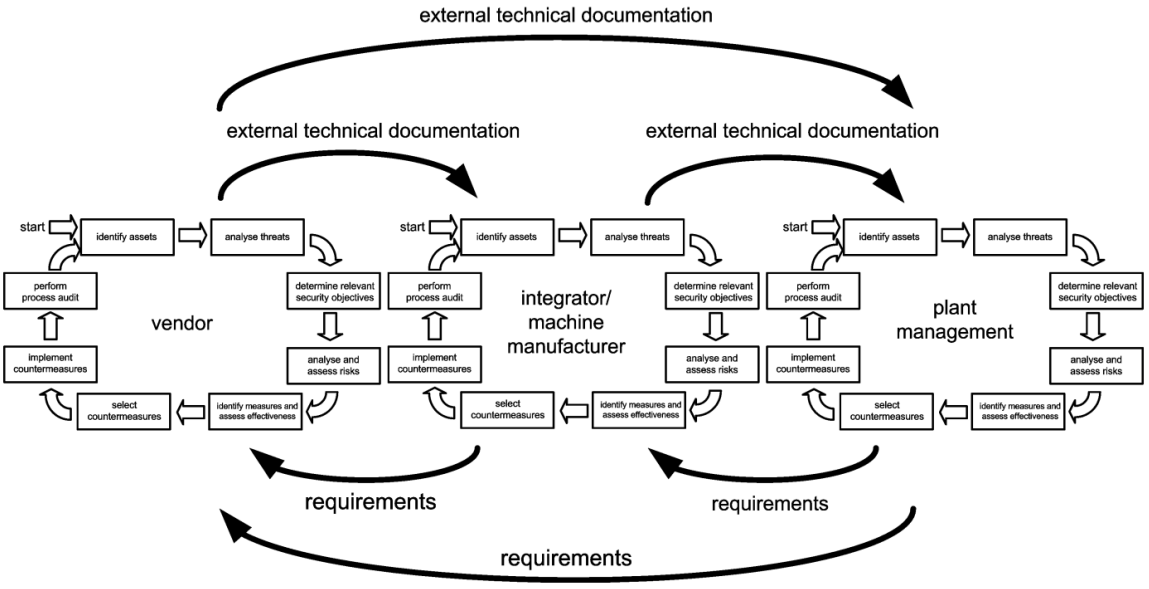

Figure 4. Dependencies between component vendors, machinery manufacturers and end users according to [VDI2182-1].

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

The United States National Institute of Standards and Technology has published several guidelines for information security, including the NIST SP 800-30, "Guide for conducting Risk Assessments" [NIST800-30], and the NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security" [NIST800-82]. In the approach provided in NIST SP 800-30, risk tables are created for the assessed system with threat events, threat source and its capabilities, likelihood and impact estimates to get a final semi-quantitative risk value. Representative threat events provided in the standard. After the risk assessment, the NIST SP 800-82 provides a list security control measures in the Annex G, which is based on the list provided in NIST SP 800-53 [NIST800-53], modified especially for ICS. The NIST standards provide a comprehensive, organizational and systems point of view. It might, however, be difficult for a machine manufacturer to apply the approach provided in these standards. [NIST800-82], [NIST800-30]

Risk assessment approaches were already discussed in this section, based on suggestions provided in the security standards. The risk assessment approach in IE 62443-3-2 [IEC62443-3-2] is given from the point of view of a complete IACS. The approach is also generally usable for product or component level, but the standard does not provide direct suggestions for example for the threat identification, like the NIST Special publications [NIST800-82], [NIST800-30] or the VDI guideline [VDI2182-1]. Both the latter provide more specific guidelines, but also take a high-level organisational and process point of view, which might be difficult to apply when considering a single machine. The organisational and process point of view is important, however, assessing risk from organisational and process point of view can be abstract and potentially misleading. It might be easier for a machine or component manufacturer to deploy the management processes provided in e.g. IEC 62443-4-1 [IEC62443-4-1] or a future machinery-specific standard as part of the general quality management processes when developing machines or machine components, which require secure product development and maintenance practices. For the technical countermeasures, which need to be built in to the machines or machine components, a risk assessment process is still meaningful.

3 METHODOLOGY FOR SAFETY AND SECURITY CO-ASSESSMENT

The previous section discussed relevant safety and security standardisation, and the related risk assessment approaches for each of the respective aspects. However, since the safety and security aspects of an interconnected machine are intertwined, the risk assessment should consider both aspects together, not separately. In this section we will introduce methodology suggested in literature for safety and security co-assessment.

A recent comprehensive survey of integrated safety and security assurance approaches and risk assessment methods can be found in [KPB+15] and [CHP+17], respectively. In this work we summarize selected methods, which could be considered as easily adoptable for the machinery industry.

The threat matrix from VDI 2182 [VDI2182-1] and the risk tables in NIST SP 800-30 [NIST800-30] resemble closely the traditional tables used in failure mode and effects analysis (FMEA) [IEC60812], originally developed for reliability, but widely used for safety systems development and machinery risk assessments. [Rau11]

Schmittner et al. suggested an extension to FMEA, called FMVEA, the failure mode, vulnerabilities and effects analysis [SGP+14]. In FMVEA the analysed system is considered physical or software component at a time, like in traditional FMEA, where both the possible failure and threat modes of the component, their possible local and system wide effects are considered. Thus, for the initial triggers, the failure or threat modes, safety and security are considered separately, their effects can be combined in to cause-effect chains, which negatively affect the system. Whereas for the failure modes the failure rates can be estimated probabilistically, the likelihood of the threat modes is estimated semi-quantitatively. For each threat mode, the approach relies on analyst expertise to identify possible vulnerabilities. Similar to using pre-defined component failure modes, like those supplied in e.g. Annex A of [IEC61508-2], Schmittner et al. suggest using the STRIDE threat modelling framework as a guideline for the threat modes. [SGP+14]

The STRIDE threat modelling framework was originally developed for the Microsoft Security Development Lifecycle [HL06], for IT-systems, but has been recently suggested also by e.g. in [KML+17] for threat modelling of cyber-physical systems. The STRIDE is an abbreviation of the following threat modes [HL06]:

- **Spoofing:** Masquerading of a legitimate user, process or system element
- **Tampering:** Modification/editing of legitimate information
- **Repudiation:** Denying or disowning a certain action executed in the system
- **Information disclosure:** Data breach or unauthorized access to confidential information
- **Denial of Service (DoS):** Disruption of service for legitimate users
- **Elevation of privilege:** Getting higher privilege access to a system element by a user with restricted authority

The STRIDE approach is based on analysing a Data flow diagram (DFD) of the studied system. The system and its information flows are depicted as entities, processes,

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

data flows and data stores. An example DFD for the FOLSA system is shown later in section 5, Figure 7. Further examples can be found e.g. in [KML+17] or [HL06]. Not all DFD elements are susceptible for all the threat modes, the susceptibility can be mapped as shown in Table 1.

Table 1. Mapping STRIDE to DFD elements [HL06]

DFD Element	S	T	R	I	D	E
Entity	X		X			
Data flow		X		X	X	
Data Store		X	X	X	X	
Process	X	X	X	X	X	X

The FMVEA could be a natural approach to include security considerations for machinery manufacturers, who likely already utilise a traditional FMEA for safety analysis. It is then up to the manufacturer to map the calculated risk values to the SL-T.

As noted also in [SGP+14], the FMVEA has similar limitations as the traditional FMEA, as a bottom up analysis method, focusing on single causes of an effect, meaning that longer causal chains of events might be overlooked. They suggest combining the FMVEA with the approach described by Steiner and Liggesmeyer in [SL13], where they combined Attack trees ([Sch99]) with Component fault trees ([KLM03]), which are a modular approach to traditional fault tree analysis (FTA, [IEC61025]). This approach, called the extended component fault tree (ECFT) could also be considered easily adoptable for machinery manufacturers already familiar with FTA.

Another possibility for finding complex causal chain of events could be to use the more recent systemic approaches, for example the Systems-theoretic process analysis (STPA), originally suggested by Leveson [Lev11]. In STPA the studied system is modelled as a hierarchical control structure, which is used as a basis to find unsafe control actions, against which further design control or other mitigation measures can be implemented. Due to the background in systems theory, STPA is better suited to detect complex causal chains in modern software-intensive systems. [Lev11]

STPA is originally a safety analysis method, but has been further extended for security analysis, STPA-Sec, by Young and Leveson in [YL14] and for safety and security co-analysis, STPA-SafeSec, recently by Friedberg et al. in [FMS+17]. Temple et al. suggested a hybrid approach, combining the STPA-Sec with FMVEA in [TWC+17]. The STPA-based methods are more recent and promising, but have not been widely applied in machinery so far, and might be more difficult to adopt.

Of the methods discussed here, the FMVEA seems to be the most suitable for adoption for machinery industry. The security assessment bears resemblance to the other approaches in [NIST800-30] and [VDI2182-1], but utilising the STRIDE threat modelling framework [HL06] instead of large threat catalogues should make it more approachable, while still providing a comprehensive approach.

4 SAFETY AND SECURITY CO-ASSURANCE APPROACH FOR MACHINERY

In this section we suggest an updated machine lifecycle model, with the basis in the traditional lifecycle model discussed in section 2 and shown in Figure 1, but integrating the cyclic approach from the security standardisation. Additionally we discuss a possible approach for machine safety and security risk assessment and reduction based on the FMVEA method and the IEC 62443-standards.

4.1 MACHINE LIFECYCLE MODEL

The updated machine lifecycle model is shown in Figure 5. When a new machine is being designed, the related risks should be assessed and when necessary, the risks should be reduced. For machinery equipped with communication interfaces, also the security aspects should be considered. Considering the machine as a cyber-physical system, first both the physical and the digital limits of the machine need to be determined. Afterwards, both the hazards and threats of the machine should be identified and the related risk estimated and evaluated. Some threat modes might not affect the safety of the machine, but it is important to recognise the interconnections, for example whether some of the threat modes can lead to safety incidents or whether the safety and security requirements collide with each other, the possibility of which was discussed e.g. in [KPB+15].

If risk reduction is deemed necessary, the guidance for the technical countermeasures can still refer to respective safety or security standards. Some of the countermeasures or mitigation techniques might be similar, for example the measures detailed for the 3rd FR, System integrity in [IEC62443-4-2], e.g. integrity checks on the software or input validation, are similar to techniques often used for safety-related software. In Figure 5, the 3-step method from [ISO12100] is shown for safety risk reduction, but only technical protective measures and information for use are considered for security, as it is difficult to see how the concept of inherently safe design could translate to security. If new hazards or threats are introduced due to the implemented measures, the assessment and reduction process should be repeated until no more new hazards or threats are found. An example of new threats arising from risk reduction could be e.g. the introduction of a safety-related control system to implement some supervisory functionality, which is equipped with communication interfaces and they will be used in the application. In this case the threat modes

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

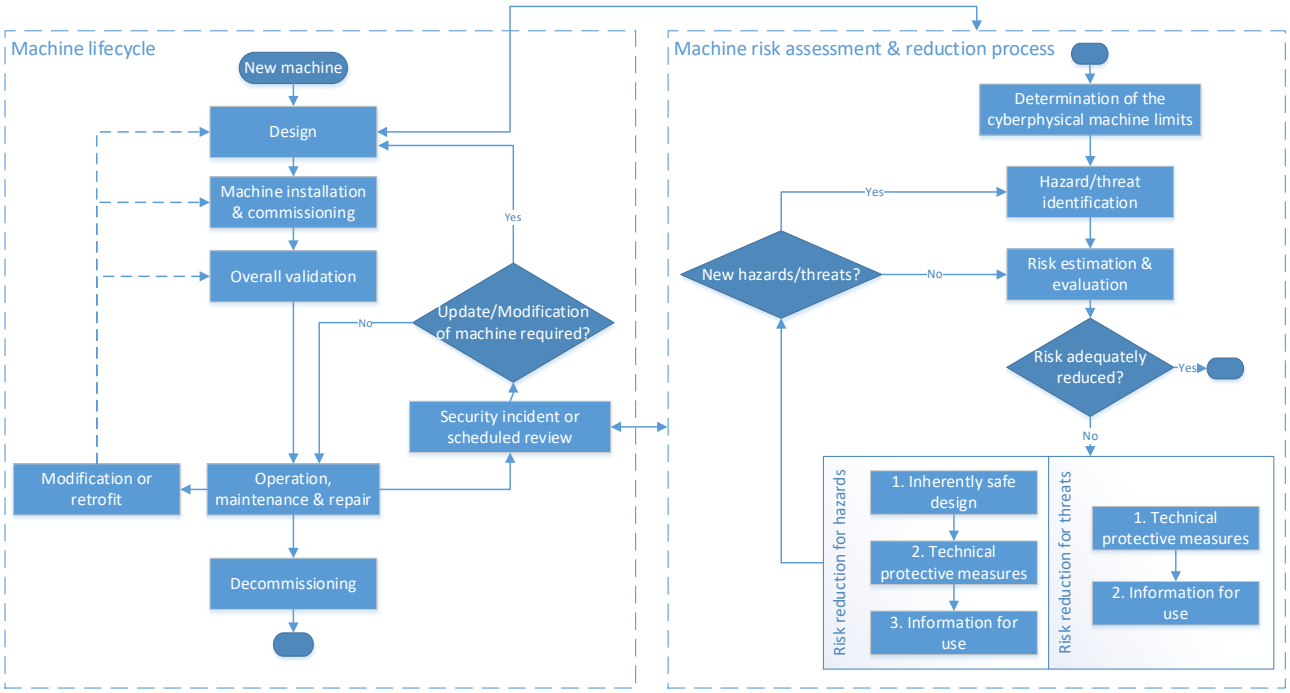

Figure 5. Machine lifecycle model considering both safety and security

related to the safety-related control system need to be assessed alongside the failure modes and the risks reduced when necessary.

Another addition to the lifecycle model are the cyclic security reviews and incident response during machine operation, based on the security management principles from [IEC62443-4-1] and the cyclic lifecycle model from both the [IEC62443-1-1] and the [VDI2182-1]. In order to maintain the security of a machine or machine component over its lifetime, the security assessment should be cyclically reviewed and updated when necessary. The re-assessment might also be triggered as a response to security incidents. If an update or other type of modification is required, it triggers a return back to the relevant part of the design process. If the security issue is directly in a safety-related part of the control system, modification might require the modification process described in section 2.1. This might be tied to high costs. At the moment the safety standardisation is not very flexible in terms of supporting quick modification processes, providing good grounds for separating the communication parts of the safety-related system from the parts directly participating in the safety functions. If the communication parts can be considered separate, the modification processes for security updates are easier.

4.2 Risk Assessment & Reduction

The machine risk assessment can be done by using the e.g. FMVEA method [SGP+14]. The FMVEA can be additionally augmented with further measures like the ECFT [SL13] or STPA-SafeSec [FMS+17] in order to identify longer cause-effect chains.

Following the risk assessment, the risk related to hazards arising from the machine are reduced using the 3-step method from ISO 12100 [ISO12100]. If technical protective measures are utilised in the risk reduction, relevant functional safety standards should be consulted in the safety system development, e.g. the ISO 13849 [ISO13849-1]. For the amount of required risk reduction, the type C-standards or e.g. the risk graph or risk matrix methods for determining the required PL/SIL from [ISO13849-1] or from [IEC62061], respectively, still apply.

Additionally, for the risks related to security issues, a single machine can be considered as a product in terms of the IEC 62443-series, and the guidance provided [IEC62443-4-1] and [IEC62443-4-2] 4-2 can be applied. For mapping the STRIDE threat modes to the IEC 62443 FRs, the mapping shown in Table 2 can be used. The table shows the original mitigation techniques according to [HL06] adopted to the FRs according to [IEC62443-1-1]. Originally, [HL06] does not provide direct mapping between timely response to events to the STRIDE thread modes, the SL-T for the TRE can be estimated based on the overall SL-T for the system. The estimated risk for each threat related to the machine or machine component being analysed can be tied to the relevant FRs based on the STRIDE threat mode used as a model for that threat. The estimated risk can be mapped to a required SL-T, like sug-

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

gested in [IEC62443-3-2]. The SL-T vector can then be derived from the worst case SL-T related to each FR. An example of this mapping is shown in the next section.

Table 2. Mapping STRIDE threat types to IEC 62443 FRs.

Threat type (STRIDE)	Mitigation technique	
	SDL [HL06]	IEC 62443 FRs
Spoofing	Authentication	Identification and authentication control (IAC)
Tampering	Integrity	System Integrity (SI)
Repudiation	Non-repudiation services	Identification and authentication control (IAC) User control (UC)
Information disclosure	Confidentiality	Data confidentiality (DC)
Denial of Service	Availability	Resource availability (RA) Restricted data flow (RDF)
Elevation of privilege	Authorization	User control (UC) System Integrity (SI)

As part of the risk reduction process, it can be considered, whether e.g. the machine manufacturer implements all the necessary measures to reach the SL-T obtained as a result of the risk assessment, or whether the risk reduction is only partially implemented and the remaining risk is informed to the end user. It is then up to the end user and their respective risk assessment to consider whether additional risk reduction measures are necessary or require the further countermeasure implementation from the supplier.

In the next section, we show a short example of the suggested risk assessment approach with FMVEA and the mapping to IEC 62443 FRs for the project FOLSA.

5 Example of Safety and Security Co-Analysis in Project FOLSA

In this section, a short simplified example is discussed for the FOLSA controller. The FOLSA unit and an example generic end application system structure is shown in Figure 6. The safety-related subsystem of the FOLSA controller is based on the HICore 1-safety system-on-chip (SoC) [HMS+14], with internal redundant safety architecture and a separate communication CPU. In the FOLSA controller the safety-related subsystem is additionally coupled with a non-safety-related subsystem, which utilises a commercial off-the-shelf SoC to act as a secure gateway for the safety system as well as execute non-safety-related functionality, which can be either control tasks or e.g. condition monitoring. The safety-related subsystem communicates to the non-safety-related subsystem through a directly connected serial bus, which can also be used for direct connection to a maintenance PC for e.g. setting safety-related parameters. The safety-related subsystem can be connected to other FOLSA units for safety-related common functions utilising the CAN-interface or to CAN-connected sensors or actuators. Direct IO controls for the locally supervised process can be directly connected to the safety CPU, the CAN-communication happens over the communication CPU. The non-safety-related subsystem is ideally communicating locally with other systems to share operational data, or sharing condition monitoring data to a cloud/backend server system over GSM network.

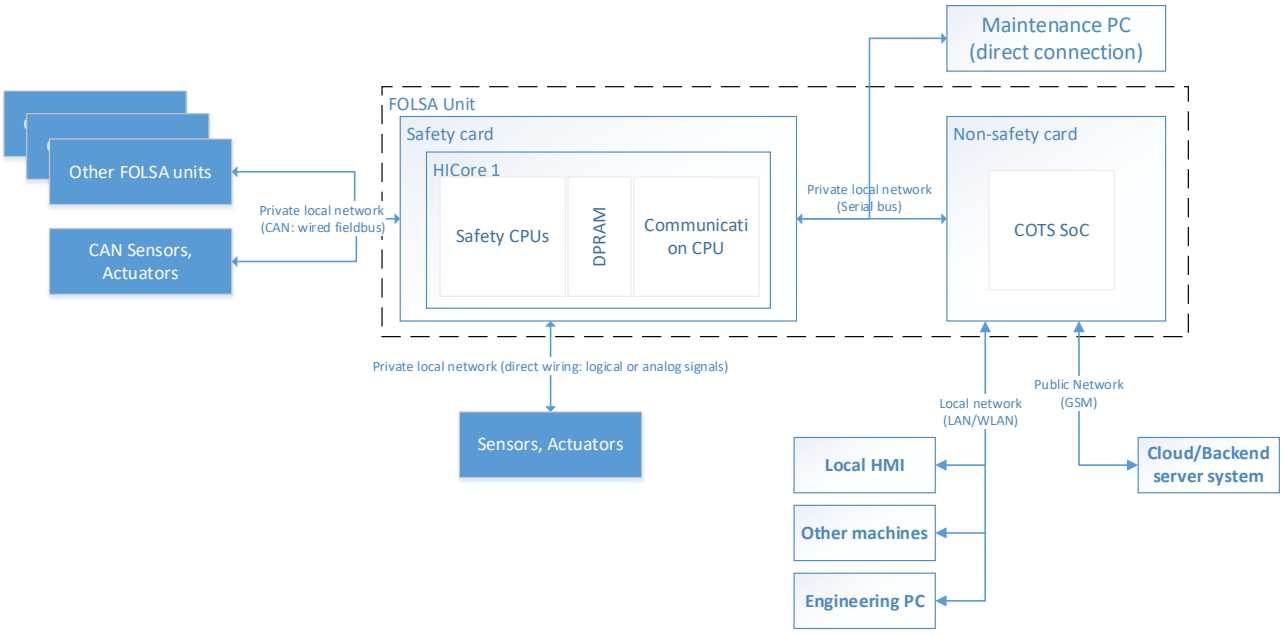

Figure 6. Generic end application system structure for the FOLSA system.

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

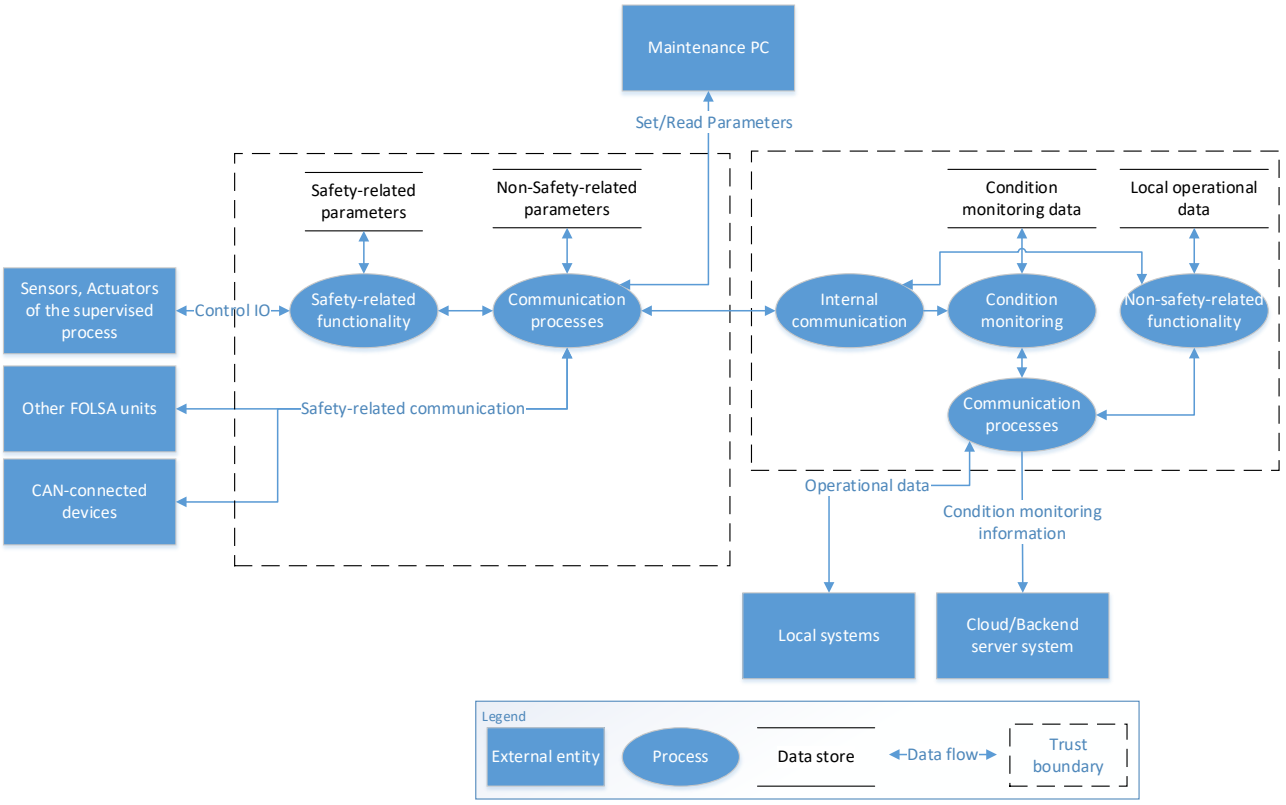

Figure 7. Example simplified data flow diagram of the FOLSA system in generic end application environment.

A simplified DFD of the system structure is shown in Figure 7, with the previously explained functionality and communication shown as external entities, processes, data stores and flows. The zones and conduits concept from [IEC62443-1-1] can be considered through the shown trust boundaries and the data flows.

For assessing the security risk, the approach from [SGP+14] is used. For each threat, the attack probability is estimated semi-quantitatively as a sum of threat properties and system susceptibility, which are estimated as follows [SGP+14]:

- Threat properties =
  Attacker motivation + Capabilities
- Attacker motivation: 1 = opportunity target, 2=mildly interested, 3=main target
- Attacker capabilities: 1=low, 2=medium, 3=high
- System susceptibility =
  Reachability + Unusualness
- Reachability: 1=no network, 2=private network, 3=public network
- Unusualness: 1=restricted, 2=commercially available, 3=standard

As a result, the estimated attack probability will be a value between 4 and 12. Additionally the severity of the threat is estimated on a scale of 1-4, which are insignificant, marginal, critical and catastrophical, respectively. Threats which affect the system safety should be estimated critical or catastrophical. This can depend on the criticality of the supervised process.

The risk is the product of the estimated attack probability and threat severity. An example mapping between the estimated risk and the SL-T is shown in Table 3. As a basis for the mapping, it was assumed that if the system being analysed includes safety-related control systems, which might be affected by security-related aspects, the minimum SL should be at least 1. Additionally, the attacker was assumed to be a skilled adversary with moderate resources at worst, limiting the maximum SL to 3, as SL 4 would mean defending the system against an adversary similar to a nation state, which was not deemed reasonable expectation for machinery.

Table 3. Mapping the estimated security risk to SL-T

Risk	SL-T
<15	1
15-23	2
>=24	3

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

Table 4. Example of FMVEA

STRIDE	Component	Vulnerability	Threat Mode	Threat effect	System effect	Severity	Threat Property	Susceptibility	Attack Probability	Risk	SL-T	FR
T	DF: Operational data	Man in the middle attack, insufficient authentication	Sending false operational data	Incorrect system operation	Reduced system integrity	2	Insider: 4	4	8	16	2	SI
						2	Hacker: 3	4	7	14	1	SI
I	DF: Operational data	Insufficient authentication, vulnerable protocols	Attacker gains access to operational data	Customer process data leaked	Loss of confidentiality	1	Insider: 4	4	8	8	1	DC
						1	Hacker: 3	4	7	7	1	DC
D	DF: Operational data	Inadequate access control, inadequate congestion control	Attacker interrupts operational data flow	Incorrect system operation	Reduced system reliability, availability	2	Insider: 4	4	8	16	2	RA, RDF
						2	Hacker: 3	4	7	14	1	RA, RDF
E	Non-safety card: Communication processes	Insufficient input validation	Attacker gains elevated access to non-safety card	Attacker gains access to safety system interface	Possible loss of safety	4	Insider: 4	4	8	32	3	UC, SI
						4	Hacker: 3	4	7	28	3	UC, SI

The risk limits were determined based on the SL definitions. SL 2 means protection against intentional violation, but with low resources, motivation and generic skills. This can be estimated as threat properties: 3 (motivation: 2, capabilities: 1), for any system: susceptibility: 2, resulting in at worst critical severity: 3, resulting in estimated risk of 15. This value was taken as the lower limit for SL-T of 2, lower risk results in SL-T of 1. For SL 3, a threat property score of 5 was assumed, which corresponds to high capability attacker with mild interest or medium capability attacker taking the machine as the main target. While retaining the other values, this results in risk of 24, which was taken as the lower limit for SL-T of 3.

An example of selected STRIDE threat modes for selected system components is shown in Table 4. The relevant STRIDE modes were applied to the data flow "operational data" between the non-safety card and the external entities in the system. The threat modes related to the data flow were not considered safety-critical, but the system integrity, confidentiality or reliability can be affected. As an example of a threat mode resulting in possible loss of safety, the elevation of privilege threat mode applied to the communication processes running on the safety card is shown as last in the table. Elevation of privilege on the non-safety card grants the attacker access to the safety system interface, which might lead to loss of safety, thus resulting in high severity. For all the cases, the attacker capabilities were considered low or medium, depending on whether the attacker is an insider or not, with the device assumed as not being the main target of the attack. As a summary of just the risk assessment shown here, the SL-T for FRs Use Control and System Integrity would be 3, for Resource Availability and Restricted data flow 2, and for Data Confidentiality 1.

6 CONCLUSIONS

In this work we have provided an extensive overview of current safety and security standards, and based on the overview, suggested an updated machine lifecycle process model, considering both safety and security. Additionally, we discussed a possible approach for safety and security risk-assessment and reduction, based on the standards and co-assessment methods suggested in literature, and illustrated the approach with a short example. The suggested approach might need adjustments as the machinery standards are updated. The discussion in this work was mainly based on the FMVEA-method, whereas in the future also the other discussed methodology should be studied further in a machinery context.

The presented work in the context of the project FOLSA is based on an on-going research project, the assessment results described in this work are not final estimates. Additionally, the technical design and implementation for the FOLSA platform is still ongoing.

7 ACKNOWLEDGEMENTS

We gratefully acknowledge that this research is funded by the German Federal Ministry for Economic Affairs and

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

Energy (BMWi: Bundesministerium für Wirtschaft und Energie) under ZIM (Zentrales Innovationsprogramm Mittelstand) cooperation grant number ZF4251405DB7.

We would like to thank Yongxin Zhou and Xueping Kong, former and current student at KIT, whose Master Theses contributed to the presented work.

BIBLIOGRAPHY

[BSI18] Bundesamt für Sicherheit in der Informationstechnik: Gefährdungskataloge. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Gefaehrdungskataloge/gefaehrdungskataloge_node.html, accessed 1 Aug 2018.

[CHP+17] Chockalingam, S. et al.: Integrated Safety and Security Risk Assessment Methods. A Survey of Key Characteristics and Applications. In (Havarneanu, G. et al. Eds.): Critical Information Infrastructures Security. Springer International Publishing, Cham, 2017; pp. 50–62.

[EC06] European Parliament and The Council of the European Union: Directive 2006/42/EC Of The European Parliament And Of The Council of 17 May 2006 on Machinery, and Amending Directive 95/16/EC (Recast).

[FMS+17] Friedberg, I. et al.: STPA-SafeSec. Safety and security analysis for cyber-physical systems. In Journal of Information Security and Applications, 2017, 34; pp. 183–196.

[HKV+16] Holzweissig, P. et al.: HiPi – A concept for a compact, IoT-enabled safety controller: Logistics Journal: Proceedings, 2016.

[HL06] Howard, M.; Lipner, S.: The security development lifecycle. SDL, a process for developing demonstrably more secure software. Microsoft Press, Redmond Wash., 2006.

[HMS+14] Hayek, A. et al.: HICore1. “Safety on a chip” turnkey solution for industrial control: 2014 IEEE 25th International Conference on Application-Specific Systems, Architectures and Processors. IEEE, 2014; pp. 74–75.

[IEC60812] International Electrotechnical Commission: EN IEC 60812:2006 - Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA), 2006.

[IEC61025] International Electrotechnical Commission: EN IEC 61025:2006 - Fault tree analysis (FTA), 2006.

[IEC61508-1] International Electrotechnical Commission: EN IEC 61508-1:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, 2010.

[IEC61508-2] International Electrotechnical Commission: EN IEC 61508-2:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safetyrelated systems, 2010.

[IEC61508-3] International Electrotechnical Commission: EN IEC 61508-3:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements, 2010.

[IEC62061] International Electrotechnical Commission: EN IEC 62061:2005 - Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems, 2005.

[IEC62443-1-1] International Society of Automation; International Electrotechnical Commission: ISA IEC 62443-1-1:2009 - Security for industrial automation and control systems - Part 1-1: Models and concepts.

[IEC62443-3-2] International Society of Automation; International Electrotechnical Commission: ISA IEC 62443-3-2 (Draft 2017)- Security for industrial automation and control systems - Part 3-2: Security risk assessment, System Partitioning and Security Levels.

[IEC62443-3-3] International Society of Automation; International Electrotechnical Commission: ISA IEC 62443-3-3:2013 - Security for industrial automation and control systems - Part 3-3: System security requirements and security levels.

[IEC62443-4-1] International Society of Automation; International Electrotechnical Commission: ISA IEC 62443-4-1:2018 - Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.

[IEC62443-4-2] International Society of Automation; International Electrotechnical Commission: ISA IEC 62443-4-2 (Draft 2017) - Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components.

[IEC63074] IEC TC44 WG15: Website. IEC 63074 Ed.1 - Security Aspects Related To Functional Safety Of Safety-Related Control Systems. http://www.iec.ch/dyn/www/f?p=103:38:1445488894672::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1302,23,23497, accessed 31 Jul 2018.

[ISA99] ISA99 Committee: ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security. http://isa99.isa.org, accessed 31 Jul 2018.

[ISO12100] International Organization for Standardization: EN ISO 12100:2010 - Safety of machinery - General principles for design - Risk assessment and risk reduction (ISO 12100:2010).

[ISO13849-1] International Organization for Standardization: EN ISO 13849-1:2015 - Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design.

[ISO15408] International Organization for Standardization: ISO IEC 15408 - Information technology - Security techniques - Evaluation criteria for IT security, 2009.

[ISO27000] International Organization for Standardization; International Electrotechnical Commission: ISO IEC 27000 Standard series - Information technology - security techniques.

[KLM03] Kaiser, B.; Liggesmeyer, P.; Mäckel, O.: A New Component Concept for Fault Trees: Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software - Volume 33. Australian Computer Society, Inc, Darlinghurst, Australia, Australia, 2003; pp. 37–46.

[KML+17] Khan, R. et al.: STRIDE-based threat modeling for cyber-physical systems: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, 2017; pp. 1–6.

[KPB+15] Kriaa, S. et al.: A survey of approaches combining safety and security for industrial control systems. In Reliability Engineering & System Safety, 2015, 139; pp. 156–178.

[Lev11] Leveson, N.: Engineering a safer world. Systems thinking applied to safety. MIT Press, Cambridge, Mass., 2011.

[NIST800-30] National Institute of Standards and Technology: NIST SP 800-30r1:2012 - Guide for Conducting Risk Assessments, 2012.

[NIST800-53] National Institute of Standards and Technology: NIST SP 800-53r4:2015 - Security and Privacy Controls for Federal Information Systems and Organizations, 2015.

[NIST800-82] National Institute of Standards and Technology: NIST SP 800-82r2:2015 - Guide to Industrial Control Systems (ICS) Security, 2015.

[Rau11] Rausand, M.: Risk assessment. Theory, methods, and applications. Wiley, Hoboken, N.J., 2011.

[Sch99] Schneier, B.: Attack trees. In Dr. Dobb's journal, 1999, 24; pp. 21–29.

[SGP+14] Schmittner, C. et al.: Security Application of Failure Mode and Effect Analysis (FMEA). In (Bondavalli, A.; Di Giandomenico, F. Eds.): Computer Safety, Reliability, and Security. Springer International Publishing, Cham, 2014; pp. 310–325.

[SL13] Steiner, M.; Liggesmeyer, P.: Combination of Safety and Security Analysis - Finding Security Problems That Threaten the Safety of a System. Technische Universität Kaiserslautern, Fachbereich Informatik, Kaiserslautern, 2013.

[TWC+17] Temple, W. G. et al.: Systems-Theoretic Likelihood and Severity Analysis for Safety and Security Co-engineering. In (Fantechi, A.; Lecomte, T.; Romanovsky, A. Eds.): Reliability, Safety, and Security of Railway Systems. Modelling, Analysis,

DOI: 10.2195/lj_Proc_kivelae_en_201811_01
URN: urn:nbn:de:0009-14-47466

Verification, and Certification. Springer International Publishing, Cham, 2017; pp. 51–67.

[VDI2182-1] Verein Deutscher Ingenieure; Verband der Elektrotechnik Elektronik Informationstechnik e.V.: VDI/VDE 2182-1:2011 - IT-security for industrial automation - Part 1: General Model, 2011.

[VDI2182-2.1] Verein Deutscher Ingenieure; Verband der Elektrotechnik Elektronik Informationstechnik e.V.: VDI/VDE 2182-2.1:2013 - IT-security for industrial automation - Part 2.1: Example of use of the general model for device manufacturer in factory automation - Programmable logic controller (PLC), 2013.

[VDI2182-2.2] Verein Deutscher Ingenieure; Verband der Elektrotechnik Elektronik Informationstechnik e.V.: VDI/VDE 2182-2.2:2013 - IT-security for industrial automation - Part 2.2: Example of use of the general model for plant and machinery installers - Forming press, 2011.

[YL14] Young, W.; Leveson, N. G.: An integrated approach to safety and security based on systems theory. In Communications of the ACM, 2014, 57; pp. 31–35.

M.Sc. Tommi Kivelä, is working as a Research associate at the Institute for Material Handling and Logistics (IFL), Karlsruhe Institute of Technology (KIT).
Email: Tommi.Kivelae@kit.edu

Prof. Dr.-Ing. Markus Golder, was the head of the chair of Safe mechatronic systems in intralogistics (SIMESI), Institute for Material Handling and Logistics (IFL), Karlsruhe Institute of Technology (KIT). He is now the head of the Professorship of Material handling and conveying engineering, Technische Universität Chemnitz.

Prof. Dr.-Ing. Kai Furmans, is the head of the Institute for Material Handling and Logistics (IFL), Karlsruhe Institute of Technology (KIT).

Address: Institut für Fördertechnik und Logistiksysteme (IFL), Gebäude 50.38, Gotthard-Franz-Str. 8, 76131 Karlsruhe, Deutschland. Tel.: +49 721-608-48621, Fax: +49 721-608-48629