Development Process for Information Security Concepts in IIoT-Based Manufacturing

Julian Koch(✉), Kolja Eggers, Jan-Erik Rath, and Thorsten Schüppstuhl

Institute of Aircraft Production Technology, Hamburg University of Technology, Hamburg, Germany
julian.koch@tuhh.de

Abstract. Digital technologies are increasingly utilized by manufacturers to make processes more transparent, efficient and networked. Novel utilization elicits the challenge of preventing deployed information technology from compromising processual security. The digital enabling of formerly analog operation technology, the extensive use of information technology connectivity like MQTT, TCP/IP, Wi-Fi, and the deployment of IoT edge computing platforms create an application scenario for the Industrial Internet of Things (IIoT), which also introduces the associated vulnerabilities, which have been extensively exploited in the past. This paper introduces a development process for information security concepts designed for production scenarios based on the IIoT. This concept is then applied using an illustrative use case from aircraft production. The main contents of the development process include: Formulation of reasonable assumptions, system modelling, threat analysis including risk assessment, recommendation of countermeasures, reassessment after incorporating countermeasures. Specifically, a Data Flow Diagram as the model is developed, and a "risk first" variation of the STRIDE methodology is applied to identify threats and prioritize them. The aforementioned state-of-the-art methodologies are adjusted to our cyber-physical use case in the IIoT. The resulting concept aims to enable manufacturing processes to be digitized as sought. The adjustments to the methodologies are independent from our use case and may be suitable to a broad field of scenarios in the IIoT.

Keywords: Threat modelling · IIoT · STRIDE · Cyber-physical systems · Information security · Industry 4.0 · DFD

1 Introduction

In recent years, the amount and impact of cyberattacks on companies in the industrial sector has increased drastically and is expected to increase further [1, 2]. Due to rising danger cybersecurity has become a high priority for any party making use of Industrial Internet of Things (IIoT) environments [3]. Although there is no single definition of IIoT [4], there are certain recurring characteristics of the IIoT in the literature that are especially relevant for cybersecurity in manufacturing companies. In particular, the connection of a wide variety of cyber-physical systems to form a network should be mentioned here, which in turn places special requirements on connectivity, interoperability,

The original version of this chapter was revised: The incorrect affiliation of all the authors has been corrected. The correction to this chapter is available at
https://doi.org/10.1007/978-3-031-18326-3_40

K.-Y. Kim et al. (Eds.): FAIM 2022, LNME, pp. 316–331, 2023.
https://doi.org/10.1007/978-3-031-18326-3_31

scalability and data processing [5]. The increasing amount and impact of cyberattacks in the industrial context are attributable to the merging of the traditionally separated domains of Operation Technology (OT) and Information Technology (IT) into the IIoT [6]. Due to differences in scope, impact, and context of possible threats, securing IIoT systems is typically arduous, and differs substantially from securing both traditional IT systems and traditional OT systems [7]. The objective of this work is to develop a process to elaborate on information security concepts for digital manufacturing processes. To ensure that information security is integrated into the introduction of digital technologies, this approach particularly focuses on systems under development. For this objective, a system-driven [8], Security-By-Design [9] approach is chosen. In Sect. 2, the necessary background such as secure system development, data flow diagrams (DFDs) and STRIDE as well as related work will be considered. Section 3 describes the actual development methodologies as well as the proposed changes to the DFDs and the STRIDE method. Section 4 applies the methodology to a use case exploring the quality assurance of aircraft structure components and presents the subsequent findings. Last, Sect. 5 discusses the presented development process and provides an outlook on future work.

2 Related work and background

This section provides essentials and related work to facilitate a better understanding on the proposed methodologies and the respective adjustments.

2.1 Secure System Development

On the strategic level, secure system development considers the overall development process of secure systems, and is divisible into two approaches. The first approach aims to develop security measures for an existing system. The second approach integrates the security development into the actual system development process which aims to achieve a Security-By-Design approach. The first approach is followed by the BSI-security process, which in its description towards the development of a security concept, is applicable to existing processes [10]. This process starts with the specification of the scope, which is followed by a structural analysis of the underlying system and the definition of protection requirements, as well as the modelling of the system based on the prior steps. Based upon the model, the system's protection requirements are checked. If the protection requirements have not already been met, a risk analysis and subsequent risk consolidation is undertaken, which then triggers the next instance of protection requirement checks. This is an iterative process until the requirements are seen to be met and pertaining safeguards are implemented. Last, the process describes the maintenance and continuous improvement of the achieved results. However, this process provides inadequate guidance for Security-By-Design approaches, since the security development process should be integrated with the system development. Therefore, such approaches cannot be built on top of an existing system. For this reason, deviations from the BSI-process were developed which aim to make it suitable for Security-By-Design approaches as the said approach does not elaborate on the specific steps in the development process [11]. Publicly available use cases regarding end-to-end security development for industrial cyber-physical

cases are rare, however the threat modelling use cases for industrial cyber-physical cases do exist [12]. Furthermore, the unadjusted application of methodologies from the cybersecurity domain does not sufficiently consider physical threats. Last, the proposed method collocates risk determination after the threat analysis, which tends to produce a high number of low-priority threats and is therefore a point of inefficiency.

2.2 System Modelling

Modelling approaches as a foundation for threat analyses, specifically also in IIoT contexts, vary, while the most common approach is to model the system as a data flow diagram (DFD) [13–19]. DFDs are based on the stages of digital data and model data-in-use as processes, data-at-rest as data stores and data-in-transit as data flows. Furthermore, DFDs may include trust boundaries which denote transitions of the respective trust assumptions between sections of the model [20]. The aptitude of DFDs regarding their use in threat analyses is a topic of scientific discussion and several enhancements to account for shortcomings exist [19, 21]. Regarding IIoT-systems, the incapability to model physical aspects will be more specifically considered and motivates the proposal of the adapted DFD notation. One aspect of enhancement included in the eSTRIDE methodology will be utilized as a reference [21].

2.3 Threat Analysis

STRIDE is the most common methodology for threat analyses, but due to its genesis in software security at Microsoft, suffers from shortcomings regarding use cases which increasingly differ from classical OS and software security [22]. However, STRIDE is used as a basis for threat analyses in the IIoT domain [14–19]. STRIDE provides six classes of common threats which facilitate the brainstorming process. The classes are “Spoofing”, “Tampering”, “Repudiation”, “Information Disclosure”, “Denial-Of-Service” and “Elevation-Of-Privilege” [20]. Deviations to account for challenges such as threat explosions and cyber-physical systems are discussed in varying literature [21, 22]. One of these approaches is called eSTRIDE and is relevant to our proposed methodology. eSTRIDE as a deviation to STRIDE applies a risk-first approach to the threat analysis, which otherwise is done after finding the threats via STRIDE [23].

3 Proposed Development Process and Methodologies

This section describes the derived development process for information security concepts (Fig. 1), including the adjusted DFD modelling and the adjusted application of the STRIDE methodology. The phases with their tactical steps of the development process will be laid out, placing greater emphasis on the proposed methodologies applied in these steps. The applied development process represents an adaptation of the BSI development process for a security concept on a strategic level, however, it is adapted for Security-By-Design approaches. The development process was devised for cyber-physical IIoT systems, while the adapted STRIDE methodology is applicable for any use case dealing with assets. The adapted DFD modelling was devised for IIoT systems with cyber-physical and physically distributed components.

3.1 Development Process

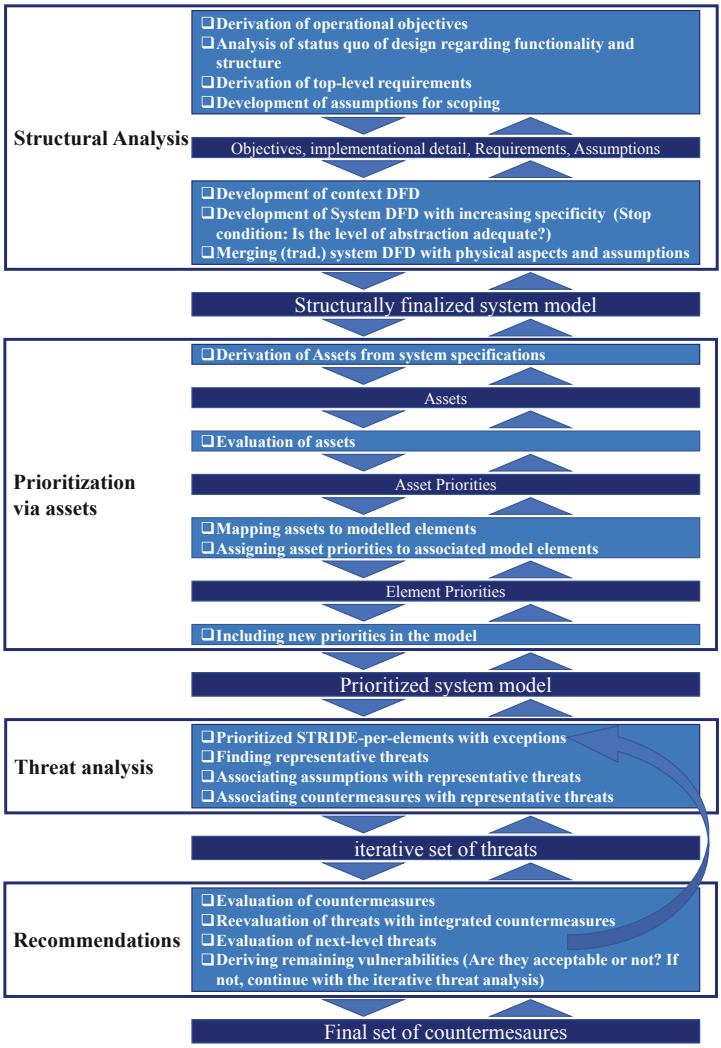

Fig. 1. Proposed development process with four phases including tactical steps.

The entire development process consists of four phases with tactical steps, which can be seen in Fig. 1. The tactical steps are shown in light blue and the results in dark blue. While in principle the development process follows the downstream flow seen in Fig. 1, the whole process is iterative in the sense that, for following the Security-By-Design approach, it must react to changes in the development of the system to be secured. Therefore, a change in system specifications triggers the upstream flow depicted in Fig. 1. In general the upstream flow might not only be triggered by a change of system

specifications, but rather when the analyst assumes that previously executed steps have for whatever reason no longer valid results. The process is then gone through backwards in order to pinpoint those aspects which no longer hold, must be changed or must be added respectively. When the most upstream step of the process, which was affected by the change, has been adequately adapted, then the process is to be applied downwards to account for resulting changes. Within the following, the development process is detailed based on the main phases.

Structural Analysis: The structural analysis serves to provide a foundation for the subsequent modelling and threat analysis. Its execution depends on the state of the design phase and the degree to which implementational detail is known. In the conceptual phase, the objectives of the system are formulated with increasing detail in order to develop functional components, which can later serve as building blocks for the model. It should be noted that "components" describe conceptual parts of the system, which are not necessarily represented directly in the model, while "elements" are the defined building blocks of the DFD model. Therefore the modelling of the system as a DFD depends on the adequate representation of system components in the DFD using elements. Subsequently, already known implementational details are gathered. The produced set of implementational details is used in the last step of the modelling process in which the traditional DFD is merged with the implementational details. After this, the top-level requirements pertaining to the development of the information security concept for the underlying system under development are devised. These requirements should state what the information security concept should provide and what requirements the process itself must meet. Last, assumptions and scoping decisions are taken to guide the development. These assumptions will later be included in the model and the assessment of found threats. The gained knowledge of the underlying conditions developed in the prior steps are then utilized to develop an adjusted DFD to model the system. A conventional DFD model is devised with the DFD notation established in [20], differing only in that the processes are denoted with circles. When an adequate model of the system has been achieved, the changes to the DFD are made, which aim to better model systems such as the considered IIoT use cases (see Fig. 2). For this, implementational detail is added to the model. First, data flows are annotated with channel information such as communication protocols, much alike to those in eSTRIDE. Second, DFD elements which are to be implemented on the same device are aggregated in that regard. Third, system sections with multiple distributed instances are marked as such. Last, the resulting model is annotated with security relevant assumptions, divided into hard security assumptions (green), soft (yellow) and compromising (red). The assumptions are either specific to an element of the model or affect several elements indirectly.

Prioritization via Assets: The purpose of this phase is to provide the foundation for the subsequent prioritization of threats which facilitates a prioritized *risk-first* approach to the implementation of mitigations. As the origin of this prioritization the potentially endangered assets are utilized. The proposed process assumes that assets have already been described in the course of functional development of the IIoT system. The assets can be any kind of data produced and needed in IIoT-based manufacturing process. Examples for assets in this context are machine data, measurement data or intralogistics

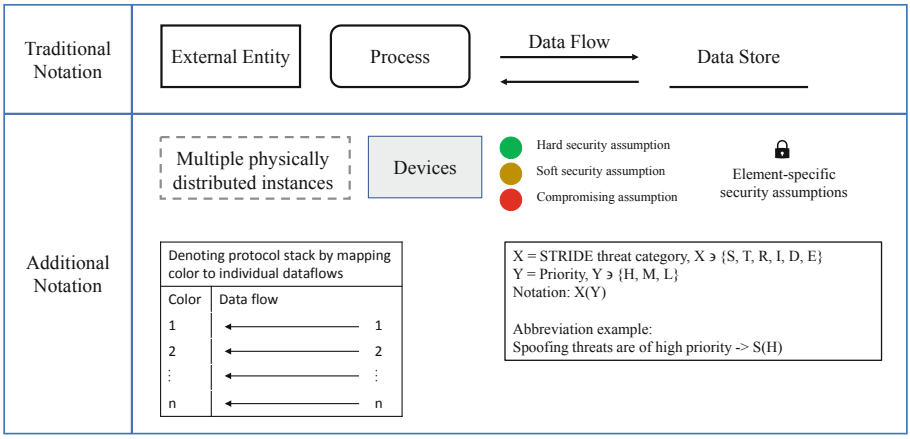

Fig. 2. Adjusted DFD Notation.

data. The derivation of assets can be performed by various techniques. For example, the system specifications can be used to create an Entity-Relationship model from which the resulting data can be derived. The assets are mapped onto the associated DFD elements, developed in phase 1. The assets are prioritized into low, medium and high priority in the categories of the STRIDE methodology regarding possible impact and exposure. Notably, this step takes place before finding threats, while in traditional STRIDE application a risk assessment or prioritization of threats of any kind is not an inherent part of the methodology and is therefore often applied afterwards, therefore the approach described in this paper is denoted as a *risk-first* approach. For this assessment, expertise regarding the underlying system and information security are required, which can be integrated by executing the assessment in collaboration with an expert of the underlying system. It is important to note that this assessment does not include *attack scenarios*, but only considers the generic STRIDE threats as basis for the assessment. The analyst is free to choose a specific existing methodology for the assessment. Examples for standardized qualitative methodologies for this task can be found in [24, 25]. When the prioritization is done, the DFD elements inherit the highest possible priority of their associated assets. It should be noted that the prioritization of assets and the inheritance of the resulting priorities by the DFD elements is a novel approach.

Threat Analysis: The threat analysis provides the threats to the system. Furthermore, the threat analysis aims to provide representative threats which group threats together if they are sufficiently similar. This serves to reduce the analysis effort. The STRIDE methodology is applied with the limiting assumptions and scope settings in order of the prioritized elements of the DFD. While the STRIDE methodology is conventionally applied to a model without prioritization, the approach in this work provides a prioritization to the model, which aims to result in focusing the threat analysis on higher priority threats. This aspect makes this a *risk-first* approach. The general approach is based on the STRIDE-per-Element variant. However, threat scenarios are generally not limited to single elements, therefore the "per-Element" notion is not regarded as absolute, rather

as more of a guiding principle. Therefore, in addition to assessing the elements in their prioritized order, the threat analysis examines scenarios in which multiple elements must partake in the threat execution. Threats are associated with their priority inherited from the priority of affected DFD elements, the affecting relevant assumptions taken prior, possible countermeasures and lastly similar threats which form a set from which later on representative threats may be drawn. The priority is used to determine in which order mitigations are considered. High priority threats are considered first and low priority threats last. The assumptions are associated because they affect the possible and recommended mitigations. This enables the analyst to directly consider affected threats if due to system specification changes certain assumptions cannot be upheld. Possible countermeasures should be associated to threats to have a set from which a selection can be done. Similar threats should be associated, because those threats may be sufficiently similar to merge certain threats into representative threats as a means to reduce analysis effort.

Countermeasure Recommendation: The countermeasure recommendation represents the mitigation of threats found in the prior phase and produces a set of countermeasures which constitute the information security concept. The potential countermeasures from the threat analysis must be evaluated in a holistic manner. This includes their mitigation potential on the respective threat category, their possible impact on other threat categories, the necessary effort of implementation and their role and interdependence in the system-wide mitigation effort. The evaluation of a potential countermeasure in these categories is carried out with expertise regarding the system. A specific evaluation methodology is not considered in this paper, but exists in standardized form e.g. in [24] under the term *consolidation*. Based on this first evaluation, a set of countermeasures is selected. Upon this selection, a reevaluation of the found threats is executed, now including the selected mitigations, and in addition, considering new threats introduced by the selected countermeasures. This triggers the second of possibly more iterations starting at the 1st step of the 3rd phase of the described process resulting in a set of first and higher-level countermeasures. These countermeasures form the recommendations representing the aspired information security concept.

4 Application of the Methodology and Results

The use case and the application of the described development process onto the use case will be illustrated in this section. For better comprehension and topical focus representative aspects of the steps described prior are presented.

4.1 Description of the Use Case

The use case for the application of the described development process evolves from the digitization of a Quality Assurance (QA) process for aircraft structure components. The original QA process requires the inspectors to examine features like steps and gaps of fuselage elements or heights of rivet heads based on an inspection plan in paper format

distributed to the inspectors. The inspection itself is executed manually with analog measurement tools (e.g. calipers) and the inspection results are to be written in paper form. From there, the resulting documentation reports are sent to be manually digitized by office staff.

The described QA process suffers from several drawbacks. First, manual unassisted inspections based on individual worker-skill are not sufficient with narrow tolerances. Second, tolerances for every feature must be extracted from the physical inspection plan. Third, a lack of information transparency regarding the state of the inspection may lead to duplicate work. Last, measurements taken manually cannot be directly integrated into higher-level data management systems.

To improve the QA process regarding the described shortcomings, several objectives were developed. Among those is the deployment of digitally enhanced inspection tools for the seamless integration of measurement data attained from the inspection of the device under test. The measurement data is forwarded to an automated documentation process, which produces a final report from incoming measurement data. This report is then stored in the data base, and appropriately forwarded for print, to be signed for legal reasons. Furthermore, an automated orchestration (flow generator) process is intended to distribute the inspection plans (workflows) and prior documentation data to the inspectors. To provide the digitally distributed data to the inspector and to provide assistance in the inspections, assistance systems such as in [26] are deployed which provide information to the inspector. Last, an operational administrator has to organize the data base for which a digital entry point is needed (Admin relay). All data in the system (flow generator, documentation, assistance, inspection) is centrally managed by the above-mentioned database system which is accessed by the respective processes. System components already known to have to store data (at least as an intermediate) are assigned temporary memory. The overall system described is currently still under development, so not all subsystems have been completely defined and rolled out. However, the implementation of the project is based on typical technologies and protocols of the IIoT. In concrete terms, this means that the measurement tool represents a cyber-physical system and that different protocols such as MQTT and HTTP are employed to transmit data between the different systems used in the process. Thus, this project constitutes a suitable use case for applying the development process for information security concepts proposed here.

4.2 Structural Analysis

First, objectives were developed with decreasing degree of abstraction and reaching an implementational approach. This aspect has already been performed in the use case description.

Second, implementational detail already known in the design process is gathered. For example digitized inspection tools are to be included to facilitate direct integration of measurement data with higher-level data management systems.

Subsequently, requirements are developed. Exemplary the QA process assures the quality of structure components therefore preventing any compromising impact regarding this assurance is representative of a top-level requirement. To guide the ensuing process assumptions are taken. One assumption maintains that Wi-Fi channels are assumed

to be secured via WPA technology. The assumption is not absolute since e.g., configuration management influences how well the employment of such technology translates into tighter security.

Based on the prior steps, the first traditional DFD is developed (Fig. 3) following the methodology illustrated in Fig. 1. First, a context diagram is constructed, which contextualizes the digital quality assurance process in the manufacturing process. Based on the developed objectives the DFD is then iteratively constructed by decomposing model elements into more specific elements until an adequate level of abstraction is achieved. This DFD is altered in respect to the described adjustments (see Sect. 3). If several DFD elements are on the same device this is denoted (e.g., the documentation process and the Flow Generator), also implementationally known communication protocols like the Bluetooth link between inspection process and documentation process are added. Furthermore, the section of the DFD which represents several distributed instances is also denoted. Last, the assumptions affecting individual elements of the DFD are integrated into the model as locks (see Fig. 4), for example the soft assumption (yellow) that Wi-Fi connections employ WPA3. Hard security assumptions are denoted in green and compromising assumptions in red. However, some assumptions may not be clearly associated with only one element and must therefore be considered implicitly for the whole system. This can be seen in the assumption that an industrial shopfloor is generally not accessible to the public.

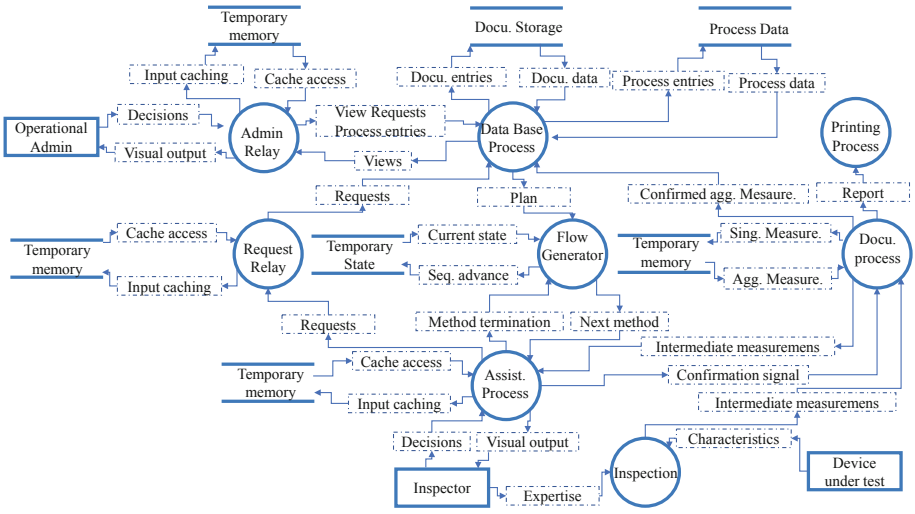

Fig. 3. Traditional system DFD.

4.3 Prioritization via Assets

Assets of the system are developed based on a preexisting Entity-Relationship model developed for the system, which followed the methodology described in [27] to cope

with extensive, heterogeneous, unstructured data. Regarding the selected exemplary objective of digitized inspection tools, the exemplary asset "intermediate measurement data" is considered (see Fig. 3 data from inspection to documentation process). This asset describes measurement data which was generated in the sensors of the digitally enhanced inspection tools, but was not yet confirmed by the inspector as the correct value.

All assets are evaluated regarding severity of the STRIDE threat categories if a threat of said category was to be executed successfully. Exemplary, the intermediate measurement data is assessed to have a high priority regarding spoofing and tampering threats, which results directly from the formulated top-level requirement that any compromise of the QA process results is of high priority.

The developed assets are mapped to their associated DFD elements. In the case of the intermediate measurement data this includes the inspection process as well as the data flow from there to the documentation process amongst others. The associated DFD elements subsequently inherit the resulting priorities, which renders the deviating model where resulting priorities are assigned to a selected set of elements (Fig. 4).

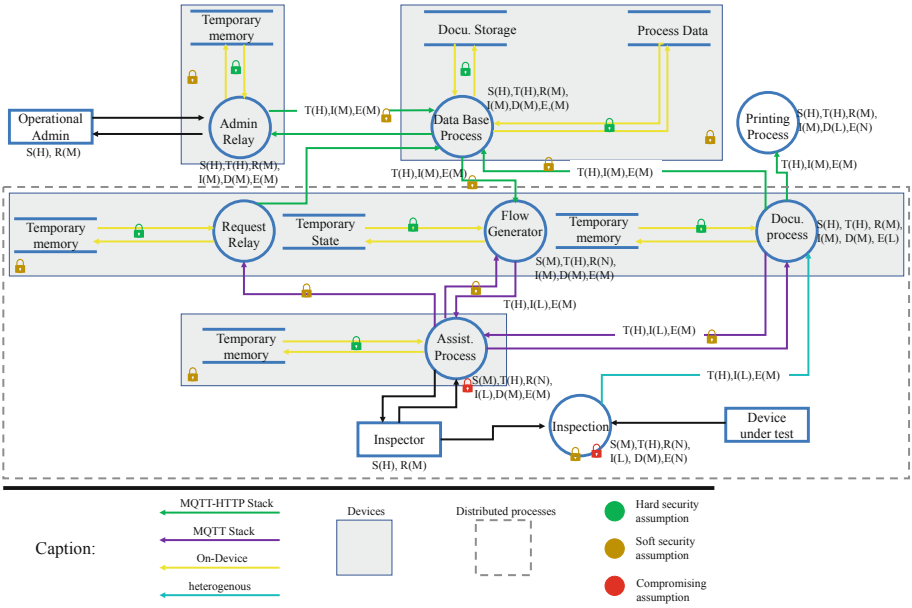

Fig. 4. System DFD with proposed adjustments and inherited priorities.

4.4 Threat Analysis

The STRIDE-per-element threat analysis was executed in the order of the assigned priorities. As an example, the tampering threats regarding the data flows associated with intermediate measurement data were among the first to be analyzed. Deviating

from the traditional STRIDE-per-element execution, the found threat scenarios were merged into representative threat scenarios in the described manner. All representative threat scenarios were assessed regarding made assumptions in the structural analysis and potential countermeasures were assigned. Amongst others, this results in a higher importance of configuration management for employed Wi-Fi technology than in the technical aspects of possible spoofing or tampering threats affecting Wi-Fi connections since WPA3 was assumed to be deployed.

4.5 Countermeasure Recommendation

The potential countermeasures from the threat analysis were evaluated in the manner described in Sect. 3.1 "countermeasure recommendation". For all countermeasures which were assessed to be promising, the threat analysis is executed again to assess if new threats are introduced. If so, those second-level threats are treated the same as first-level threats. This iterative process was executed until residual vulnerabilities were considered acceptable. Exemplary, spoofing threats from human actors in the system are aimed to be mitigated with an authentication scheme. As a second-level threat, the authentication scheme might require only weak passwords or degrading back-up authentication. These common threats are assessed to be mitigated by employing state-of-the-art authentication schemes implementing concepts described for example in [28]. The set of countermeasures in its totality forms the information security concept.

4.6 Results

The analysis of the adjusted DFD model with its prioritized sections resulted in 20 representative threats with 13 high-priority threats (see Table 1). The countermeasure recommendation provided respective mitigations for almost all found threats. Further, it produced residual vulnerabilities such as the possibly compromising capabilities of digitized inspection tools regarding secure device authentication schemes and potential architectural improvement regarding security by transferring interactions with "feature tolerance" assets to the inspectors instead of the operational administrators. It should be noted that the vulnerability arising from the inspection tool capabilities is a Security-By-Design related aspect since this can either be specified or considered solved when more implementation detail becomes known. As key results the mentioned representative high priority threats are presented.

Table 1. Representative high priority threats.

#	Threat description
1	Spoofing of the operational admin and manipulating documented measurement values and feature tolerances
2	Admin repudiates against illegitimate manipulation of data, e.g. altering feature tolerances
3	The inspector is spoofed to the inspection process and produces illegitimate measurement data
4	The inspector is spoofed to the assisting process and to the inspection process which enables the adversary to produce measurement data and confirm it
5	Documented values or a report contain problematic entries and no inspector claims responsibility
6	Documentation process is tampered with as a means to manipulate measurement data after it has been confirmed
7	Spoofing the documentation process to the printing process and printing illegitimate reports
8	Spoofing inspection process to documentation process and sending illegitimate measurement data
9	Spoofing the documentation process to its temp data store to manipulate cached confirmed measurement values
10	Inadequate authorizations and consequentially usability issues undermining security policies
11	Tampering with the aggregated measurement values transmitted from documentation process to DB process
12	Information tampering threat on dataflow from inspection process to documentation process
13	Tampering with the documentation data store of the DB to alter reports or with the association data store to alter tolerances

5 Discussion and Future Work

In summary, this paper presented a strategic development process utilizing adjusted DFDs and an adjusted STRIDE methodology. IIoT use cases have distinct aspects which justify the adjustments. The aspects are: their cyber-physical nature, the Security-By-Design approach and lastly their size regarding modelled elements and assets.

5.1 Summary

The presented strategic development process provides a modular framework for Security-by-Design threat modelling approaches in the IIoT domain and is integrated with the development of the underlying system. Objectives, functional requirements,

assumptions, implementational detail and assets result from the functional system development and are integrated with security-oriented requirements, scoping decisions and asset prioritizations. Based on the strategic phases 1 and 2 and the outlined prioritized model, the threat analysis can be executed in 3 and followed up by the recommendation of countermeasures in 4.

The proposed deviation from the traditional DFD modelling integrates the description encompassing data flow communication channels from physical to application layer. Additionally, it introduces the notion of devices into the DFD, which provides context for the threat analysis. Last, it includes notation for centralized and singular system sections and vice-versa for decentralized sections with various instances, which provides information affecting exposure and impact of attacks.

The adapted STRIDE method applies a risk-first approach where the deviation from the eSTRIDE method consists of transferring the perspective from the evaluated assets back to the DFD elements. This deviation makes it possible to apply the risk-first approach with more traditional STRIDE variants like STRIDE-per-element and STRIDE-per-interaction. Similar to eSTRIDE, assets are identified beforehand and evaluated. In the proposed method this evaluation is based on the STRIDE threat categories. The resulting priorities are assigned to the assigned DFD elements and in the prioritized order threats are analyzed with the STRIDE-per-element variant of the STRIDE method.

5.2 Discussion About the Methodology and Its Application

The application of the strategic development process with its modularization into phases and tactical steps onto the use case described in Sect. 4 systematically produced an information security concept covering all found threats or describing system aspects, which could not be concluded upon due to the design stage of the considered system under development. The process allowed for swift adaption in the event of a change in prior phases or tactical steps and its results present a solid starting point for the continuous development in the sense of Security-By-Design. It thereby successfully adapts the BSI-security process to Security-By-Design development. Furthermore, the process is clearly modularized regarding the purpose of the described phases and tactical steps. Last, it provides the strategic perspective for risk-first threat analysis approaches and embeds them into the overall development process.

Regarding the adapted DFD modelling approach, the time consumption of the additional aspects of the model proved negligible in comparison to the traditional system modelling, while the device notation enabled the analysis to consider threats aimed at whole devices rather than pure cyberattacks aimed at traditional DFD elements. By using the protocol annotation for data flows, the produced threats become more specific in comparison to the threats associated with more generic DFD elements. Annotating distributed system components with multiple instances facilitates assessments of exposure and impact of possible attacks. While the analysis benefitted from annotating the assumptions, it became apparent that due to on the quantity of assumptions and their difference in specificity (to one element) and generality (affecting all elements), they may struggle to be manifested through a visualized format. Given that assumptions may be very peculiar, it also did not seem reasonable to proceed in unison to the asset priorities

and let the DFD elements inherit a general level of security based on taken assumptions. Therefore, a selection of assumptions to present visually might be made.

The prioritized and adapted STRIDE method is based on the evaluation of assets. This was considered positive, given that the assets were conceptually known while the implementational detail was still only partly defined. The categories to evaluate the assets may be improvable, seeing as the evaluation based on STRIDE threat categories pushes the analyst to consider threats before the actual threat analysis. This may cause confusion regarding the otherwise clearly separated phases. A solution would be to use security properties as the basis of evaluation (e.g., Confidentiality, Integrity, Availability, Accountability and Authenticity). Another notable aspect is that the risk-first approach prioritizes the threat analysis such that high priority threats are found faster, while in traditional STRIDE threats are found without regard to their possible priority. Many of those unprioritized threats may then be discarded afterwards when a risk assessment renders a low priority. This however, means that the effort that was spent finding them was spent inefficiently [eSTRIDE case studies "Finding security threats that matter"]. Furthermore, the possibility to combine the risk-first approach and thereby integrating its benefits with the well-established and documented STRIDE-per-element variant is considered the most important beneficial take-away. Notably, it serves as an alternative to eSTRIDE if the prior development steps render many assets in comparison to the number of DFD elements. In such a situation, the described approach might reduce analysis effort.

With regard to the manufacturing domain, the presented process with the associated methodologies can be used to examine IIoT-based applications for critical aspects of security even during their development phase. Using the adjusted DFD, a graphical representation of the use case with critical aspects is modeled, fostering a common understanding between manufacturing and security experts. Impacts of design decisions, such as the choice of a particular communication protocol, can be quickly captured and evaluated, and countermeasures to potential threats can be developed in parallel with the overall application. This work thus represents a contribution to the enablement of secure IoT applications in manufacturing.

5.3 Future Work

Future work should investigate modelling approaches to cyber-physical systems which do not depend as heavily on the perspective of digital data as DFDs. Furthermore, efforts should be made to find standardized manners of integrating physical system aspects into the modelling process. Additionally, approaches for the piecewise integration of implementational detail into models for iterative Security-by-Design approaches may be explored. Regarding the application of the STRIDE methodology in cyber-physical systems further research should consider options to better include physicality; either in modelling or in the analysis itself. The same holds true for the threat analysis of architectural systems, where the promising research might exist in efficient approaches to threat modelling of systems of higher abstraction.

This work provides a development process for information security concepts containing three novel approaches which enable the efficient and effective integration of security into the development process of IIoT-systems, thereby minimizing security risks.

References

1. Morgan, S.: Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021(2020). https://cybersecurityventures.com/annual-cybercrime-report-2020/. Accessed 08 Feb 2022
2. CSIS. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 08 Feb 2022
3. Yu, X., Guo, H.: A survey on IIoT security. In: 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS). IEEE (2019)
4. Boyes, H., et al.: The industrial internet of things (IIoT): an analysis framework. Comput. Ind. **101**, 1–12 (2018). https://doi.org/10.1016/j.compind.2018.04.015
5. Bostjancic Rakas, S., et al.: Industrial Internet: architecture, characteristics and implementation challenges. In: 2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH): 17–19 March 2021, Jahorina, East Sarajevo, Republic of Srpska, Bosnia and Herzegovina: Proceedings, pp. 1–4. IEEE, Piscataway, NJ (2021)
6. Ani, U.P.D., He, H., Tiwari, A.: Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. J. Cyber Secur. Technol. **1**, 32–74 (2017). https://doi.org/10.1080/23742917.2016.1252211
7. Tsochev, G.: Some security problems and aspects of the industrial internet of things. In: 2020 International Conference on Information Technologies (InfoTech), pp. 1–5 (2020)
8. Burnap, P.: Risk Management & Governance: Knowledge Area (2021). https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf. Accessed 08 Feb 2022
9. Santos, J.C.S., Tarrit, K., Mirakhorli, M.: A catalog of security architecture weaknesses. In: 2017 IEEE International Conference on Software Architecture Workshops (ICSAW), pp. 220–223. IEEE (2017)
10. Bundesamt für Sicherheit in der Informationstechnik BSI-Standard 200–2 - IT-Grundschutz Methodology (2017)
11. Eckert, C.: IT-Sicherheit: Konzepte, Verfahren, Protokolle, 10. Auflage. De Gruyter studium. De Gruyter Oldenburg, München (2018)
12. Mohamed Shibly, M.U.R., Garcia De Soto, B.: Threat modeling in construction: an example of a 3D concrete printing system. In: Proceedings of the 37th International Symposium on Automation and Robotics in Construction, ISARC 2020: From Demonstration to Practical Use - To New Stage of Construction Robot, pp. 625–632 (2020)
13. Shevchenko, N., et al.: Threat Modeling: A Summary of Available Methods (2018)
14. AbuEmera, E.A., ElZouka, H.A., Saad, A.A.: Security framework for identifying threats in smart manufacturing systems using STRIDE approach. In: 2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), pp. 605–612. IEEE (2022)
15. Borgaonkar, R., et al.: Improving smart grid security through 5G enabled IoT and edge computing. Concurr. Comput. Pract. Exper. **33**, 1–16 (2021). https://doi.org/10.1002/cpe.6466
16. Danielis, P., Beckmann, M., Skodzik, J.: An ISO-compliant test procedure for technical risk analyses of IoT systems based on STRIDE. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, pp. 499–504 (2020)
17. Empl, P., Pernul, G.: A flexible security analytics service for the industrial IoT. In: Gupta, M., Abdelsalam, M., Mittal, S. (eds.) Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, pp. 23–32. ACM, New York, NY, USA (202)
18. Khan, R., et al.: STRIDE-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pp. 1–6. IEEE (2017)

19. Yampolskiy, M., et al.: Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. In: 2012 5th International Symposium on Resilient Control Systems, pp. 55–62. IEEE (2012)
20. Shostack, A.: Threat Modeling: Designing for Security. Wiley, Indianapolis (2014)
21. Tuma, K., et al.: Finding security threats that matter: two industrial case studies. J. Syst. Softw. **179**, 111003 (2021). https://doi.org/10.1016/j.jss.2021.111003
22. Shevchenko, N., Frye, B.R., Woody, C.: Threat Modeling for Cyber-Physical System-of-Systems: Methods Evaluation. Carnegie Mellon University Software Engineering Institute, Pittsburgh, United States (2018)
23. Tuma, K., Scandariato, R., Widman, M., Sandberg, C.: Towards security threats that matter. In: Katsikas, S.K., et al. (eds.) Computer Security. LNCS, vol. 10683, pp. 47–62. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-72817-9_4
24. Bundesamt für Sicherheit in der Informationstechnik BSI-Standard 200-3 - Risk Analysis based on IT-Grundschutz (2017)
25. Joint Task Force: Risk management framework for information systems and organizations. National Institute of Standards and Technology, Gaithersburg, MD (2018)
26. Müller, R., et al.: The Assist-By-X system: calibration and application of a modular production equipment for visual assistance. Procedia CIRP **86**, 179–184 (2019). https://doi.org/10.1016/j.procir.2020.01.021
27. Koch, J., Lotzing, G., Gomse, M., Schüppstuhl, T.: Application of multi-model databases in digital twins using the example of a quality assurance process. In: Andersen, A.-L., et al. (eds.) Towards Sustainable Customization: Bridging Smart Products and Manufacturing Systems. LNME, pp. 364–371. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-90700-6_41
28. Grassi, P.A., et al.: Digital identity guidelines: authentication and lifecycle management. National Institute of Standards and Technology, Gaithersburg, MD (2017)