Combining Safety and Security Analysis for Industrial Collaborative Automation Systems

Sándor Plósz[1(✉)], Christoph Schmittner[1], and Pál Varga[2]

[1] Department of Safety and Security, Austrian Institue of Technology, 1220 Vienna, Austria
{Sandor.Plosz.fl,Christoph.Schmittner}@ait.ac.at
[2] Department of Telecommunications and Media Informatics, Budapest University of Technology and Economics, Budapest 1117, Hungary
pvarga@tmit.bme.hu

Abstract. In collaborative automation systems, providing both security and safety assessments are getting increasingly important. As IoT systems gain momentum in the industrial domain, experts stress their concerns about security and safety. Improperly or carelessly deployed and configured systems hide security threats, and even raise issues on safety, as their behavior can threaten human life. The cloud based back-ends are getting used for processing sensor data – on the other hand, legacy equipment, which may contain sensitive information, is made interoperable with broader infrastructure. Safety risks can be triggered by attacks on the backend and confidential information is at risks by attacks on legacy equipment.

In order to maintain safe and secure operations, safety and cybersecurity assessment methods have been established. There is an increased demand in modern industrial systems to perform these regularly. These methods however require a lot of time and effort to complete. A solution to this problem would be combining the assessments. This requires that proper safety and security analysis methods must be selected – those that have compatible elements.

In this paper we propose a method that combines the elements of existing methodologies, in order to make the safety and security analysis process more effective. Furthermore, we present a case study, where we verified the combined methodology.

1 Introduction

The advantages of utilizing the Internet and service-oriented information technology systems on physical systems are beyond dispute. Consequently, the physical world and the world of information technologies are converging. This results in the appearance of Cyber-Physical Systems (CPS). Industrial CPS systems (or Cyber-Physical Production Systems, CPPS) contain critical business information, which will be made accessible in the cloud. It is clear, that any weak

S. Tonetta et al. (Eds.): SAFECOMP 2017 Workshops, LNCS 10489, pp. 187–198, 2017.
DOI: 10.1007/978-3-319-66284-8_16

points in the cloud domain can cause serious reactions in the physical domain, resulting in significant impact on commercial and company values – as well as on human safety.

In order to ensure safety, security and reliability of such systems, threats and failures need to be considered on all (both physical and cyber) levels of its operation. Security is a property which expresses the ability to maintain confidentiality, integrity and availability of the system and its assets. Safety is a property which guarantees that the system cannot cause damage to life, health, property, or environment. In other words security needs to ensure the system is protected from the environment, whereas safety needs to protect the environment from the system [7].

Although well-suited and proven analysis methods exist in the IT domain, the different aspects of CPPS pose new and more strict requirements. In CPPS, security objectives such as availability and integrity are of the utmost importance – however, due to the connections with the physical world, assuring safety and reliability are just as critical. Similarly, there are established techniques to assure safety and reliability in the IT domain, but they do not consider new challenges introduced by this wide connectivity. Security threats can have impact on the safety and reliability of the system, therefore these are no longer completely independent properties. Following this finding, such a combined approach would be beneficial, which allows the analysis of the complete data path – from the industrial M2M communication to the Internet and cloud connectivity –, and considers threats and failures. The goal is that both availability and integrity be ensured on the lowest level of the machinery by closing all the weak points in the system.

For safety and reliability, the challenge is that most techniques were developed for not-connected systems, consisting of almost solely hardware parts. Electronics and software is challenging, because the calculation of risks is different than for hardware. Software does not randomly fail due to aging or environmental influences, but has built-in weaknesses that are triggered. Instead of quantitative assessments, only qualitative evaluations are possible. In addition to that, detailed analysis methods such as Fault Tree Analysis are challenged by the increasing complexity and connectivity.

To overcome these challenges we have created a combined approach, which merely requires some affordable efforts to point out the main risks in such systems, hence it is quite effective.

2 Related Work

There are a handful of existing approaches to analyze system security. A number of them is based on Threat Analysis and Risk Assessment (TARA) [4] which is a simple procedural approach. [17] presents a different approach, a framework to analyze security requirements based on fuzzy logic and calculate how security resources should be allocated.

There are several methods to perform TARA such as TVRA (Threat, Vulnerabilities, and implementation Risks Analysis), OCTAVE (Operationally Critical

Table 1. Brief summary of security analysis methods

Method	Summary
EVITA	Result of the EVITA research project; classifies different aspects of the consequences of security threats (operational, safety, privacy, and financial); classification of safety-related and non-safety-related threats differs and could thus lead to in-balances; accuracy of attack potential measures and expression as probabilities is still an open issues [10]
TVRA	Models the likelihood and impact of attacks; developed for data - and telecommunication networks; applicability for cyber physical systems is unclear [4]
OCTAVE	Developed for enterprise information security risk assessments; applicability for cyber physical systems is unclear; includes interviews and workshop with all stake holders to consider all concerns [8]
HEAVENS	Based on Microsoft's STRIDE approach; determination of threat level (TL), impact level (IL), and security level (SL) for classification of threats; does not scale easily with number of threats; requires discussion of each factor of each single threat [12]
Attack Tree Analysis (ATA)	Analogous to fault tree analysis (FTA); identifies attack paths and vectors in hierarchical manner, describes movement of an attack through the system to reach attack goal; benefits from a stable system design and known vulnerabilities; requires already identified attack goals [21]

Threat, Asset, and Vulnerability Evaluation) or Attack Trees. These methods are summarized in Table 1. The TVRA method can determine security risk based on the likelihood and impact measures of identified threats. In order to identify threats, it is best to model the system as components. The Microsoft Threat Modeling Process [20] can be used for modeling and threat identification. It describes the model elements and the meta-language for producing a threat catalog – based on the model.

The industrial sector is not aided with security standards in the same extent as the IT domain. The ISA/IEC 62443 family of standards is being developed from the ISA99 US standard family jointly by ISA (International Society of Automation) and IEC (International Electrotechnical Commission). These target Industrial Automation and Control Systems (IACS) security [6]. The concept to perform security risk assessment and management is similar to what is outlined in the ISO 27000 family [18].

In order to identify the possible safety risks in a system, safety analysis investigates potentially hazardous situations for causes and probability. Based

on the severity of the hazardous situation and the probability of the cause, the risk can be calculated. The FMEA method [2] is a well known and thoroughly used method for the safety assessment.

There have been some research on performing safety and security analyses in combination. In [14] an overview of approaches and methods are given based on the SAE J3061 guidebook [5] for analyzing security in the automotive domain. Kriaa et al. developed a survey of approaches combining Safety and Security for Industrial Control Systems [13]. The challenge with most of the presented methods is that they focus only on the connected safety-critical system and not on the complete communication system, e.g. from the safety-critical system to the IT back end.

The safety domain is aware of these issues and started to tackle the new challenges of considering safety and security in an holistic way. The IEC 61508 standard [3] is applied when no domain-specific standard is available, and is used to develop domain-specific standards.

Complementing this activity, IEC workgroup TC 65/WG 20 "Industrial-process measurement, control and automation – Framework to bridge the requirements for safety and security" works on how to combine safety with security engineering and lifecycles.

3 Case Study

The Arrowhead project produced an interoperability framework for IoT automation systems. The framework has been demonstrated on different use-cases; many of them comprising CPS. We have performed safety and security assessment on an automotive use-case. The use-case scenario was to aggregate device measurement data at customer test sites into the backend of the equipment provider for statistical and diagnostic purposes in order to optimize the maintenance schedule of the measurement equipment. There have been multiple versions of the solution architecture for each of the three generations of the Arrowhead framework. We had performed risk analysis and based on the result the architecture had been refined. Beside analysis and assessment huge emphasis was also put on service level security in the Arrowhead framework [19].

The use case is a legacy system, used in automotive production for the testing of engines, which needs to communicate with the system manufacturer. The goal is to collect system status data in order to optimize maintenance, predict and increase system availability. The challenge in adopting a legacy system to meet the needs IoT and collaborative automation was to handle the increased attack surface without completely re-designing the existing system. There was no reference guides to follow for system adoption. This resulted in a sequential process of safety and security risk analysis and threat mitigation solution.

During the first assessment we identified the most critical assets. These are the configuration and test data on the test system, and the data in the backend, which must be kept confidential.

Figure 1 shows a high level data-flow model of the analyzed use-case created in the Microsoft Threat Modeling Tool. The model can be divided in two major

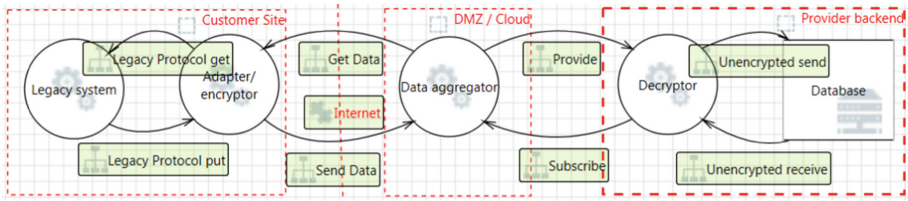

Fig. 1. Generic threat model (Color figure online)

parts, the local network and the cloud/backend network; these are outlined by red striped rectangles. These are called trust boundaries, in order to express a separation of security requirements. The other form of expressing separation of trust is a red striped line crossing data flows, in this case the Internet as the communication channel.

Most elements of the architecture are modeled as processes depicted as spheres in the figure. Processes exhibit the widest functionality but can also be affected by most of the possible threats according to the threat analysis model detailed in the next section. The model consists of three main parts:

- Customer site: includes the measurement CPS, which is the legacy system designed without extensive security measures or the need to be connected to the Internet. In the described use case it is connected through its supported legacy protocol to an adapter. This adapter provides security by encrypting the data and also implements an Internet transport protocol. Data is sent periodically to the service provider under the supervision of the customer to maintain the desired level of information privacy.
- DMZ/Cloud: the remote site in the DMZ (Demilitarized Zone), which can be in a cloud or a separated network of the service provider. The process called as data aggregator implements a publish-subscribe interface, but also acts as a firewall, authenticating the clients. The service provider can subscribe for the data of particular clients.
- Provider backend: comprised of elements on the provider network such as the decryptor which requests, receives and decrypts the data from the measurement devices, processes the data, calculates statistics and schedules maintenance of the equipment. This latter information is communicated back to the customer through another communication channel. Some of the data is put in the database unencrypted.

Even on this basic model the threat modeling tool detects 74 different security threats.

4 Safety and Security Assessment

Assuring safety and security are very crucial both in IT and industrial systems in order to avoid loss of value, damage or injury. Therefore safety and security

aspects are advised to be considered from the design phase early on, but they need to be observed and assessed constantly during the system lifetime. Safety and security assurance is a process which includes planning, design, assessment and mitigation.

In this section we present a solution for performing safety and security assessment in combination to minimize the required effort.

4.1 Security Assessment

The goal of security assessment is to identify weaknesses in the system under analysis, and evaluate the risk these pose on the system. The security analysis method which we have followed is in line with security risk assessment described in ISA/IEC 62443 [6]. According to the standard, at first we identify potential vulnerabilities in the system which can pose threats; then assess the risks in terms of their consequence and likelihood; finally, the risks are communicated and understood in the form of summarizing and documenting results that can be used for evaluation and treatment. Our security analysis approach comprises several steps, which are detailed below.

Threat Modeling. The process of risk assessment generally has an initial step: modeling the system under investigation. This can be performed on many levels of detail, but usually is an iterative process by creating a simple model and iteratively refining it for the required detail. The sufficient level of detail is determined by the detail-level that the expected results should point out.

The most widely used modeling format in this domain is the Data Flow Diagram (DFD). DFDs can model system components and their interactions. Microsoft's threat modeling tool [15] allows DFD modeling of the system, as well as creating a threat catalog based on the DFD. A DFD may consist of the following elements: External Entity (EE, e.g. users), Processing Node (PN, e.g. a process), Data Store (DS) and Data Flows (DF). Assembling the threat catalog from the DFD is based on the STRIDE method [11]. The acronym stands for the six possible threat categories. Table 2 lists these categories, the security objectives that are violated by that kind of threats and the components where such threat may arise.

Table 2. STRIDE threat categories and affected security objectives

Threat	Affected security objective	Involved element
Spoofing	Authentication	EE, PN
Tampering	Integrity	DF, DS, PN
Repudiation	Non-Repudiation	EE, PN
Information disclosure	Confidentiality	DF, DS, PN
Denial of Service	Availability	DF, DS, PN
Elevation of Privilege	Authorization	PN

The idea behind building a threat catalog from a DFD is that a vulnerability is only possible due to an interaction between DFD components. The components between te endpoints of a data flow determine what kind of vulnerability may be exploited in that flow as shown in the table.

Risk Assessment. Risk assessment determines threat criticality based on the likelihood of exploitation, and the resulting impact. Several ranking schemes can be used. We have found ETSI TVRA a simple-to-apply, but sufficiently detailed method. It is a qualitative analysis method, described in standard TS 102 165-1 [4]. According to this, the likelihood measure depends on two factors, (i) the difficulty of executing a successful attack and (ii) the motivation an attacker may have behind it. This latter relates to what an attacker can gain from the attack, which can be either objective (e.g. information) but also subjective (e.g. revenge).

Table 3. Result of security risk assessment

Threat name	Type	Difficulty	Motivation	Likelyhood	Scale	Detectability	Impact	Risk
Improper data protection of Database	Interception	None	High	Likely	Whole NW	Low	Significant	Critical
Spoofing of Database	Masquerade	None	High	Likely	Whole NW	Low	Significant	Critical

The impact measure is determined by the scale level (extent) of the attack and detectability (and recoverability) of the attack, e.g. the difficulty to restore the system to the state prior the attack.

This standard qualifies each of the above measures in three levels. For each threat, the resulting risk can have three possible values as well, namely: minor, major or critical. In Table 3 we listed the threats which possess the most critical risk as the result of the risk assessment process.

4.2 Safety Assessment

The goal of safety assessment is to identify those risks that are related to the system, and have non-malicious and internal causes. We have found that the FMEA method can be applied to Data Flow Diagrams (DFD), the same model we use for the security assessment, and delivers results with a similar level of granularity as our security assessment approach.

Adaption of Failure Modes. FMEA was originally developed for hardware and electronic elements. For such elements, failure mode lists based on experience and probability data based on reports and testing of components exists. As an example, the Siemens Norm 29500 [16] is often used to calculate reliability

and failure data for electronic components. It contains extensive lists for Failure Modes for different types of electronic components and formulas to calculate failure probability based on use and environmental conditions. In order to apply the assessment method to software and network based systems – where failure modes are more likely to be caused by software bugs than by failing resistors – some adaption is necessary. While Failure Modes for hardware components are clear failure modes, they can be much harder to define for software components. Haapanen [9] surveys different approaches for FMEA regarding software components.

Table 4. Faults and affected elements

Fault description	Element			
	Function	File/ Database	Input/ Output	Flow
Missing Data e.g. lost message, data loss due to hw failure		x		x
Incorrect Data e.g. inaccurate, spurious data		x		x
Timing of Data e.g. obsolete data, data arrives too soon for processing			x	x
Extra Data e.g. data redundancy, data over-flow		x	x	
Halt/Abnormal Termination e.g. hung or dead-locked at this point	x			
Omitted Event e.g. event does not take place, but execution continues			x	
Incorrect Logic e.g. preconditions are inaccurate; event does not implement intent	x			
Timing/Order e.g. event occurs in wrong order; event occurs too early/late	x		x	x

We have created a mapping between the list of failure modes of software components and the elements of the DFD that are prone to that failures. This mapping, shown partially in Table 4 is similar to how STRIDE defines which kind of threat affect which diagram component. This makes it possible to use a single system model for the safety and the security assessments and automate the process. This can also facilitate the exchange and cooperation between safety and security experts and to avoid differences based on different system representations.

The goal of FMEA is to consider failure modes, the effects and probability of these for all elements of a system. Starting with a system model, in our case the DFD of the use case, for each element the potential failure modes are identified based on the above table. Then potential system level effects for each failure mode are investigated and causes determined.

Table 5. Result of safety risk assessment

Element	Threat name	Type	Likely-hood	Scale	Detect-ability	Impact	Risk
Database	Error in config.	Incorr. Data	Un-likely	Whole NW	Low	Safety Critical	Critical
Adapter - test system comm.	Incorr. timing	Timing	Likely	Node	Low	Relia-bility	Major
Adapter - test system comm	Msgs. transm. twice → undef. system state	Extra data	Possible	Node	Low	Safety Critical	Critical

Risk Assessment. We utilized the basic risk assessment approach as defined in IEC 60812 [1] for the results of the FMEA analysis. While it is not possible to calculate the probability exactly like for hardware elements, we discussed each element and its *Failure Modes* with domain experts and estimated a quantitative likelihood, divided in 5 levels. In order to ease the cooperation with the security experts, we adopted a similar approach for impact assessment. The *Scale* level describes whether a *Failure Mode* only effects part of one installation or multiple installations, recoverability was adapted to include *Detectability*. This is similar as envisioned for the FMEDA, which extends the basic FMEA with a *Detectability* parameter. *Impact* ranges from no impact to safety/reliability or availability impact. Due to the connected risk, a safety-impact leads automatically to a risk-rating of critical. Table 5 shows the most critical safety threats found as the results of the safety assessment.

4.3 Combined Assessment

Performing detailed safety and security analysis on an industrial use-case is a very time-consuming task. We have found that safety and security are not completely separable properties of such systems. We have shown that security and safety analysis can be automated using a common model and risk analysis guidelines. The first step of the analysis is to create a system model. A Data Flow Diagram represents system components as interacting processes. The process is the most basic entity which can represent the encompassed state machine of both hardware and software elements. We used the STRIDE method for creating a security threat catalog, and also adapted its methodology for creating the safety threat catalog.

The combined method assembles the threat catalog based on the data flows connecting components and the constraints of those. The same way as for security we can also define safety constraints, so the algorithm for security threat generation can be extended for safety as well. This realization implies that we can use the same system model and automate the process of both security and safety assessments. There is more to deliberate on the impact and risk levels of safety threats as there can be dangers to humans involved – which obviously cannot be ranked the same level as data corruption and financial losses.

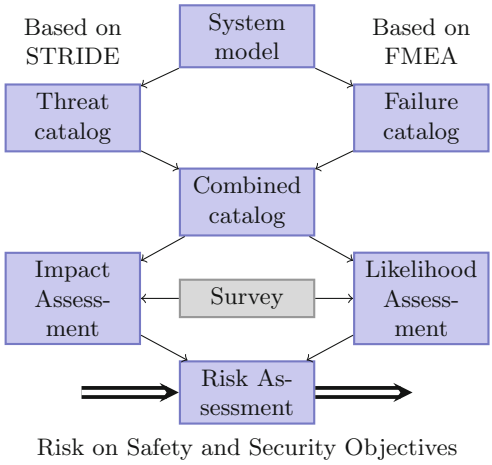

Fig. 2. Combined risk assessment process

The STRIDE threat generation process puts threats into different categories according to what security objectives are affected. During risk assessment for each threat the risk level can be calculated separately for all the objectives. These objectives can however be amended with safety related ones, which solves the threat ranking issue and the fact that certain security threats can have impact on safety. This is what we have followed in our combined analysis method, which is depicted in Fig. 2.

4.4 Advantages of the Combined Assessment

The combined assessment has the following advantages.

Ruling Out Duplication of the Assessments. Safety and Security assessments have a lot of common, overlapping issues in all domains (such as hardware, information handling, etc.). As a natural advantage of the combined assessment, it saves a lot of effort by handling these commonalities at once.

Combined Safety and Security Catalog. The combined catalog is built from the Threat Catalog (of security assessment) and the Failure Catalog (of safety assessment). Its elements can be commonly addressed by the impact and likelihood assessments. This allows raising awareness on issues that has high impact or likelihood on both safety and security.

Supporting Multi-dimensional Decisions. One of the desired output of both the safety and the security assessments is to provide information on system development decisions (even if the system is deployed already). As we pointed out in the introduction, these are multi-dimensional decisions, that are supposed

to find the balance between security, safety, privacy, reliability, power efficiency, and even price. The combined assessment supports this decision by handling four factors at once: beside security and safety, privacy and reliability is also assessed. Privacy issues are part of the threat catalog, reliability issues are part of the failure catalog – and these are both utilized when the combined catalog is created.

5 Conclusion

Collaborative automation systems invoke fresh motivation for safety and security assessments, since they mix issues related to physical equipment (e.g. industrial machinery), data handling (e.g. storage and networking) and virtualized IT solutions (e.g. cloud computing).

When such Cyber-Physical Systems are used in industrial applications, both safety and security issues need to be covered, otherwise the meaning of IoT would quickly inflate from Internet of Things towards Internet of Trash. CPS systems that have elements with security vulnerabilities can be a potential threat to human life. Such ideas conceived our concept of creating a combined safety and security assessment method.

Our practical experiences of utilizing various standards when assessing complex and extensive CPS systems lead to the realization of a combined safety and security assessment method, described in this paper. The method builds upon STRIDE and FMEA approaches, and it uses a combined catalog for threats and failures – in order to conduct impact and likelihood assessments as an input for assessing risk.

The advantages of this combined assessment include (i) saving effort by handling the commonalities of separate assessments at once; (ii) utilizing the combined catalog for raising awareness on issues that has high impact or likelihood on both areas, and (iii) supporting multi-dimensional decision making by decreasing the problem space through tackling security, safety, reliability and privacy issues, as well.

References

1. IEC 60812: Analysis techniques for system reliability - procedure for failure mode and effects analysis (FMEA)
2. IEC 60812: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) (2006)
3. ISO 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems (2010)
4. ETSI - TS 102 165–1: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis (2011)
5. SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (2016)

6. ISA: The 62443 series of standards - industrial automation and control systems security, December 2016. http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf
7. Bloomfield, R., Netkachova, K., Stroud, R.: Security-informed safety: if it's not secure, it's not safe. In: Gorbenko, A., Romanovsky, A., Kharchenko, V. (eds.) SERENE 2013. LNCS, vol. 8166, pp. 17–32. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40894-6_2
8. Caralli, R., Stevens, J., Young, L., Wilson, W.: Introducing octave allegro: improving the information security risk assessment process. Technical report, CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh (2007). http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419
9. Haapanen, P., Helminen, A.: Failure mode and effects analysis of software-based automation systems. Techncial report, Radiation and Nuclear Safety Authority, Helsinki (Finland) (2002)
10. Henniger, O., Apvrille, L., Fuchs, A., Roudier, Y., Ruddle, A., Weyl, B.: Security requirements for automotive on-board networks. In: 2009 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST), pp. 641–646, October 2009
11. Howard, M., Lipner, S.: The Security Development Lifecycle. Microsoft Press, Redmond (2006)
12. Islam, M.M., Lautenbach, A., Sandberg, C., Olovsson, T.: A risk assessment framework for automotive embedded systems. In: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, CPSS 2016, pp. 3–14. ACM, New York (2016). http://doi.acm.org/10.1145/2899015.2899018
13. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y.: A survey of approaches combining safety and security for industrial control Systems. Reliab. Eng. Syst. Saf. (2015). http://linkinghub.elsevier.com/retrieve/pii/S0951832015000538
14. Macher, G., Armengaud, E., Brenner, E., Kreiner, C.: A review of threat analysis and risk assessment methods in the automotive context. In: Skavhaug, A., Guiochet, J., Bitsch, F. (eds.) SAFECOMP 2016. LNCS, vol. 9922, pp. 130–141. Springer, Cham (2016). doi:10.1007/978-3-319-45477-1_11
15. Microsoft: Microsoft Threat Modeling Tool 2016 download page (2016). https://www.microsoft.com/en-us/download/details.aspx?id=49168
16. SN 29500: Failure rates of components 6 (1996–06)
17. Park, K.C., Shin, D.H.: Security assessment framework for IoT service. Telecommun. Syst. **64**(1), 193–209 (2017). doi:10.1007/s11235-016-0168-0 http://dx.doi.org/10.1007/s11235-016-0168-0
18. Piggin, R.S.H.: Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security. In: IET Conference on Control and Automation 2013: Uniting Problems and Solutions, pp. 1–6, June 2013
19. Plósz, S., Hegedűs, C., Varga, P.: Advanced security considerations in the arrowhead framework. In: Skavhaug, A., Guiochet, J., Schoitsch, E., Bitsch, F. (eds.) SAFECOMP 2016. LNCS, vol. 9923, pp. 234–245. Springer, Cham (2016). doi:10.1007/978-3-319-45480-1_19
20. Scandariato, R., Wuyts, K., Joosen, W.: A descriptive study of Microsoft's threat modeling technique. Requirements Eng. **20**(2), 163–180 (2015). doi:10.1007/s00766-013-0195-2
21. Wiseman, D.R.: Risk, reliability and safety: innovating theory and practice. In: Attack tree analysis, pp. 1023–1027. CRC Press, September 2016. doi:10.1201/9781315374987-154