A Cybersecurity Risk Assessment Process for Model-Based Industry 4.0 Development

Matthias KERN, Thomas GLOCK, Victor PAZMINO BETANCOURT, Bo LIU, Eric SAX, Jürgen BECKER
FZI Research Center for Information Technology
Karlsruhe, 76131, Germany

ABSTRACT

Cybersecurity risk assessments are important to define a well-justified cybersecurity concept that regards the trade-off between security, costs, and performance. Heading toward Industry 4.0 (I4.0), plants get connected with an increasing amount of sensors and functionalities that have more and more communication interfaces and paths. This leads to a growing cybersecurity attack surface and a higher complexity compared to current plants. Today, a well-structured course of action for a cybersecurity risk assessment is missing in the domain I4.0. Therefore, in this paper, a cybersecurity risk-assessment process containing an asset-, a threat- and an attack-analysis with adapted methodologies from other domains is proposed and the necessary terms for the approach are introduced. Furthermore, a model-based approach is proposed and its prototypical implementation supporting the proposed cybersecurity risk assessment process. Finally, the evaluation of the approach was done by applying it to an industrial use-case.

Keywords: cybersecurity, risk-assessment, industry 4.0, model-based, process

1. INTRODUCTION

Industry 4.0 (I4.0) is the vision to make production smart and as easy as possible, especially for small and medium sized enterprises. This vision can be accomplished by managing every product with an identifier and an associated virtual image [1]. The main goals of I4.0 are a high flexible, easily changeable, optimized and smart production as well as continuous maintenance [2]. Hence, the requirements are that the plants, their modules and products should have the ability to communicate with each other and their data should be collectable and analyzable. This leads to I4.0 plants that requires more flexible communication than plants today. Therefore, the hierarchical communication structure disappears more and more on the way to fully implemented 4.0 plants and it is assumed that the number of interfaces and communication paths will rise sharply. Accordingly, the attack surface for cyber-attacks will increase on the way to fully implemented I4.0 plants. Considering that especially small and medium sized enterprises have, in general, less resources and expertise in cybersecurity, makes concepts necessary that allows understanding the impact of system decisions to cybersecurity easily with a well-structured course of action for a cybersecurity risk assessment. This well-structured course of action is currently missing in the domain I4.0. Existing I4.0 guidelines provide a collection of security mechanism and recommendations for actions but do not describe the path to perform a security assessment in the development phase following the security by design approach. “Security-by-Design is an approach to … designing and building security in every phase of the Systems Development Lifecycle (SDLC) [3].” “*But many systems fail because their designers protect the wrong things, or protect the right things but in the wrong way*” [4]. To protect the right things with an appropriate effort it is important to “*… understand the tradeoff between risk and reward* [4]”. In other words, it is necessary to find a tradeoff between risks, costs, usability and latency. The first step towards this tradeoff is a risk assessment as defined in the ISO/IEC 27005. Another challenge today is the missing tools supporting cybersecurity risk assessments during the development of I4.0 plants. Therefore, in this paper, a model-based applicable cybersecurity risk-assessment process that supports security by design during the early design phase of I4.0 systems is proposed. Necessary terms for the presented approach and categories for assets are introduced. For the threat analysis, the Microsoft STRIDE methodology from the domain information technology is adapted. The HEAVENS risk assessment metric is adapted to evaluate threats and the EVITA methodology to define attack-scenarios. Both EVITA and HEAVENS are from the domain automotive. In the automotive industry, security methods are being developed and developed to serve a mass market with vehicles that have secure connectivity capabilities. In addition, the technologies between automotive and I4.0 has similarities e.g. both work with distributed system architectures. This lead to the decision to transfer methodologies from automotive to I4.0.

2. RELATED WORK

A. Cybersecurity standards and guidelines

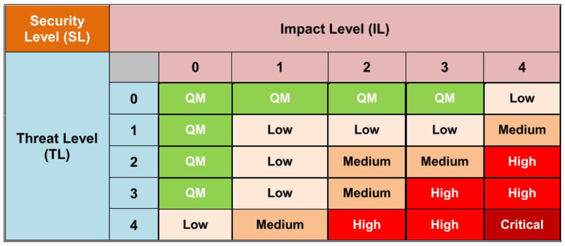
The standard ISO/IEC 27005 „ Information technology – Security techniques – Information security risk management“ defines an information security risk management process based on ISO 31000 and supporting ISO 27001. The proposed process in this paper bases on ISO/IEC 27005 and considers the requirement from ISO 27001 that the information security risk evaluation must be repeated after considerable changes [5].

The information security risk management process defined in ISO 27005 consists of the steps: context establishment, risk assessment, risk treatment and risk acceptance. Beside these steps, there are the step risk communication and the step risk monitoring and review, both not further regarded here. The context in the step context establishing refers to the scope and boundaries. The scope encompass all assets that should be considered during the risk assessment. The boundaries should be gathered to address the associated risks. In addition, the basic criteria for the evaluation of the information security risks should be defined during this step [6]. Risk identification, risk analysis and risk evaluation are part of the step risk assessment. The purpose of risk identification is to determine what could happen to cause a potential loss [6]”. During the risk evaluation, threats, existing controls and vulnerabilities will be identified. During the risk evaluation, the risks will be leveled using the risk evaluation criteria and the risk acceptance criteria. The risk evaluation criteria defines the levels and the rules to rank the risks. The acceptance criteria defines one or more thresholds determining the acceptance of risks under certain circumstances. In the step risk treatment the evaluated risks can be modified, retained, avoided or shared [6].

The standard IEC/TS 62443 “Industrial communication networks – Network and system security” defines basic concepts for the security of industrial automation and control systems. The standard addresses plants that follows a hierarchical communication structure from the field level up to the management level.
The “Plattform Industrie 4.0” is a German association that aims to develop within six working groups the basic concepts towards I4.0, to give recommended actions for science, companies and politics, to support small and medium size enterprises (SMEs) and to facilitate the exchange especially in the scope of IT security and standardization. Within the six working groups, there is a working group for IT security focused of networked systems and a working group that defines a “reference architecture model for I4.0” (RAMI 4.0) and advances the standardization of RAMI 4.0 and belonging topics. The Security working group has published a document “Industrie 4.0 Securtiy Guidelines – Recommendations for actions” [1] containing a section about risk analysis that reduced the risk analysis process down to four steps: identification of assets, determining of protection goals, identification of threats and evaluation of risks [2]. In addition, there is the NIST Cybersecurity Framework Manufacturing Profile that offers general requirements for a cybersecurity risk assessment [7]. However, a well-structured course of action is missing.
The standard SAE J3061 “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems” offers processes and methodologies for the vehicle cybersecurity that base on existing practices, and industry, government and conference papers. SAE J3061 contains an overall cybersecurity process framework that is divided into the concept phase and the phase production and operation. In this paper, the focus is on the concept phase. For the concept phase, SAE J3061 defines seven activities: feature definition, initiation of the cybersecurity lifecycle, threat analysis and risk assessment, cybersecurity concept, identify functional cybersecurity requirements, initial cybersecurity assessment, and concept phase review. In addition, SAE J3061 presents the HEAVENS security model and the EVITA methodology [8].

B. Security Risk Assessment Techniques

We propose to use the risk assessment technique from HEAVENS to evaluate threats. In this context, HEAVENS defines the terms: impact level, threat level and security level. The impact level consists of the parameters: safety, financial, operational, privacy and legislation. It describes the influence from a threat on an asset and is a measure of the damage potential referred to the asset. The threat level is a measure for the probability of a threat that is defined with the parameters: expertise, knowledge about the target of evaluation, window of opportunity and equipment. For both the impact level and the threat level, points for each parameter have to be set and added to a total number that is assigned to a specific level [9]. These levels are used to define the security level as described in Figure 1.



Security Level (SL)		Impact Level (IL)				
		0	1	2	3	4
Threat Level (TL)	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

Figure 1: security level table as defined in HEAVENS [8] [9]

Beside the HEAVENS risk-assessment there are further threat evaluation approaches as described in [10] or [11]. We chose HEAVENS because it is a well-prepared method with well-defined parameters that can be easily adapted to I4.0 and used in model-based tools.

Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks [12].

“In the EVITA approach to attack trees, a generic structure is proposed consisting of the following levels:
• Level 0: attack goal (analogous to the top event in a fault tree)

• Level 1: attack objectives

• Level 2: attack methods

• Level 3: (n - 1): intermediate goals / methods

• Level n: asset attacks (the base level methods of performing an attack; analogous to base events in a fault tree) [8]”.

STRIDE is an analysis methodology from Microsoft to find threats with the help of data flow diagrams during the design of IT applications. The name “STRIDE” of the methodology itself is an acronym for six types of threats that are used as guidewords to find and classify threats and stands for: Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege [13].

C. Steps toward a model based I4.0 development tool

In [14] we presented a model-based development tool called SysKit I4.0 development tool. The tool focuses on the design and analysis of I4.0 systems to enhance their security. In addition, we introduced in [14] a layer-based approach, with layers for different technical domains to address different aspects of the design process. An extract of this approach is depicted in Figure 2 and contains the layers, logical functional architecture, hardware, software and security assessments. On all layers, the model artefacts can be linked with each other. For this paper, the logical functional layer is particularly relevant. This layer can be used to describe the functionality of an I4.0 system independent from its hardware or software model and is used as a logical representation of the I4.0 system. The most important artefacts of this layer are logical functions, services, sensor, actuators and the connections between these artefacts.

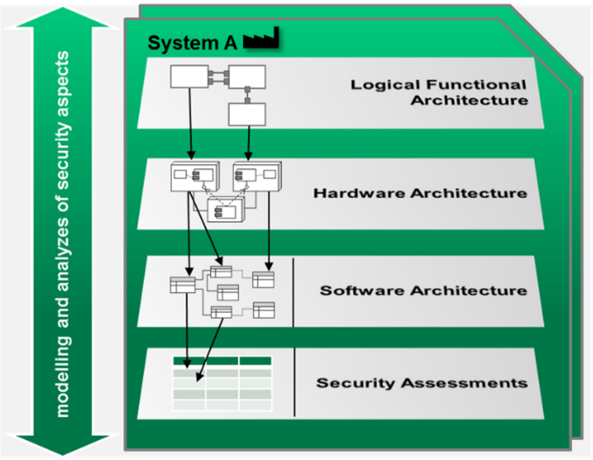

modelling and analyzes of security aspects
System A
Logical Functional Architecture
Hardware Architecture
Software Architecture
Security Assessments

Figure 2: Excerpt of the layer concept of the SysKit tool [14]

3. SECURITY DEFINITIONS

The standard ISO 27005 distinguish between primary and supporting assets. Primary assets are business processes and activities or information. The supporting assets encompass software, hardware, network, personnel, site and the organization structure. Supporting assets could have vulnerabilities that are exploitable by threats aiming to impair the primary assets [6].

To support the asset-analysis of the cybersecurity process, four asset categories are defined here: Enterprise, Plant, Information and I4.0 Implementation (cf. Figure 3). Assets belonging to the category Enterprise are business related assets like the reputation of the organization or their share in the market. The asset category "plant" is associated with recipes, procedures, parts of the plant, personnel or environmental aspects. The asset category "information" is associated with assets configurations, data and static information. The asset category "I4.0 implementation" is associated with assets like functions, hardware, software and communication. The supporting assets defined in ISO 27005 correspond to this category. Here the focus is on the I4.0 plant. Therefore, in the following the enterprise category is neglected.

Assets are closely linked with threats. A threat is any circumstance or event with the potential to adversely impact organizational operations or asset [15]. Therefore, a threat is associated in the model-based approach with one or many assets.

A vulnerability is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy [15]. Therefore, the vulnerabilities are associated here with the I4.0 implementation assets.

The risk is the expectation of loss expressed as the likelihood that a particular threat will exploit a particular vulnerability with a particular consequence [15]. In the proposed approach here, the risk is expressed through the security level.

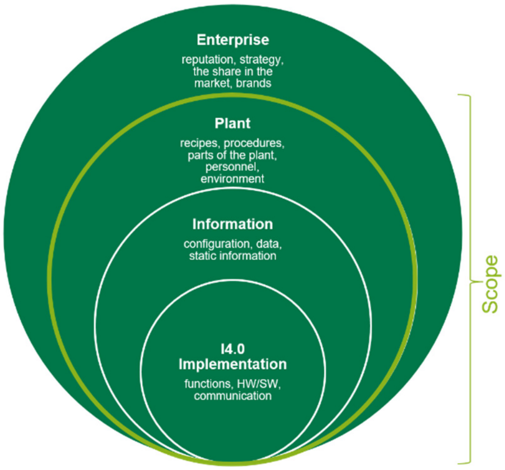

Enterprise
reputation, strategy, the share in the market, brands
Plant
recipes, procedures, parts of the plant, personnel, environment
Information
configuration, data, static information
I4.0 Implementation
functions, HW/SW, communication
Scope

Figure 3: asset categories for I4.0 plants

4. INTRODUCTION OF THE USE CASE

Here, the use case to explain the cybersecurity risk assessment process on an example is introduced. In Figure 4 the use case is depicted in an Unified Modeling Language (UML) use case diagram. The focus is on a mobile robot of an I4.0 smart factory that produces individual phone cases according to customer requirements. In this smart factory, the phone cases are produced on a production line. After production, the mobile robot carries the smart phone cases to a hand-work place, where the quality checks takes place. For this, the mobile robot receives orders from the Manufacturing Execution System (MES) and sends its status to the MES. In addition, the MES can receive the mobile robot sensor signals. To avoid collisions the mobile robot detect obstacles on its way to the both stations.

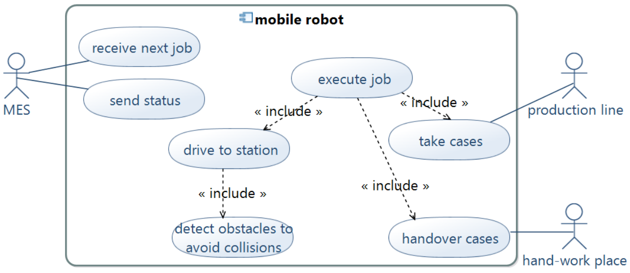


Figure 4: use case diagram of the I4.0 smart factory

5. THE I4.0 CYBERSECURITY PROCESS

Below the I4.0 cybersecurity risk assessment process is introduced (cf. Figure 5). The order of activities is numbered. The colored numbers are reentry points (step: one, three, seven). The process is reentered from step one if a new function is defined or a function changes. The process is reentered from step three if a new primary threat occurs and from step seven if a new attack scenario appears. New threats and attack scenarios are checked according to a security plan, which will not be discussed in this paper. The process is finishing in step ten if the residual risk is acceptable. The dashed lines shows where the steps have associations to results of former steps.

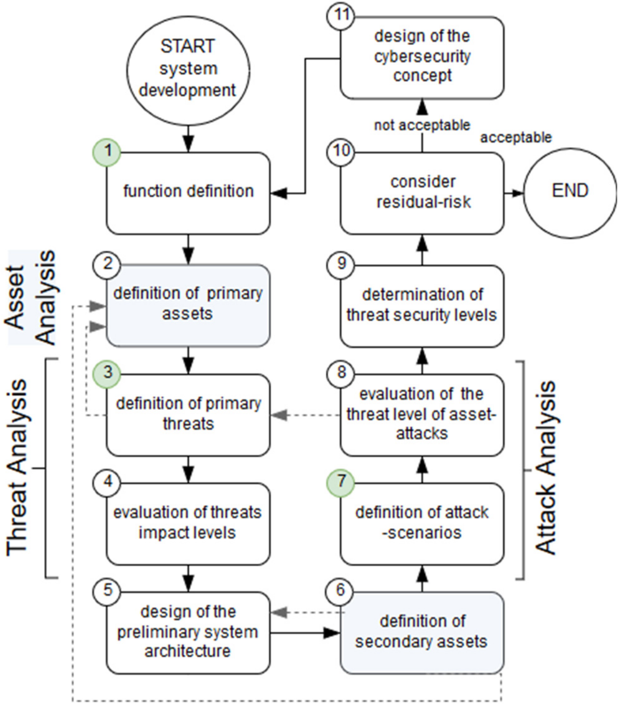

START system development
11
design of the cybersecurity concept
not acceptable
acceptable
1
function definition
10
consider residual-risk
END
Asset Analysis
2
definition of primary assets
9
determination of threat security levels
Threat Analysis
3
definition of primary threats
8
evaluation of the threat level of asset-attacks
Attack Analysis
4
evaluation of threats impact levels
7
definition of attack -scenarios
5
design of the preliminary system architecture
6
definition of secondary assets

Figure 5: the cybersecurity risk assessment process

STEP 1: The process follows the security by design approach by starting with the function definition of the I4.0 system or subsystem. This step refers to the functional requirement analysis. To this analysis belongs the use-case description (cf. Figure 4). To define the functionality in more detail the system architect can model the logical functional architecture as presented in Figure 6, to describe the dependencies between the inputs, functions, services and outputs. In the logical function architecture diagram white boxes describe the functions of the system. Grey boxes describe external dependencies to the environment and blue boxes describe services. This diagram belongs in addition to the preliminary architecture and is modeled with the SysKit I4.0 development tool.

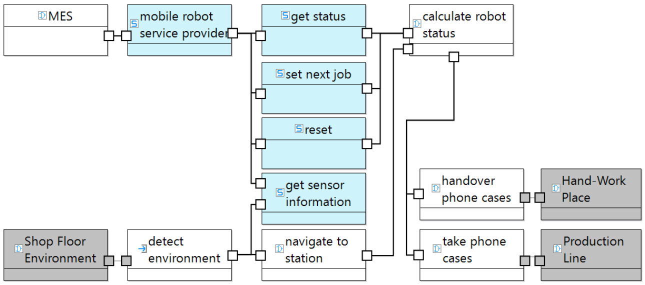


Figure 6: functional logical architecture of the I4.0 smart factory

STEP 2: In Step two, primary assets are defined that are associated with the asset category "plant" (cf. Figure 3).
Primary Assets can be grouped into the subcategories: recipes/processes/procedures, parts of the plant, personnel, personal data and environment. To define the primary assets, all information from the function definition should be regarded and all primary assets should be grouped into these subcategories.

For the defined use case, three primary assets where exemplarily defined as shown in Table 1.

Table 1: primary assets of the I4.0 smart factory

Asset Category	Primary Asset
processes	production process
parts of the plant	mobile robot
personal data	personal data at the hand-work place

STEP 3: In step three, primary threats are defined by means of the threat categories: steal, harm/damage/destroy, sabotage/block. These threat categories are combined with the primary assets to build primary threats. A rating which combination is important is shown in Table 2. Here the pluses means that this combination should be regarded. The "o" means that this combination is possible but likely less relevant or an implication in case of the category sabotage/block.

Table 2: combinations of threat categories and asset categories

Prim. Asset / Prim. Threat	Steal	Harm/Damage/Destroy	Sabotage/Block
Recipes/Processes/Procedures	+	o	+
Parts of the Plant	o	+	o
Personnel		+	o
Personal Data	+	o	o
Environment		+	

In the following, the meaning of the categories without completeness is discussed. The category "steal" can refer to industrial espionage to steal information about manufacturing processes. Tangible goods or parts of the plant could be stolen e.g. through hacked autonomous I4.0 mobile transport systems. Personal data like identities (e.g. usernames and passwords) with the belonging roles and rights can also be stolen.

Harm/Damaging/destroying can refer to parts of the plant. One well-known cyber-attack where parts of a plant were destroyed is the cyber-attack with a malicious computer worm called "Stuxnet" [16]. It is also possible that products are damaged during their factoring process through tampered production parameters or processes. Companies intellect property can be harmed e.g. if databases, documents and software are damaged or destroyed. The health and life of a plant's personnel and the environment can be harmed by a cyberattack when machines are manipulated and reach critical status.
Sabotage/blocking can refer to manufacturing processes and procedures. This could implicate to block or sabotage parts of the plant, the personnel or to block personal data.

With this methodology the primary threats for the I4.0 smart factory use case are defined in Table 3.

Table 3: Primary threats of the I4.0 smart factory

Threat Category	Primary Asset
Steal	production process
Steal	personal data (from hand-work place)
Harm/Damage/Destroy	mobile robot
Sabotage/Block	production process

STEP 4: In step four, the impact of a threat to an asset is defined with means of the parameters: safety, financial, operational, privacy and legislation from the HEAVEN methodology. The rating system is overtaken and adapted here to I4.0. For each parameter the values: no impact, low, medium, and high can be chosen. In Table 4 and Table 5 the impact level of the threats from the I4.0 smart factory use case are rated. In these tables the value in the brackets describes the rating of each parameter. The higher the sum of all the values of a threat, the higher the threat level. Explaining this parameters at this point and how to rate them would go beyond the scope of this paper. Therefore, just the parameters in this example that are not "no impact" are explained here. A sabotage of the production process regarding the mobile robot leads to a disruption of the production. This disruption can be easily compensated through additional work force. Therefore, the operational impact is medium. Here it is assumed that this leads to lower financial impact to the organization. The theft of the production process does not ruin the company but has a significant financial impact. Therefore, the value medium is chosen. The theft of the personal data via the mobile robot could affects here the hand-work place. It could be possible to get information who is working at the hand-work place. Here it is assumed that this has low impact to impersonate someone with further consequences.

Table 4: Rated threats of the I4.0 smart factory (part 1)

Parameter/Threat	Sabotage Production Process	Steal Production Process
Safety	no impact (0)	no impact
Financial	low (10)	medium (100)
Operational	medium (10)	no impact
Privacy and Legislation	no impact (0)	no impact
Impact Level	Medium (2)	High (3)

Table 5: Rated threats of the I4.0 smart factory (part 2)

Parameter/Threat	Steal Personal Data (from hand-work place)	Damage Mobile Robot
Safety	no impact (0)	low (10)
Financial	no impact (0)	no impact (0)
Operational	no impact (0)	medium (10)
Privacy and Legislation	low (1)	no impact
Impact Level	Low (1)	Medium (2)

STEP 5: In step five, the preliminary system architecture is defined on the logical functional design layer, the hardware layer, and the software layer under consideration of the communication (see Figure 2).

In the SysKit I4.0 development tool it is possible to model the information flow into the already existing logical function model (c.f. Figure 6) from step 1 and to create detailed logical function diagrams for each function block. Furthermore the hardware and network can be modeled on the hardware layer (c.f. Figure 2) and the logical functions can be assigned to the hardware.

In the I4.0 smart factory use case the robot uses super sonic sensors and a camera for the collision avoidance and orientation. In addition, a configuration to define route points and to set a speed limit of the mobile robot is available.

STEP 6: In step six; the secondary assets are defined that belong to the secondary asset category "information" of Figure 3. Therefore, the defined information of the preliminary logical functional architecture and communication architecture are grouped into the secondary asset subcategories: static information, data and configuration. Afterwards the secondary assets are assigned to the primary assets.

Table 6 shows an example with regard to the information about the use case that were defined in the previous step.

Table 6: Secondary assets of the I4.0 smart factory use case

Category	Secondary Asset	Primary Asset
static information	availableServices_mRobot	mobile robot
data	nextJob_MES	production process
	currentStatus_mRobot	mobile robot
		production process
	cameraStream_mRobot	mobile robot
		personal data (from hand-work place)
		production process
	superSonic_mRobot	mobile robot
configuration	maxSpeed_mRobot	mobile robot
	routepointSettings_mRobot	mobile robot
		production process

STEP 7: In step seven, attack scenarios are defined with means of attack trees. This covers also the vulnerability analysis for the system design. However, the vulnerability analysis for software and hardware can only take part after a selection of available soft- and hardware components e.g. a specific stored program control (SPC).

The categories of the secondary threats are reading, tampering, preventing/disturbing. At first, the threats with the highest impact level are selected for a more detailed analysis. For each selected primary threats the primary assets are selected. For each selection of the primary assets, all secondary assets that are associated with the primary assets are selected. To define the attack objectives in the attack tree, each secondary asset is used in combination with a category of the secondary threats.

In Table 7 the combination of primary threat categories and secondary threat categories to define secondary threats is presented. The pluses describes the most common combinations that should be at least regarded.

Table 7: Correlation between primary threat categories and secondary threat categories

Prim. Threat Cat. / Sec. Threat Cat.	Read	Tamper	Prevent/Disturb
Steal	+	o	o
Harm/Damage/Destroy	o	+	+
Sabotage/Block	o	+	+

In the use case the threat "steal production process" is investigated more in detail, because it has the highest impact level. The primary asset here is the production process. The secondary assets that belongs to the production process are:

- nextJob_MES
- currentStatus_mRobot
- cameraStream_mRobot
- routpointSettings_mRobot.

Because the primary threat category is "steal" at least the secondary threat category "read" has to be regarded. Therefore, for each secondary asset an attack objective with the secondary threat category "read" is created for the I4.0 smart factory use case as presented in the attack-tree in Figure 7.

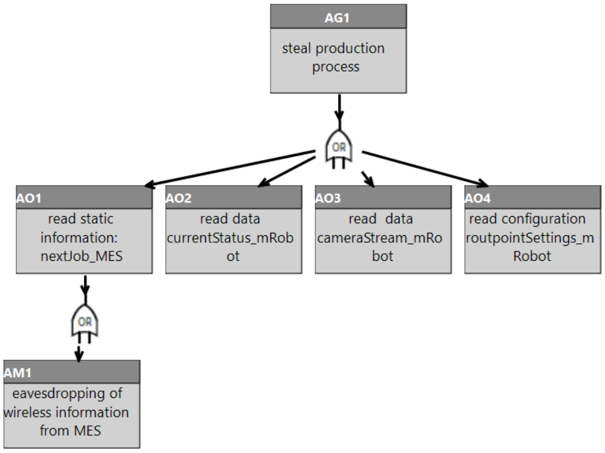

AG1
steal production process
OR
AO1
read static information: nextJob_MES
AO2
read data currentStatus_mRobot
AO3
read data cameraStream_mRobot
AO4
read configuration routpointSettings_mRobot
OR
AM1
eavesdropping of wireless information from MES

Figure 7: Exemplary attack tree of the I4.0 smart factory

The attack trees are defined according to the EVITA methodology described in SAE J3061. In Figure 7 an example of such an attack-tree is shown that refers to the I4.0 smart factory use case. This attack tree is incomplete and serves only to demonstrate the principle. There are different levels. Each level is connected via a logical "AND" or "OR". "AND" means that all child nodes need to be fulfilled to reach the parent node. "OR" means only one child node has to be fulfilled to reach the parent node. The top level contains an attack-goal that correspond to a primary threat. The next level below describes the attack-objectives in the EVITA methodology. Here the secondary threats describe the threats that are used on the information level. The next level below the attack objectives contains in the EVITA methodology the attack-methods. Here the possible attack surface in the system model should be regarded. The possible attack surface can be identified by analyzing the information flow to detect all paths where the information is available. It is possible to describe an attack method with another attack method more in detail. In Figure 7 only one attack method is exemplarily shown. The assets attacks describes how an attack could be performed and describe the necessary preconditions. To find asset attacks a detail knowledge about the used hard- and software and communication protocols is necessary.

STEP 8: In step eight, the threat levels for the attack tree leafs, are defined with means of the adapted HEAVENS methodology. Thereby, the highest threat level is propagated up to the tree root and assigned to the primary threat.
In the I4.0 smart factory use case it is assumed that the data from and to the MES are transmitted unencrypted via WLAN. It is assumed that the access to the WLAN is protected. This leads to a high window of opportunity. Furthermore, it is assumed that the manufacturer of the MES and the robot system offers manuals with detailed information about both systems. This leads to a public knowledge about the TOE. WLAN is a very common communication technology where standard equipment is available. More information how to define the threat level is given in [9].

Table 8: Example, threat level of the attack method AM1

Expertise	Knowledge about TOE	Equipment	Window of Opportunity	Threat Level
laymen (0)	public (0)	standard (0)	high (1)	critical (4)

STEP 9: In step nine, the security level of the primary threats is defined with means of the HEAVENS methodology (cf. Figure 1). In the I4.0 smart factory use case leads the high impact level (cf. Table 4) and the critical threat level (cf. Table 8) to a high security level.

STEP 10: In step ten, the overall risk is regarded. The overall risk is the highest risk of all threats. If the overall risk is above a defined threshold, a cybersecurity concept has to be developed for all threats above this threshold. If the overall risk is below a defined threshold, the process ends but can be resumed as described above.
For the threat steal production process of the I4.0 smart factory use case a cybersecurity process has to be developed, because a high security level is not acceptable in each case.

STEP 11: Finally, in step eleven, the cybersecurity concept is defined based on the prioritized threats as defined in step ten. The cybersecurity concept can lead to new functionalities for the security mechanism. The concept for the cybersecurity concept is out of scope of this paper.

6. CONCLUSION AND FUTURE WORK

In this paper, a first approach for an Industry 4.0 (I4.0) cybersecurity risk assessment process with a structured course of actions for the early design phase of an I4.0 plant is presented. Therefore, it is shown how selected and adapted methodologies could work together to define the necessary artefacts for the cybersecurity risk evaluation. First approaches how to support the cybersecurity assessment process on different model layers with means of the discussed layer approach in [14] are introduced. It is outlined how this process could be integrated into a model-based I4.0 development tool. With this approach, it is possible to combine the risk assessment with the architectural design, thereby enabling security by design. The proposed process and the selected methodologies offers potential for further work and evaluations. It is planned to investigate further methodologies to support the presented process particular to support the cybersecurity concept. In addition, a detailed evaluation of the proposed methodologies and implementation into the SysKit I4.0 development tool is ongoing within the project SysKit_HW supported by the German Federal Ministry of Education and Research (BMBF).

ACKNOWLEDGMENT
This work was supported by the German Federal Ministry of Education and Research (BMBF) with funding number 16KIS0662.

REFERENCES

[1] R. Heidel, M. Hofmeister, M. Hankel und U. Döbrich, Industrie 4.0 - Basiswissen RAMI4.0, Berlin, Wien, Zürich: Beuth Verlag GmbH, VDE Verlag GmbH, 2017.

[2] German Federal Ministry for Economic Affairs and Energy, "plattform-i40," 21 Januar 2019. [Online]. Available: https://www.plattform-i40.de/I40/Navigation/EN/Industrie40/.

[3] Cyber Security Agency of Singapore, "www.csa.gov.sg," 09 November 2017. [Online]. Available: https://www.csa.gov.sg/~/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf.

[4] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Indianapolis: Wiley Publishing, 2008.

[5] *DIN EN ISO/IEC 27001:2017-03, Information technology – Security techniques – Information security management systems – Requirements.*

[6] *ISO/IEC 27005:2011-06, Information technolog - Security techniques - Information security risk management.*

[7] National Institue of Standards and Technology, "NIST Cybersecurity Framework," September 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf. [Accessed 1 6 2019].

[8] *SAE International: J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,* (1 2016).

[9] A. Lautenbach and M. Islam, "HEAVENS Deliverable D2 - Security models," 18 März 2016. [Online]. Available: http://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf.

[10] G. Macher, H. Sporer, R. Berlach, E. Armengaud and C. Kreiner, "SAHARA: A Securtiy-Aware Hazard and Risk Analysis Method," *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE),* pp. 621-624, 2015.

[11] A. Y. Javaid, W. Sun, V. K. Devabhaktuni and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," *2012 IEEE Conference on Technologies for Homeland Security (HST),* pp. 585-590, 2012.

[12] B. Schneier, „Attack Trees: Modeling Security Threats," *Dr. Dobb's Journal,* pp. 21-29, 12 December 1999.

[13] M. Howard und S. Lipner, The Security Development Lifecycle – SDL: A Process for Developing Demonstrably More Secure Software, Redmond: Microsoft Press, 2006.

[14] V. P. Betancourt, T. Glock, M. Kern, E. Sax and J. Becker, "Model-based development tool for the design and analysis of secure industry 4.0 systems," VDI-Verlag, Baden Baden, 2018.

[15] DIN EN 62443-3-2:2018-10, *Security for industrial automation and control systems - Part 3-2: Security risk assessment and system design,* 2018.

[16] Y. Wang, D. Gu, S. Chen und H. Yang, „Stuxnet Vulnerabilities Analysis of SCADA Systems," *NCIS 2012: Network Computing and Information Security,* pp. 640-646, 2012.