Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Increased IT security by model-based vulnerability analysis of IT/I&C systems and proof of ISO conformity

Mathias Lange, Yongjian Ding*
Martin, Szemkus**

** University of Applied Sciences Magdeburg-Stendal, Magdeburg, CO 39114 Germany (e-mail: {mathias.lange; yongjian.ding}@ h2.de).*
***ICSS GmbH, Magdeburg, Germany (e-mail: martin.szemkus@icss.de)*

Abstract: This paper shows the extension of an entity model developed in cooperation with project partners by an "Organizational Entity" in order to detect potential weaknesses in IT security as well as to prove the standard conformity (IT security level according to IEC 62443) of the examined systems. This allows suitable security measures to be taken systematically and IT security to be optimized in the overall system. The first application of this progressive approach on a subsystem, the distillation, of the model factory ET of the University of Applied Sciences Magdeburg-Stendal is promising.

Keywords: Industry 4.0, automation, cyberattacks, IT-security, entity model

1. INTRODUCTION

Industry 4.0 aims at the optimization of all processes of a value chain. According to Platform Industry 4.0, this will be possible through "intelligent networking of machines and processes in industry using information and communication technology" (BMWi, 2018). Modern production plants are characterized by greater transparency of information, better technical assistance and decentralized control structures. From the point of view of automation, this means that the classic, hierarchically structured automation pyramid is abandoned. This resolution of the structure begins at the field level and continues through various automation stations to the control room.

This networking can extend to the office world. If not, it can even extend to the Internet, if we look at the ever-increasing "cloud applications". This will lead to "total networking" of the vertical and horizontal levels, resulting in increasingly complex communication structures. Under these conditions, cyber-physical systems (CPS) or cyber-physical production systems (CPPS) can enable intelligent, autonomous, flexible and optimized production processes (Andelfinger & Hänisch, 2017), (Hausegger, et al., 2016), (Roth, 2016), (Scheer, 2013), (VDI, April 2013). Due to this complete networking of facilities and the associated digitalization of the value chain, the complexity of communication structures increases and the vulnerability to cyberattacks increases [(Fischer, et al., 2016), (Szemkus, et al., 2017), (Flatt, et al., 2016), (Hänisch & Rogge, 2017)], new potential "gateways" emerge. Therefore, systematic and flexible approaches are required to model the IT security aspects, especially in automation networks.

1.1 Examples of cyberattacks in industrial environments

There is already a risk of becoming the victim of such an attack in classically structured production facilities. The BSI report for 2018 (BSI, 2018) showed that hacking and DoS attacks account for 37% and malware attacks for 57% of current security incidents.

In a German steel plant, whose blast furnace control was taken over and manipulated, considerable damage occurred, which led to massive damage to the blast furnace. (BSI, 2014). Another example from another industry sector shows a Denial of Service (DoS) attack on a Canadian food producer. The result was a loss of production lasting several weeks, including the replacement of all affected pipelines (Ries, 2015). The topicality of the topic is reflected in the cyberattack on Krauss-Maffei in November 2018. After a Trojan was smuggled in, the company's production capacity was restricted for 2 weeks because most of the systems had failed at one location (Bünte, 2018).

These examples demonstrate that cyberattacks are already a topical issue today. For this reason, networks and systems must be able to provide basic protection against external and internal cyberattacks, both in traditional production plants and from an industrial 4.0 point of view, in order to ensure trouble-free operation [(Fischer, et al., 2016), (Szemkus, et al., 2017), (Fischer, et al., 2016), (Eckert & Fallenbeck, 2015)]. This not only requires compliance with current standards, but also the development and adaptation of new concepts and tools for maintaining IT security (Eckert, 2014), because "new challenges arise in the area of IT security and in systematic implementation" (Lass & Kotarski, 2014). This should give the operator the opportunity to take preventive measures through comprehensive vulnerability analyses, to detect cyberattacks in good time if necessary and to react effectively.

2. INTRODUCTION TO THE ENTITY MODEL

2.1 The basic structure

The project partners, the Magdeburg-Stendal University of Applied Sciences and Otto von Guericke University, developed a modeling concept for the clear mapping of complex industrial infrastructures (Fischer, et al., 2016) as part of the "Smartest" joint project funded by the BMWi (funding code 1501502A-D). This is based on theories of the Entity Relationship Model (Chen, 1976) from computer science.

According to (Spath, et al., 2013), a basic idea of industry 4.0 is to network information technology and communication technology to an Internet of things, services and data across the board. As a result, communication structures in highly complex IT landscapes are becoming increasingly complex (Kagermann, et al., 2013). A modular concept is suitable for efficiently uncovering weak points in such environments, because the level of detail of the investigation can be adapted to the relevant information level for the security investigation [(Szemkus, et al., 2017), (Fischer, et al., 2016), (Ding, et al., 2018)].

This component-based modelling begins with the determination of the starting point of a system to be investigated. This is referred to as the "Root-Entity", see Figure 1.

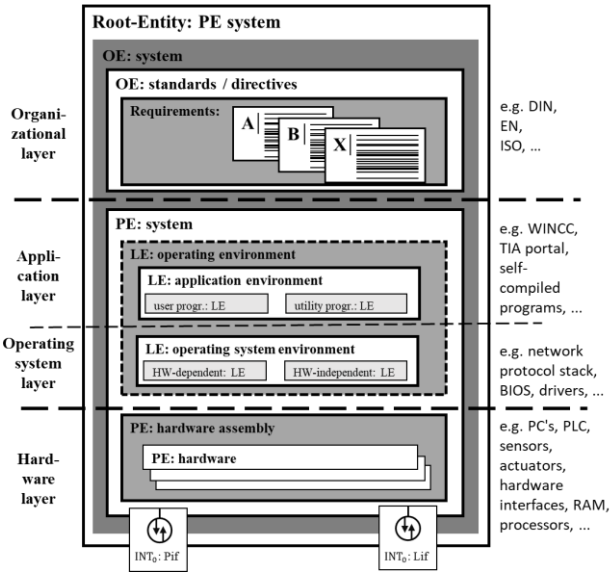

Fig. 1: Structure of the entity model with the analysis layers

The next step is an analysis of all components that are located within the system to be investigated, can be reached via communication channels, offer interfaces for the exchange of information or process information. The analysis then passes through various system layers. The determined components are divided into physical (PE) and logical entities (LE).

The analysis starts in the hardware layer. All information about the hardware components, such as PLC, HMI, etc., including interfaces, is recorded and stored in the "PE hardware compilation".

Depending on the level of detail of the system analysis, it is possible to differentiate whether individual components are recorded reduced as a "black box" or with a high level of detail, e.g. down to the processor model. For a more efficient security investigation, irrelevant information can be hidden.

In the next step, the components of the “LE: operating environment" are analyzed. With the operating system layer and application layer, this comprises two further system layers. From these the “LE: application environment" and “LE: operating system environment" originate.

The "LE: Operating System Environment" considers hardware-dependent as well as hardware-independent software, such as information from drivers, BIOS or firmware. The “LE: application environment" is examined in the last analysis step. User programs and utility programs that work in this layer are identified, such as WINCC, TIA, self-compiled programs and others.

2.2 The Organizational Entity

Up to this point it is a pure component-based system analysis using the entity model according to [(Fischer, et al., 2016), (Ding, et al., 2018)]. However, up to this point in the analysis there is no possibility to prove that the investigated system also conforms to the standards. For this purpose, the “*Organizational Entity*” (OE) was introduced. As shown in Figure 1, the “PE system" is enclosed by a superordinate module called "OE: system". In the OE: system is the module OE: standards/ directives in which the security requirements (SR) are defined. Depending on the definition of the “Root-Entity”, these apply either to a complete system or to a section of a system that is to be examined. The security requirements derive from applicable standards or are guidelines from organizational processes. In the “Root-Entity”, all security requirements that are to be observed within the system are stored in a database. Before defining the security requirements for a system, an individual risk assessment of the system to be examined is carried out. On the basis of this risk assessment, the levels of the security level (SL-T) to be achieved for the respective security requirements are defined. Thus, it can occur that different sections of a system to be examined may have different security requirements, but also different levels of security levels with the same security requirements. A future analysis tool based on this modeling concept should primarily show security requirements that represent a violation of the desired security requirement. The remaining security requirements should be able to be optionally shown if required, for example to control, change or extend existing or supplement new security requirements. Subsystems within the root entities represent at least a subset of the security requirements defined in the root entities.

This enables a comparison to be made between the security requirements to be achieved (SL-T) and the security levels currently achieved (SL-A). The existing need for action is

visualized to the user and measures can be initiated to eliminate the detected weak points in the examined system.

2.3 Implementation of SR's in the OE using the example of IEC 62443

The focus in Figure 2 is designed to explain the content structure of the Organizational Entity, "OE: System" module, including the implementation of security requirements with exemplary reference to a part of the IEC 62443 (IEC, 2012) series of standards.

This series of standards was selected as an example of security requirements in the OE because the security requirements defined in it apply to a broad interest group of industry (equipment and machine manufacturers, system integrators and plant operators). It thus stands for a holistic approach to security measures, considering the different roles of the users of this series of standards. In addition, the protective measures described in it can be implemented in various network levels and systems (Koschnick, 2017) and it is based on the "Defense-in-depth" strategy (Jiang, et al., 2018), an approach for the coordinated use of several security measures to protect data stocks.

This enables a comparison to be made between the security requirements to be targeted (SL-T) and the security levels currently achieved (SL-A). The existing need for action is visualized to the user and measures can be taken to eliminate the detected vulnerabilities in the examined system.

The selected part from the series of standards is IEC 62443-3-3 (IEC, 2015). For a better orientation for the future user the OE is called "OE: Standard IEC 62443-3-3". This OE contains a complete database with the SR's that are to apply to the system. They are abbreviated as "SR" in accordance with the standards. The identifier "y.z" in the column "SR" represents the coding of the SR according to the standard. The 3 following columns contain the different security levels (SL) according to IEC 62443-3-3. Column A contains the achieved security level, column C the capability security level and column T the target security level. The SL levels range from SL 0 to SL 4. The SL 0 corresponds to a system that does not require any special SR. As a rule, this is a partial component that is already protected by other components.

The SL 4 is intended to "provide protection against an intentional infringement" which is carried out with "sophisticated means", considerable effort, automation skills and high motivation. Attacks with sophisticated means and considerable resources are understood to mean, for example, the use of computing clusters to execute Brutforce attacks for password theft, but the attack of syndicates that have sufficient motivation and time to analyze systems and program and deploy zero-day exploits. When a system is configured with a level 4 SL, it is protected against internal and external attacks for a finite period of time. Further details on the individual SR's and SL levels can be found in the standard (IEC, 2015).

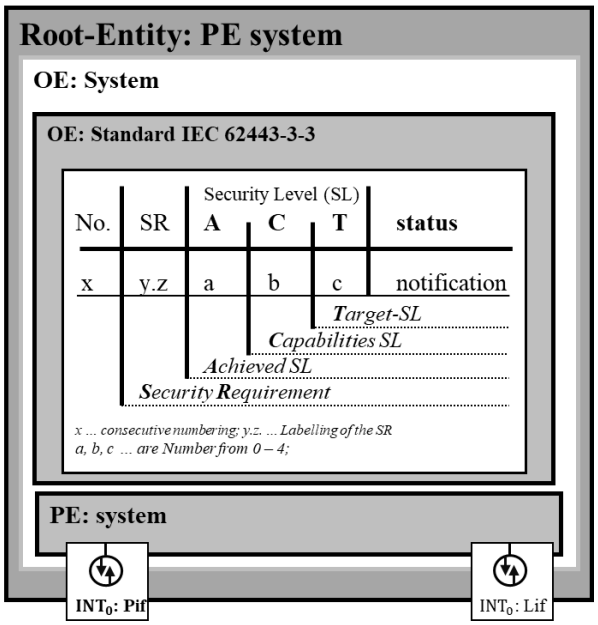

Fig. 2: Representation of the Organizational Entity with security requirements in accordance with IEC 62443-3-3

The last column Status indicates whether the SL's of the SR are fulfilled by the examined system. 3 different notifications are output. The output is "warning" if the SL-C does not fulfill the conditions of the SL-T, "injury" if the SL-A does not fulfill the SL-C, but the SL-C can fulfill the specification of the SL-T and "OK" if there are no incidents. For the visualization of errors resulting from deviations of the security levels, a color coding, for example according to a traffic light principle, can also be carried out in order to visually better differentiate the states.

3. EXEMPLARY APPLICATION TO THE MODEL FACTORY

The following section shows the conceptual application of a component-based modeling using entity model to a complex industrial environment. For this application a part of the model factory ET of the university Magdeburg-Stendal served as reference object. This model represents the production process of a complete filling plant with different production stages. The further illustrations in the case studies refer to the section "Distillation".

In the following, the focus is on the conceptual application of the previously presented OE: System. For this reason, neither the risk analysis of the plant nor the system analysis of the individual components will be dealt with here.

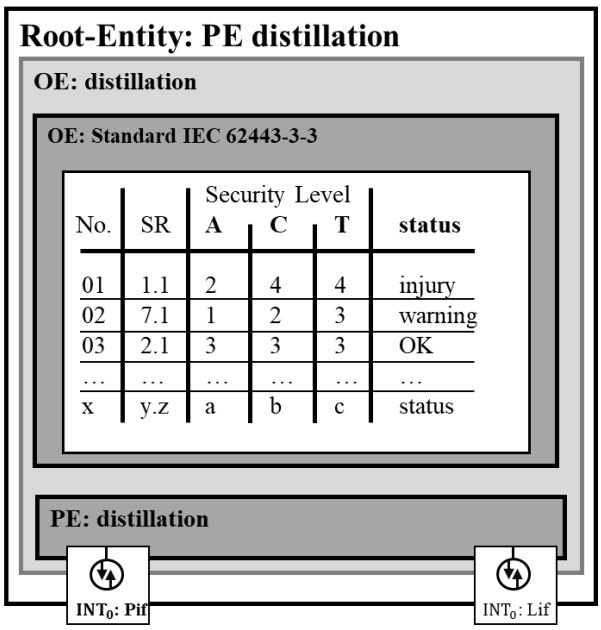

Fig.3: OE with exemplary SR´s

For the OE: distillation, Figure 3, 3 SR's were defined. The process control of the distillation is done by the controller ET200SP from Siemens with a PLC of the series S7-1515SP PC (F). This PLC offers the possibility to connect a monitor via the DVI port in order to use it as Human Machine Interface (HMI). Operation is to be carried out either via mouse and keyboard, which are connected via USB port, or via remote access.

In the 1st line of Figure 3 the SR 1.1 was defined with an SL-T: 4. The SR 1.1 regulates the identification and authentication of human users. The security analysis revealed the status "injury". If you click on the status, it is planned to get detailed information. In this case the message refers to the HMI, because the security level SL-T: 4, which requires a "multi-factor authentication over all networks", is currently not achieved by the HMI with an SL-A: 2. Since the operator can directly influence the critical "distillation" process via the HMI, an SL-T: 4 is required according to the risk analysis.

However, the achievable security level (SL-C: 4) indicates that the existing hardware basically contains the functionality required to meet the SL-T target. This means that with this deviation of the SL levels one is able to fulfill the criteria of the SL-T by changing the existing hardware. This would have detected a weak point due to a misconfiguration of the HMI, which would have represented a violation of the security requirement.

The situation is different in the second case study. In critical processes, but also in industrial plants in general, one should keep control over the controller. SR 7.1 regulates protection during DoS events. After the risk analysis of the plant, it was demanded that in the event of a DoS attack, the effects on other systems and networks could be limited and the network load controlled (SL-T: 3). The hardware analysis revealed that the network technology used does not offer these features (SL-C: 2). At this point an investment in new hardware has to be made.

In the 3rd line the SR 2.1 "enforcement of authorization" was defined. During the system analysis there were no deviations between the achieved, achievable and achievable SL. Thus it receives the status "OK".

4. CONCLUSIONS

With the help of the entity model, the analysis of IT/I&C systems provides a complete overview of the current status of the investigated system. By a systematic comparison with the target state we can uncover potential weak points in the system. By supplementing the Organizational Entities, it is also possible to prove conformity with the applicable IT security standards, e.g. IEC 62443. The application to the "distillation" subsystem of the model factory ET illustrates the advantage of this systematic concept.

The objective is to model the entire system automatically and tool-supported in future and to compare the system data with existing exploit databases, such as the CVE databases (CVE, 2019), which provide information on known weak points, in order to identify weak points in the system and to increase IT security through suitable measures.

REFERENCES

Andelfinger, V. P. & Hänisch, T., (2017). *Industrie 4.0 - Wie cyber-physiche Systeme die Arbeitswelt verändern*, p. 1-271 .Springer Verlag, Wiesbaden.

BMWi, (2018). *https://www.plattform-i40.de/*. [Online] Available at: https://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html, [Date: October 1st 2018].

BSI, (2014). *BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk*. [Online] Available at: https://www.heise.de/security/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html [Date November 5th 2018].

BSI, (2018). *Die Lage der IT-Sicherheit in Deutschland 2018*, s.l.: Bundesamt für Sicherheit in der Informationstechnik (BSI).

Bünte, O., (2018). *Cyberangriff: KraussMaffei von Hackern erpresst.* [Online] Available at: https://www.heise.de/newsticker/meldung/Cyberangriff-KraussMaffei-von-Hackern-erpresst-4244880.html [Date: Dezember 7th 2018].

Chen, P. P.-S., (1976). *The entity-relationship model — toward a unified view of data*, New York (USA): ACM Trans. Database Syst., DOI=http://dx.doi.org/10.1145/320434.320440.

CVE, (2019). *CVE - Common Vulnerabilities and Exposures*. [Online] Available at: https://cve.mitre.org/

Ding, Y. et al., (2018). *Model-based vulnerability analysis of Complex infrastuctures*, Berlin: Preceeding of 49th Annual Meeting on Nuclear Technology 2018 (AMNT), (May, 29.-30.).

Eckert, C., (2014). *IT-Sicherheit und Industrie 4.0 – Vernetzung, Big Data und Cloud*. Fachzeitschrift für

Innovation, Organisation und Management, Special, 01, p. 40–45..

Eckert, C. & Fallenbeck, N., (2015). *Industrie 4.0 meets IT-Sicherheit: eine Herausforderung!*. Berlin: Springer-Verlag Berlin-Heidelberg, Informatik Spektrum 2015, Vol. 38, S. 217-223, https://doi.org/10.1007/s00287-015-0875-z.

Fischer, R., Clausing, R., Dittmann, J. & Ding, Y., (2016). *Industrie 4.0 Schwachstellen: Basisangriffe und Szenarien*, Klagenfurth/Österreich: Tagungsband - DACH Security.

Fischer, R., Clausing, R., Dittmann, J. & Ding, Y., (2016). *Your Industrial Facility and Its IP Address - A First Approach for Cyber-Physical Attack Modeling*. International Conference on Computer Safety, Reliability and Security. In: Proceeding. Springer International Publishing Cham: Springer Verlag, pp. 201-212.

Flatt, H. et al., (2016). *Analyse der Cyber-Sicherheit von Industrie 4.0-Technologien auf Basis des RAMI 4.0 und Identifikation von Lösungsbedarfen*, Automation 2016 - "Secure & reliable in the digital world" : 17. Branchentreff der Mess- und Automatisierungstechnik, 07. -08. Juni 2016,S. 103-104, Baden-Baden: Düsseldorf: VDI Verlag, 2016 (VDI-Berichte 2284).

Hänisch, T. & Rogge, S., (2017). *IT-Sicherheit in der Industrie 4.0. In Industrie 4.0: Wie cyber-physische Systeme die Arbeitswelt verändern*, V P Andelfinger, and T Hänisch (eds.), pp. 91–98.. Wiesbaden: Springer .

Hausegger, T., Scharinger, C., Sicher, J. & Weber, F., (2016). *Qualifizierungsmaßnahmen im Zusammenhang mit der Industrie 4.0*, Wien: prospect Unternehmensberatung GmbH.

IEC, (2012). *IEC-62443-1-1 (ISA99.01.01): Security for industrial automation and control systems*. Terminology, Concepts and Models, Draft 1, Edit 7, August 2012.

IEC, (2015). *E DIN IEC 62443-3-3 VDE 0802-3-3:2015-06: Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level.* 2015. VDE: www.vde-verlag.de.

Jiang, N., Lin, H., Y. Z. & Zheng, L., (2018). *Performance Research on Industrial Demilitarized Zone in Defense-in-Depth Architecture*, Wuyishan, China: 2018 IEEE International Conference on Information and Automation (ICIA), pp. 534-537.

Kagermann, H., Wahlster, W. & Helbig, J., (2013). *Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 –Abschlussbericht des Arbeitskreises Industrie 4.0*, s.l.: Forschungsunion im Stifterverband für die Deutsche Wissenschaft.

Koschnick, G., (2017). *Orientierungsleitfaden für Hersteller zur IEC 62443*, Frankfurt am Main: ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V., Fachverband Automation.

Lass, S. & Kotarski, D., (2014). *IT-Sicherheit als besondere Herausforderung von Industrie 4.0*, Schriftenreihe der Hochschulgruppe für Arbeits-und Betriebsorganisation eV (HAB): Industrie (2014): S.397-419, Berlin: GIto: s.n.

Ries, U., (2015). *Cyberattacke in der Keksfabrik*. [Online] Available at: http://www.spiegel.de/netzwelt/web/erpressung-durch-cyberattacken-angriffsziel-industrieanlage-a-1048034.html, [Date: November 10th 2018].

Roth, A., (2016). *Industrie 4.0 – Hype oder Revolution?* In: Roth A. (eds) Einführung und Umsetzung von Industrie 4.0, Wiesbaden: Springer Verlag.

Scheer, A.-W., (2013). *Industrie 4.0 – Wie sehen Produktionsprozesse im Jahr 2020 aus?*. [Online] Available at: https://www.researchgate.net/profile/August_Wilhelm_Scheer/publication/277717764_Industrie_40_-_Wie_sehen_Produktionsprozesse_im_Jahr_2020_aus/links/55ee9e5608ae0af8ee1a1d72/Industrie-40-Wie-sehen-Produktionsprozesse-im-Jahr-2020-aus.pdf [Date: Oktober 1st 2018].

Spath, D. et al., (2013). *Produktions-arbeit der Zukunft – Industrie 4.0*, Stuttgart: Fraunhofer.

Szemkus, M., Lange, M. & Ding, Y., (2017). *IT-Security-Untersuchung an einer Modellfabrik unter Berücksichtigung der Industrie 4.0-Anforderungen*, Magdeburg: Tagungsband - Kommunikation in der Automation 2017 (KommA), (November, 14.-15.).

VDI, (2013). *Thesen und Handlungsfelder - Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation*, Düsseldorf: VDI.