INTERNATIONAL DESIGN CONFERENCE – DESIGN 2022
https://doi.org/10.1017/pds.2022.201

Cyber-Security Aware Design of Automated Systems

R. Stetter [1,✉], M. Witczak [2] and M. Till [1]

[1] University of Applied Sciences Ravensburg-Weingarten, Germany, [2] University of Zielona Góra, Poland
✉ ralf.stetter@hs-weingarten.de

Abstract

One of the main current threats for producing companies is the possibility of cyber-space attacks. Due to several reasons, industrial companies need to connect their plants over some kind of networks. Obviously, today many approaches from information technology (IT) exist which will greatly reduce the danger of attacks. Still, no producing company can completely rely on these IT solutions. This paper proposes a systemic approach to design processes and products for increased cyber security. This approach is based on an attack model and is explained based on an automated storage system.

Keywords: mechatronics, cyber-physical systems, industry 4.0, systems design

1. Introduction

In the last decades, numerous cyber-attacks concerning technical systems were reported. One famous example is the malicious computer worm Stuxnet which attacked supervisory control and data acquisition (SCADA) systems using Siemens Step 7 software. Today, producing companies fear cyber-attacks because in the scope of Industry 4.0 large quantities of measurement and control data need to be transmitted. Production systems need to be engineered in such a way that they can be continuously monitored, coordinated and controlled; the use of communication networks and heterogeneous IT components makes the resulting cyber-physical systems vulnerable to the threat of cyber-physical attacks (Teixeira et al. 2015). Obviously, the companies are aware of this threat and the IT departments have implemented several measures and concepts to counteract cyber-space attacks, such as dedicated networks, virtual private networks (VPN), frequently in combination the Industrial Internet of Things (IIoT), as well as different kinds of encryption technology. The main research literature is focusing on the three main properties of data and IT services, namely confidentiality, integrity and availability (Teixeira et al. 2015; Whitman and Mattord 2022); an enormous body of knowledge was created and is already implemented in production companies. However, the current experience shows that also the attackers will develop more and more powerful attacks and that no producing company can completely rely on these IT solutions. In the second half of 2020 194 attacks on production companies were reported (Johansson 2021); it is probable that some of these attacks will bypass the IT counteraction systems. Obviously, the consequences on the automated systems should be as small as possible. This paper proposes a systemic approach to design processes and products for increased cyber security, i.e. to reduce or eliminate the consequences of cyber-attacks. It has to be pointed out that this research is still in an exploratory stage - this paper is intended to foster discussions in the design research society. The underlying research question can be formulated as follows:

How can products and process be designed in a systematic manner in order to decrease the chance that a cyber-space attack will endanger human beings, resources or the environment?

Current research in this area is concerned with establishing an architectural system engineering methodology (Bayuk & Horowitz 2011), the recognition of modelling errors in supervisory controller design (Goorden et al. 2019) and robust design for cyber-physical systems (Vogel et al. 2018). The role of cyber-security for small and medium sized enterprises (SMEs) is also discussed (Wichmann et al. 2019). As the presented research is closely connected to Industry 4.0, also research activities concerning design for industry 4.0 (e.g. Kadir et al. 2019) play an important role.
The understanding of cyber-security in this paper is the absence of short-time and long-time negative consequences from cyber-attacks on the respective company, on human beings within or outside the organisation and on the environment. Concerning long-time consequences of cyber-attacks, also the theft of intellectual property lies within this definition.
The structure of this paper is as follows. The necessity of communication in current industrial companies is highlighted in Section 2. Networked control system security has to consider threats at both the cyber and physical environment and it is of the utmost importance in the study of cyber-attacks on control systems to capture the adversary's resources and knowledge (Teixeira et al. 2015); consequently, this aspect of external attacks is the focus of Section 3. Section 4 summarizes measures to eliminate or reduce the consequences of these external attacks. The scientific results presented in in this paper are further explained using the example of a logistics system in a high-rise warehouse with automated guided vehicles (AGVs); this is contained in Section 5. The paper is concluded in Section 6 with a summary and outlook.

2. Necessity of communication - Industry 4.0

In the scope of cyber-security, one may ask, why is it not possible to waive any external data connections of a manufacturing or assembly system and, by doing so, to totally avoid any external attacks. The answer is closely connected to the well-known trend towards industry 4.0. Industry 4.0 …

- … includes a range of concepts in automation, digitalization and networking,
- … relies on the integration of dynamic value-creation networks,
- … integrates the physical systems and control systems within a company over buildings and production locations (even internationally) and
- … integrates the physical systems and control systems with other branches and economic sectors and with other industries and industry types.

The different elements of industry 4.0 can be described using an Architectural Model (Figure 1).

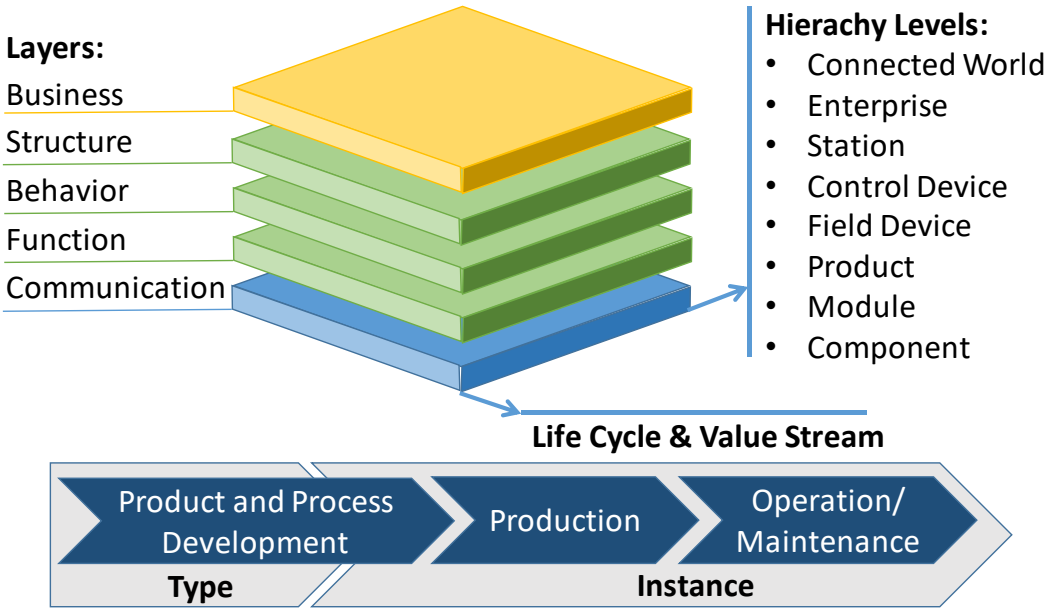

Figure 1. Architectural Model of Industry 4.0

https://doi.org/10.1017/pds.2022.201 Published online by Cambridge University Press

The shown model is based on a well-known model which is intended to describe all crucial aspects of Industry 4.0 - the Reference Architectural Model Industry 4.0 (RAMI 4.0), which is proposed by the German Electrical and Electronic Manufacturers' Association. The layers in this model (listed on the left side - vertical axis) describe the decomposition of a technical system into layers which allow a certain views of the system; these views contain the well-known function-behaviour-structure ontology (Gero and Kannengiesser 2014) but also include a business layer and a communication layer which originate from information and communication technology. The hierarchy levels (listed in the right side - right horizontal axis) correspond partly to IEC 62264 but are extended in order to include information concerning the product structure. The life cycle and value stream processes are visible in the front of Figure 1 (left horizontal axis) and are based on IEC 62890, but are adapted to allow the inclusion of products, which are developed specifically for one customer. A distinction is represented between "types" and "instances". A "type" will become an "instance", i.e. is instantiated, when one actual product is being considered. For products developed specifically for one customer, the product and process development extends into the "instance" phase. The advantages of the application of Industry 4.0 result from this multi-layer, multi-dimension nature; the most prominent are: Industry 4.0 allows to …

- … combine the performance of several distributed production sites, warehouses and distribution sites,
- … avoid waste (e.g. parts which are need in small quantities but are present in several warehouses),
- … realize process quality comparison and consequently optimization (e.g. one production site may realize certain processes more efficiently),
- … perform process benchmarking even with other industries,
- … perform distant process monitoring and parameter tuning,
- … perform distant fault accommodation and networked fault accommodation,
- … perform distant control reconfiguration and distant service.

Due to this advantages, no production company can face global competition without the capability to operate cyber-physical systems. These systems can be the victim of digital attacks from the outside; these attacks are characterised in the subsequent section.

3. External attacks on automated systems

If one seeks to investigate the nature and consequences of cyber-attacks on control systems, it is mandatory to capture the available resources of the attacker and the attacker's knowledge (Teixeira et al. 2015). The nature of external attacks and possibilities to identify certain characteristics were investigated in several important research works (Johansson 2021). In order to fully understand the nature of external attacks a systemic view is sensible (Figure 2).

The systemic view shown in Figure 2 is based on considerations by Teixeira et al. (2015), but was expanded to include all aspects of automated systems. The core of the system model is the physical system, i.e. the manufacturing, assembly or logistics plant with its actuators (e.g. industrial robots or AGVs) and its sensors (e.g. cameras or ultrasonic position sensors). In this system, commonly some kind of product is produced or transported. The physical system receives actuator commands that may come from other system units or over the network from external locations. The core system sends sensor readings directly to other units or over the network to external location. These sensor readings are usually processed by a control system which should guarantee a stable operation of the core system. This control system will send actuator commands which are intended to lead to the intended stable operation of the physical system. The sensor information is additionally sent to a diagnosis system. which is primarily intended to detect faults, i.e. deviations from the nominal behaviour of the physical system. Such diagnosis systems often depend on mathematical models which can also take actuator commands into consideration; therefore, the actuator commands are frequently also sent to the diagnosis system. This diagnosis system may also detect an external attack, because external attacks frequently also lead to anomalies in the sensor readings. However, this possibility will be discussed in Section 4.

https://doi.org/10.1017/pds.2022.201 Published online by Cambridge University Press

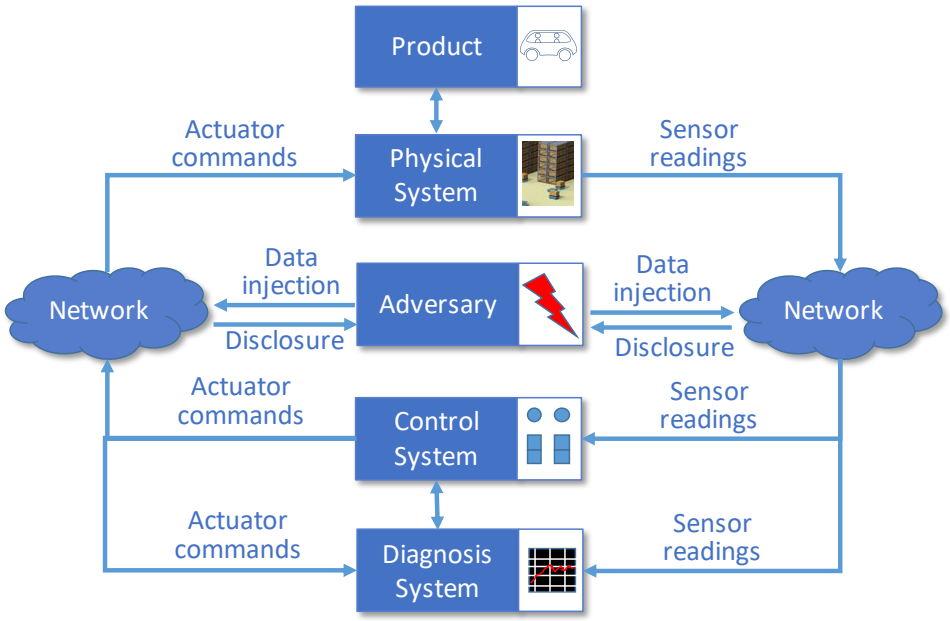

Figure 2. System model of an external attack to an automated system

Also visible in the centre of Figure 2 is the adversary, i.e. the entity that wishes to perform an external attack. From an abstract viewpoint it maybe deduced that in the network two general types of information are available: actuator commands or sensor readings. The adversary has now initially four options: to disclose sensor readings (e.g. to receive information in order to learn about the nature of the physical system), to disclose actuator commands (e.g. to receive information in order to learn about the actuator structure of the physical system), to inject data in actuator commands (e.g. to alter commands leading to harmful actuator actions) and to inject data in sensor readings (e.g. to alter the input information for the control system so that the control system will give "wrong" actuator commands leading to harmful actuator actions in the physical system). Only data injection can lead to a direct attack, but in the long term also disclosure attacks can be dangerous.
In this context, it is sensible to analyse the adversary more closely. This can lead to an adversary model (Figure 3, adapted from Teixeira et al. (2015)).

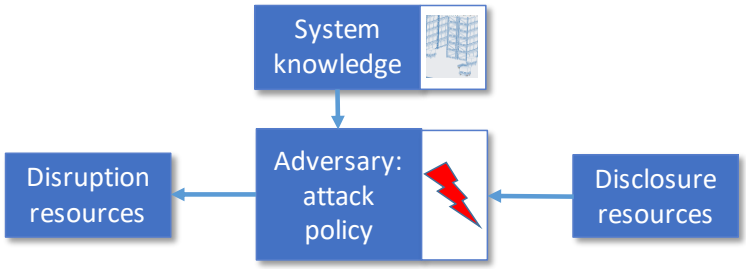

Figure 3. Adversary model

Adversaries are pursuing certain goals with their attack, for instance to prevent the production of a certain product, to damage the resources of the automated system or even to endanger human beings. Obviously, this attack might be just one element in a bigger plan, for instance in a plan to extort money from the owners of the automated production system. For the attack itself, a certain attack policy has to be formulated, which represents the disruption resources (usually the data injection - compare Figure 2) and their effect on the physical system. This effect can be realised either direct via changing actuator commands or indirect via changing sensor readings. An attack policy can only be successful, if a certain knowledge concerning the physical system is available to the adversary; usually this is obtained via disclosure resources (other possibilities to acquire this knowledge are connected with industrial espionage - the system knowledge can, in theory, also be expanded using such sources). Applying the mentioned aspects, a three-dimensional model can be derived (Figure 3).

https://doi.org/10.1017/pds.2022.201 Published online by Cambridge University Press

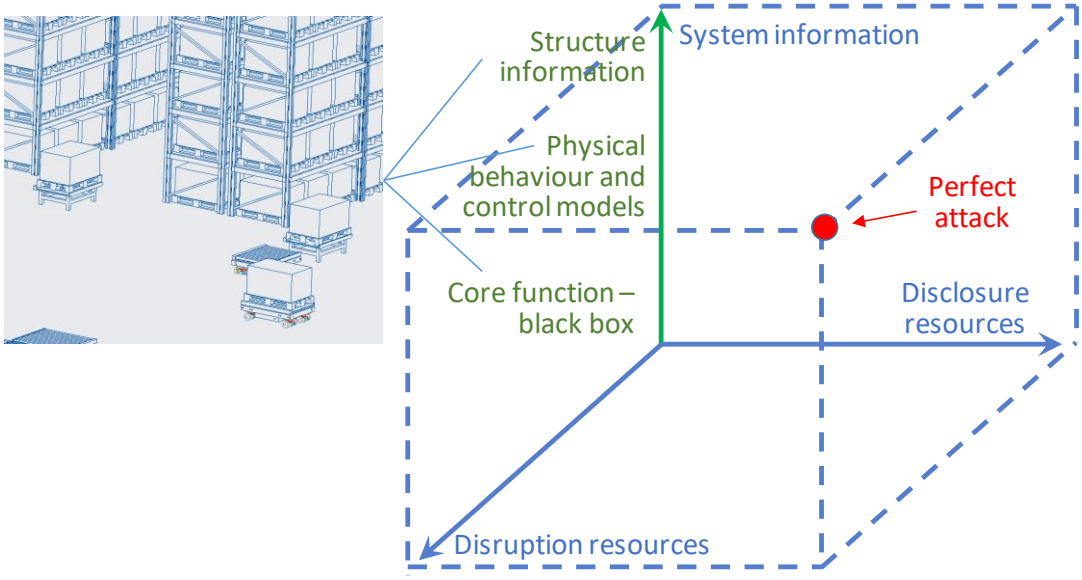

Figure 4. Three-dimensional model of an attack - the attack space

A three dimensional model was also proposed by Teixeira et al. (2015). In Figure 4 a classification of the system knowledge was added. In the best case, seen from the position of the attacked company, the adversary only has some kind of functional knowledge in form of a so-called "Black-Box", i.e. the adversary knows what a certain plant is producing using which main prefabricated goods, but has no knowledge about the internal structures and processes within the plant. A worse case is present, if the adversary was able, e.g. by means of disclosure resources, to obtain models of the physical behaviour of the system and its control system (or even diagnosis system). In the worst case, the adversary also knows the structure of the automated system, for instance what industrial robot is present at which position and how it is protected. Also visible in Figure 4 is a perfect attack - an adversary has perfect disclosure resources, perfect disruption resources and full system knowledge. In this case, it would be nearly impossible to counteract this attack. But even attacks which are less than perfect can have enormous consequences; approaches to reduce or eliminate these consequences are discussed in the next section.

4. Reducing or eliminating the consequences of attacks

In this section it is assumed that the disruptive resources of an attack have passed the IT security "barriers" (probably most of the attacks will not pass these barriers, but one still has to assume that no protection is perfect) and are influencing either the actuator commands or the sensor readings within the system. Obviously, the severity of such attacks can range from a simple system performance degradation over the necessity of a system shutdown up to endangering human operators or human product customers. Still, the involved designers have to assume that an adversary will try to realize the most severe attack possible, given his/her disclosure and disruption resources and system knowledge.
The main thesis of this research work is that a conscious design of the elements and structure of the physical system would allow to reduce or eliminate the consequences of this attack. At this point, one may ask, if the underlying design considerations are different from the design considerations in design for safety or fault-tolerant design. Obviously, these considerations will support the cyber-security aware design because the former will reduced negative consequences of any system behaviour and the latter will contribute to the possibility to ensure graceful degradation of a system.
However, a substantial conceptual difference is caused by the fact that cyber-attacks and faults have inherently different distinct characteristics:

- faults are certain physical events which affect the system behaviour, where simultaneous events are assumed to be non-colluding, i.e., the events do not act in a coordinated way and

https://doi.org/10.1017/pds.2022.201 Published online by Cambridge University Press

- cyber-attacks may be performed over a significant number of attack points in a coordinated fashion (Teixeira et al. 2015).

Consequently, specific methodologies are needed to deal with cyber-attacks and this direction needs to be explicitly stated in the system requirements in order to assure an appropriate consideration; sensible requirement management activities and models are described e.g. by Holder et al. (2017). This section describes an initial collection of design approaches which were collected based on the experience of the authors and discussions with colleagues in academia and industry. For the measures for reducing or eliminating the consequences of attacks, six general directions or principles can be distinguished: separation, limitation, protection, monitoring&diagnosis, warning and redundancy. For those directions certain sub-directions can be found. The directions and sub-directions are listed together with examples in Figure 5.

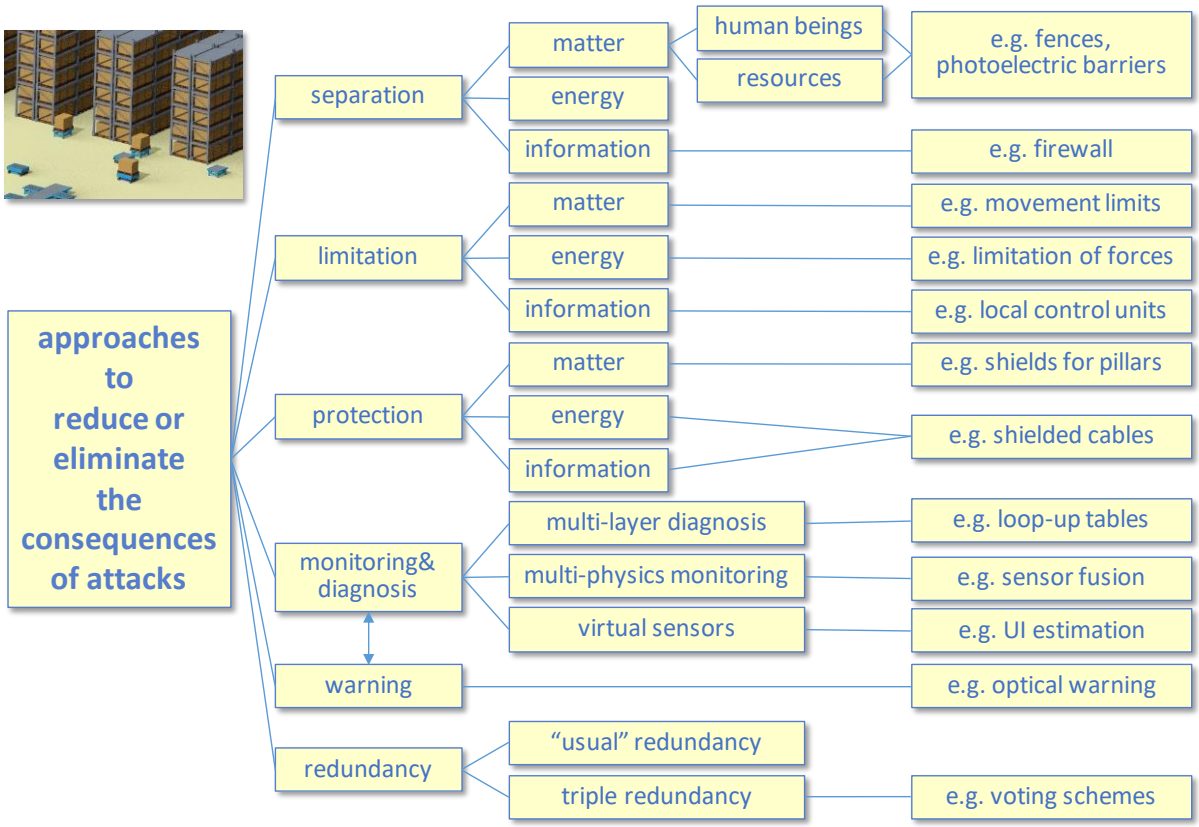

Figure 5. Approaches to reduce or eliminate the consequences of attacks

The first main direction concerns the separation of matter, energy and information from the consequences of an attack. In most cases the most serious consequences will be unwanted actions by the actuators in a system, e.g. an undesired movement of an industrial robot or automated guided vehicle (AGV), which could endanger a human operator. The consequences of such actions can be eliminated, if any endangered objects are separated from the actuator - in this case an inherently safe configuration is present. This can be done for instance by means of fences or photoelectric barriers. A separation of the control is possible, if mechanical or hydraulic control loops are realized, which can be per se not be influenced by cyber-attacks. For a separation of information, a so-called firewall can be used which establishes a barrier between a trusted and an untrusted network. In many cases a separation may not be possible or sensible, in such cases a limitation of matter, energy or information may be a promising direction. Hard-programmed movement limits in industrial robots, a limitation of forces and moments using limited torque clutches and limited data transfer through local control units are possible examples. The concepts of robust control and robust design also employ limiting strategies, such as limiting the effect of tolerances or limiting to allowable ranges of control actions. The precedent measures can be accompanied by protection measures, which again can concern matter,

https://doi.org/10.1017/pds.2022.201 Published online by Cambridge University Press

energy or information. In a warehouse certain structural elements of shelves may be protected by flexible protection elements. Shielded cables will protect the energy or information flows. In the system model in Figure 2 a diagnosis system is visible, which can also be used to detect anomalies, which are caused by cyber-attacks. As the necessary basis for diagnosis is always a continuous monitoring of the system state, the monitoring plays a central role. It is more probable that diagnosis will capture the anomalies caused by a cyber-attack, if many independent diagnosis layers are operative. One example for an additional layer would be a low-level real-time diagnosis process on a local process unit, which relies on a plausibility check with look-up tables (this local diagnosis system could compare sensor readings with predefined lock-up tables in order to check plausibility - this is possible in real time and with low processing power). The probability is also enhanced when a multi-physics monitoring is relying on sensors with different physical sensing mechanisms and the information are combined with sensor fusion (Stetter 2020a) or when virtual sensors are used, e.g. by means of unknown input (UI) estimation (UI estimation is an analytical calculation of unknown inputs - the results can be compared with sensor readings and differences and anomalies can be detected). The results of an anomaly detection should be brought immediately to the attention of the operators, e.g. by means of an optical warning. A straight forward measure can be the implementation of redundant elements, for instance could a second conveyor line still transport goods, when a first line is damaged by the actions of an actuator with unwanted behaviour because of a cyber-attack. More important is the use of redundant sensors, because a difference in the sensor readings could help to discover a data injection attack in these readings. Even more advantageous can be a triple redundancy concept, because a voting scheme could achieve that the right sensor readings are still sent to the control and diagnosis system, even if a data injection attack occurs to one of the sensor readings. It is important to note that the presented taxonomy may be expanded in future.
It is the task of the designer to choose the right measures for a certain system. It is important to note that a concise view on cyber-security also includes socio-technical and human aspects. The first entry of a cyber-attack might be eased by the intentional or unintentional disclosure of information concerning the system. It is also important that the designer is aware that an attacker might have a good knowledge of the automated system and that the attacker may use several coordinated attacks which aim at possible weaknesses of the system. Several possible measures are explained in detail in the next section.

5. Application example: automated logistics system

The automated logistics system under consideration concerns a high-rise warehouse with a logistics system realised by means of AGVs (Figure 6).

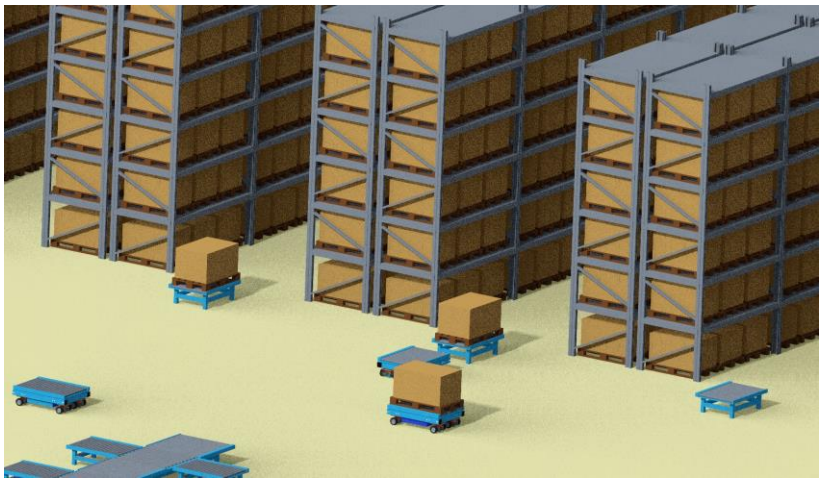

Figure 6. Automated system - logistics for a warehouse

The warehouse shown in Figure 6 consists of high-rise shelves with packaged goods on regular palettes placed on these shelves. Between the shelves are aisles for automated forklifts. High-rise

https://doi.org/10.1017/pds.2022.201 Published online by Cambridge University Press

warehouses have the advantages of a good access to every article, good height utilization, pressure-avoiding storing of the goods and a rational design (Martin 2016). The storage and retrieval system can be realised by forklifts, which receive items from transfer stations or deliver them to transfer stations. Form these transfer stations the items are delivered by means of a transportation system consisting of AGVs (Witczak et al. 2020). The individual AGVs are equipped with a roller conveyor for the transportation of palettes and dispose of a certain steering mechanism which allows unlimited manoeuvrability. The design of this AGV is realized in the form of a multi-purpose production platform (Figure 7).

Figure 7. Transportation platform in the automated system

The AGVs of the transportation system can theoretically move freely in the zone in front of the warehouse and can deliver and retrieve items on palettes to and from the transfer stations as well as to and from an external transportation unit (visible in the lower part of Figure 6). In the following sentences possible measurements which are appropriate, amongst others, to reduce the consequences of cyber-attacks:

- For the AGVs in such systems a large set of **requirements** is necessary - ranging from dimensional requirements over the carrying capacity to possible inclinations and certain allowable floor distortions. Some of these requirements also concern a safe operation even in the case of the occurrence of certain events such as sensor fault. An additional risk is caused by the fact that an adversary could start several attacks simultaneously or in an especially dangerous sequence. For the AGV, it could mean that the trajectories of two AGVs are modified and a following collision could be even more dangerous. Consequently, a conscious consideration of such possibilities should be listed as **explicit** requirement. For instance, a requirement "an alteration of the trajectories of AGVs from the outside of the company has to be avoided" can be formulated.
- As a first measure to reduce the consequences of cyber-attacks and other unfavourable events, the AGVs can only operate in a secure area and human beings are **separated** from the whole movement area. A separation is also visible concerning information, because the AGVs have their own dedicated control system and the influence possibilities of the supervisory control are limited.

https://doi.org/10.1017/pds.2022.201 Published online by Cambridge University Press

- The maximum speed of the AGVs is **limited** on a low, local control level. The maximum speed can only be changed using a key protected special setting mode that is present locally on the AGV.
- On the AGV four elastic bumpers are present at the front and the rear end (they are nearly identical) and **protect** the ultrasonic sensors when the usual driving mode (straight forward or straight backward) is used. In the field close to the AGV, ultrasonic sensors (visible in Figure 7) will detect obstacles.
- Obviously, on higher control and **diagnosis** levels the AGV position is monitored using odometry and cameras mounted in the building, but on the low level these sensors can still reduce the consequences of any unwanted operation of the AGVs.
- For the whole system, the use of many **redundant** AGVs can also reduce the consequence of a cyber-attack or other events which will result in the inoperability of one AGV. Another measure based on the principle of redundancy is the use of redundant and overlapping (compare Stetter 2020a) ultrasonic sensors.
- One very specific measure is the application of a virtual sensor for **monitoring&diagnosis**. This sensor is based on a detailed kinematic and kinetic model of the AGV driving system. This model is realized in form of a discrete state space model which was developed analysing the longitudinal and lateral wheel forces as well as the yaw rate dynamics (Stetter 2020b). Due to the presence of this kind of model it is possible to apply an unknown input estimator similar to the one proposed by Gillijns and De Moor (2007). This approach is based on a recursive filter an allows to estimate an unknown input to the system - in this case the longitudinal forces acting on each wheel and the total torque acting on all wheels. Based on the estimation, nine residual signals can be achieved, i.e. differences between the estimations by the unknown input estimator and current measurements. These residuals can be used to detected anomalies, which may be caused by a cyber-attack. In general, virtual sensors, i.e. mathematical models of the system, which are compared to current measurement and can be used to detect anomalies, are a promising means to reduce the consequences of external attacks.

Besides these examples, several other measures can be taken which will also support the listed principles of cyber-security aware design.

6. Conclusions and outlook

Cyber-attacks are one of the most prominent threats to our daily life and also to all industrial activities. Researchers in IT have developed numerous concepts, algorithms and methods to counteract such attacks and especially larger companies have implemented these in their systems. However, due to the exponentially increasing number of attacks, responsible designers should not just rely on IT measures - they should support these endeavours by designing their technical systems in a way that makes it less vulnerable to these attacks. In this scope one may ask, if it would not be sensible to isolate certain control systems completely from external networks. However, as presented in Section 2, concepts like Industry 4.0 dispose of several advantages and companies need to apply them in order to compete in the global competition; the trend towards cyber-physical systems points in the same direction. Consequently, responsible designers have to choose the right measures to limit the consequences of cyber-attacks not detected by the IT-system. It is important for the designers to consider the fact that an adversary might have a good knowledge of the technical system and may use several coordinated attacks which aim at possible weaknesses of the system. It is important to add cyber-security aware consideration into the set of requirements. Additionally, designers can choose from a set of general principles, an initial collection was presented in this paper and explained based on an automated system. It is important to note that the presented collection of design approaches is in an exploratory research stage and is rather intended to be a starting-point for further investigations. The principles support designers on a rather abstract and general level; analytic and quantitative methods are needed to support the implementation of these principles - this will also be the focus of future research

https://doi.org/10.1017/pds.2022.201 Published online by Cambridge University Press

activities. The socio-technical and human aspects of cyber-security also require further research in order to establish a conclusive understanding of this important issue.

Acknowledgement

Parts of this research were supported in the scope of the project "Automatisierter Entwurf eines geometrischen und kinetischen digitalen Zwillings einer Rohbaufertigungsanlage für die Virtuelle Inbetriebnahme (TWIN)" which is funded by the German Federal Ministry of Education and Research.

References

Bayuk, J.L.; Horowitz, B.N.: An Architectural Systems Engineering Methodology for Addressing Cyber Security. Systems Engineering Vol 14, No. 3, 2011, pp. 294 - 304, https://doi.org/10.1002/sys.20182.

Gero, J.; Kannengiesser, U.: The Function-Behaviour-Structure Ontology of Design. In An Anthology of Theories and Models of Design; Chakrabarti, A., Blessing, L.T.M., Eds.; Springer: Berlin, Germany, 2014.

Gillijns, S.: De Moor, B.: Unbiased minimum-variance input and state estimation for linear discrete-time systems. Automatica. 43 (2007), pp. 111 – 116, https://doi.org/10.1016/j.automatica.2006.08.002.

Goorden, M.; van den Mortel-Fronczak, J.; Etman, P.; Rooda, J.: DSM-based Analysis for the Recognition of Modeling Errors in Supervisory Controller Design. In: 21st International Dependency and Structure Modeling Conference, 2019, pp. 121 - 129, https://doi.org/10.35199/dsm2019.7.

Holder, K.; Zech, A.; Ramsaier, M.; Stetter, R.; Niedermeier, H.-P.; Rudolph, S.; and Till, M. (2017) "Model-Based Requirements Management in Gear Systems Design based on Graph-Based Design Languages". Appl. Sci. 2017, 7, 1112, https://doi.org/10.3390/app7111112.

Johansson, K.H.: Cyber Security and Privacy in Networked Control Systems. Keynote at the IEEE International Conference on Control and Fault-Tolerant Systems, Systol, 2021.

Kadir, B. A.; Broberg, O.; Souza da Conceição C.; Jensen, N. G.: A Framework for Designing Work Systems in Industry 4.0. In: Proceedings of the Design Society; Cambridge, Part 1, pp. 2031-2040. Cambridge: Cambridge University Press. (2019) DOI:10.1017/dsi.2019.209.

Kushner, D.: The Real Story of Stuxnet. IEEE Spectrum. Accessed 12 October 2021.

Martin, H.: Transport- und Lagerlogistik. Systematik, Planung, Einsatz und Wirtschaftlichkeit. 10th Edition. Springer Vieweg 2016.

Stetter, R.: Fault-Tolerant Design and Control of Automated Vehicles and Processes. Insights for the Synthesis of Intelligent Systems. Springer: (2020a), ISBN 978-3-030-12845-6.

Stetter, R.: A Fuzzy Virtual Actuator for Automated Guided Vehicles. Sensors (2020b), Vol. 20, No. 15, 4154, https://doi.org/10.3390/s20154154.

Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K. H.: A secure control framework for resource-limited adversaries, Automatica, Volume 51, 2015, pp. 135-148, https://doi.org/10.1016/j.automatica.2014.10.067.

Ustundag, A. and Cevikcan, E.: Industry 4.0: Managing the digital transformation. Springer, 2019.

Vogel, S.; Martin, G.; Schirra, T. and Kirchner, E.: Robust Design for Mechatronic Machine Elements - how Robust Design Enables the Application of Mechatronic Shaft-hub Connection. In: Proceedings of the international design conference Design 2018, pp. 3033 - 3040, https://doi.org/10.21278/idc.2018.0203.

Whitman, M. E.; Mattord, H. J.: Principles of Information Security, 7th Edition. Cengage Learning, 2022.

Wichmann, R. L.; Eisenbart, B. and Gericke, K.: The direction of industry: a literature review on industry 4.0. In: Proceedings of the Design Society; Cambridge, Part 1, pp. 2129-2138. Cambridge: Cambridge University Press. (2019) DOI:10.1017/dsi.2019.219.

Witczak, M.; Majdzik, P.; Stetter, R. and Lipiec, B.: A fault-tolerant control strategy for multiple automated guided vehicles. Journal of Manufacturing Systems (2020), Vol. 55, pp. 56 – 68, https://doi.org/10.1016/j.jmsy.2020.02.009.

ZVEI: German Electrical and Electronic Manufacturers' Association. Industrie 4.0: The reference architectural model Industrie 4.0 (RAMI 4.0). 1, 2015.