H. Langweg, M. Meier, B.C. Witt, D. Reinhardt (Hrsg.): Sicherheit 2018,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 133

Harmonizing physical and IT security levels for critical infrastructures

Vanessa Chille[1], Sibylle Mund[2], Andreas Möller[3]

Abstract: We present a concept for finding an appropriate combination of physical security and IT security measures such that a comprehensive protection is provided. In particular, we consider security for critical infrastructures, such as railway systems. For classifying physical security measures, the so-called Protection Classes from the standard EN 50600 are used in our approach. To provide comprehensive protection for a system under consideration, these sets of explicit physical security measures need to be combined with other kinds of security, such as IT security and organizational security. We present a new classification approach named 'Type of Attack(er)' that allows for taking all aspects of security into joint consideration, and harmonizes physical and IT security levels by creating a link between EN 50600 and IEC 62443.

Keywords: physical security, IT security, IEC 62443, EN 50600, critical infrastructures

1 Introduction

In recent times, threats for critical infrastructures have attracted increasing attention. The motivation and character of suspected attacks differ greatly. They range from vandalism through cyber attacks that are not specifically targeted towards a particular organization to international terrorism. A typical example for a critical infrastructure - requiring security measures to ensure not only the system's availability but also the safety of people – is a railway system.

A comprehensive approach towards security necessitates the consideration of a number of different aspects of security. Beside the aspect of IT security that is being treated with increasing care by now, physical security plays an important role. It represents a necessary complement to enable overall security that deserves more attention than it often receives. Appropriate physical security measures prevent two different types of attacks: purely physical attacks and attacks on the IT system enabled by physical access (for example to a USB port). In the latter case, physical security measures represent an important additional security perimeter complementing IT security measures. Purely physical attacks may consist of damaging equipment or performing other manipulations, mostly causing an impairment of the system's availability and financial losses. Even though the consequences may be less severe for the latter case, the operator of a critical infrastructure will have great interest in avoiding the effects of both types of attacks.

[1] Siemens AG, Mobility Division, Ackerstraße 22, 38126 Braunschweig, vanessa.chille@siemens.com
[2] Siemens AG, Mobility Division, Ackerstraße 22, 38126 Braunschweig, sibylle.mund@siemens.com
[3] Siemens AG, Mobility Division, Ackerstraße 22, 38126 Braunschweig, andreasmoeller@siemens.com

doi:10.18420/sicherheit2018_10

For this purpose, appropriate measures have to be identified, which requires an evaluation of the effectiveness of the measures (Sec. 2). Furthermore, the security of a system depends strongly on how well all aspects of security are coordinated and work together. Therefore, only a holistic point of view can lead to comprehensive protection (Sec. 3). In the end of the present paper, we also comment on how such protection can be achieved for the example of railway systems (Sec. 4). The first step in this direction is to find a possibility for classifying physical security measures. Only few works exist that address the topic of physical security in a detailed and comprehensive way. Standards for particular components such as doors and windows [EN27], cylinder locks [EN03] and the like go in the very details, and for instance even comment on testing procedures. Standards addressing security on a global level make mostly only general statements about how to achieve physical security and do not give explicit requirements or precise measures that should be taken. For example [NE-4d] gives a number of organizational measures that shall be taken, but does not go into detail about requirements for measures intending to prevent unauthorized access. Another prominent example is ISO/IEC 27001 [ISO01], which, for instance, states that physical security perimeters shall exist, but does not elaborate on how to implement them. In IEC 62443 [IEC3-3], the physical security measures suggested as compensating countermeasures are not specified either. In that context, it is also necessary to understand which physical security measures correspond to which IT security measures. Furthermore, there are the German publications VdS 2007 [VdS07] and VdS 2333 [VdS33], the combination of which provides a consistent and detailed concept for sets of physical security measures. International standards are however to be preferred in an international context. A vast amount of general literature exists that comments on how to implement measures such as video surveillance or physical barriers in an appropriate way for particular sites. Most of it, however, does not provide any real classification of physical security measures but rather comments on principles. A very convenient standard in that context is EN 50600 ([EN-1] and [EN2-5]): we found that it is also well-suited for our purposes, and describe its main aspects in Sec. 2. We use the physical security classification from this standard as a tool in our approach. To the best of our knowledge, a systematic and holistic approach to physical security, in particular for critical infrastructures, has been missing so far. We present an approach that is suitable for critical infrastructures, and also for the very special conditions of railway systems. Our concept uses existing standards and, in particular, unites IEC 62443 and EN 50600. For that purpose, we introduce a new classification named ‘Type of Attack(er)’ that captures all aspects of security at once (see Sec. 3.2). It might be regarded as a continued development of the holistic security concept discussed in [Ko16] by adding the aspect of physical security.

An illustration of this idea can be found in Fig. 1, where the most important kinds of security and their interplay are depicted. It is indicated that the basis of all security is the process maturity that describes an organization’s capability to follow procedures. All other security measures are in vain if one cannot rely on the organization to implement the required organizational security measures. The Maturity Model from IEC 62443-2-4 [IEC2-4] can be utilized for the evaluation. It uses four Maturity Levels; from Maturity Level 3 on, the performance is repeatable, i.e. the organization is able to actually adhere

to processes. IT security and physical security are built on the foundation formed by process maturity and need to complement each other. Both of them also contain organizational security measures. IT security is addressed in IEC 62443 and classified by Security Levels (SL). The topic of physical security shall be addressed in detail in the present paper. The joint effect of all these aspects of security shall be the resistance against particular attacks or attackers, classified by the 'Type of Attack(er)'.

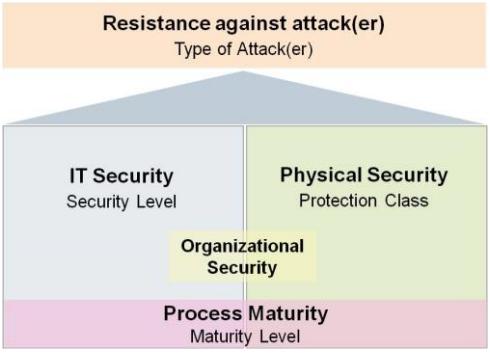

Fig. 1: Different aspects of security and their interplay

2 The standard EN 50600

The standard EN 50600 is not the obvious standard to be used for critical infrastructures, as it provides regulations for data centre facilities and infrastructures. However, an examination of the details reveals that it is well-suited for ensuring the physical security in any kind of building.

2.1 Basic principles

EN 50600 gives a practical concept for the implementation of physical security using common security principles [EN-1]. Firstly, a risk assessment is to be performed that is then used as the foundation of decisions on which security measures shall be taken. For this reason, it is frequently referred to throughout the standard. Furthermore, EN 50600 also explicitly addresses the topic of organizational security and requests organizational measures to accompany physical security. Another concept appearing also in many other contexts related to security is Defense in Depth. It means that multiple security measures shall be taken for the protection of the assets such that an attacker cannot intrude by overcoming one single security measure. For physical security, it means quite literally that security perimeters consisting of physical barriers shall be arranged in an onion skin-like configuration (see Fig. 2). EN 50600 utilizes a system of four Protection Classes (PC). The assets that require the strongest protection shall be located in PC 4, i.e. the highest class, where the criteria for gaining access are the most restrictive.

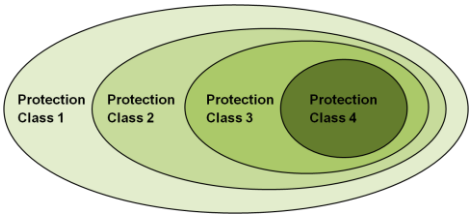

Fig. 2: Concept for the Defense in Depth principle on the level of physical security [EN-1]

2.2 Protection of boundaries

The boundaries of the areas associated with the various Protection Classes (as indicated in Fig. 2) are supposed to be protected by means of passive elements, i.e. mechanical barriers, as well as technical security systems for the prevention of unauthorized access. The latter are further described by referring to specialized standards for the respective systems: security lighting, video surveillance systems (EN 62676-1-1:2014, Grade 2, where justified according to the risk assessment), intruder and holdup alarm systems (EN 50131, security grade according to risk assessment), access control systems (EN 60839-11-1, security grade according to risk assessment), and alarm monitoring (EN 50136 series and EN 50518 series).

The passive elements are characterized by referring to the so-called Resistance Classes (RC) from EN 1627 on burglar resistance [EN27]. Elements such as doors, windows, locks, and the like are supposed to resist the attack of a particular kind of burglar with a defined tool set and a limited amount of time. The Resistance Classes utilized in EN 50600 are illustrated on the right-hand side of Fig. 3. The tool sets get more elaborate the higher the Resistance Class; the pictures only mean to give an idea, please find the detailed lists of allowed tools in EN 1630 [EN30].

2.3 Protection Classes

The Protection Classes require different sets of the aforementioned protective measures [EN2-5]. Here, we only want to give a basic impression of the most important requirements, detailed information can be found in EN 50600 itself [EN2-5]. For the passive elements, the requirements are given in a precise way by attributing particular Resistance Classes to the Protection Classes (PC 1 – RC 2 / PC 2 – RC 3 / PC 3 & 4 – RC 4). Concerning the technical systems, the standard does not make explicit statements on their deployment in the various Protection Classes. It is sometimes however implied when, for example, from PC 2 on, the opening of an emergency door must cause an alarm by the intrusion alarm system. Another topic worth mentioning is the one of the co-location of boundaries. Areas designated to different Protection Classes need to be separated by identifiable physical barriers. Not all boundaries of the areas attributed to the various Protection Classes are allowed to be co-located, which ensures the presence

of multiple physical security perimeters around the most critical assets. One can regard this as a contribution to the fulfilment of the Defense in Depth principle.

Please note that EN 50600 offers flexibility concerning the conditions to be provided for the Protection Classes. On the basis of the risk assessment, one may decide to apply particular protective measures or not. The conditions that one is supposed to establish for the Protection Classes originate from their definitions that describe how many and which kind of people shall have access to the respective areas. They can be found in Tab. 1 below.

Protection Class 1	**Protection Class 2**	**Protection Class 3**	**Protection Class 4**
public or semi-public	accessible to all authorized personnel, employees as well as visitors	accessible only for specified employees and visitors	accessible only for specified employees with an identified need for the access

Tab. 1: Definitions of the Protection Classes via access authorizations [EN-1]

3 Comprehensive protection

3.1 Physical security & IT security

The above approach using access authorizations as the defining characteristic of the classification can pose difficulties. A system's need for protection might not always be perfectly in line with the intended limitations of access authorizations. Therefore, the approach is not the most convenient basis for the decision which of the Protection Classes is suitable for an individual system under consideration. Furthermore, the definition of the Protection Classes is an inconvenience in another way: we aim at a holistic view on security and for this purpose want to analyze the interplay between IT security and physical security. IT security is commonly classified via the Security Levels from IEC 62443 [IEC3-3]. This standard has originally been designed for industrial automation and control systems, but is being utilized in other domains as well. In order to understand the correspondence between IT security and physical security, we aim at finding correspondences between Security Levels and Protection Classes. The Security Levels are defined via a characterization of the expected attacker and his means, resources, skills and motivation. The definition of the Security Levels thus follows a philosophy that is entirely different from the aforementioned approach for the Protection Classes. However, as discussed above, for passive elements, the Protection Classes refer to the so-called Resistance Classes from EN 1627. These are again defined via a characterization of the burglar that is to be expected. The close resemblance to the definition of the Security Levels offers a convenient way of matching Protection Classes and Security Levels. One may argue about whether it is fair to base the argument for the correspondences only on the characterization of the passive elements. However, since the respective Resistance Classes are regarded as an adequate component of the

protection required for a particular Protection Class, this seems to be a legitimate approach.

Fig. 3 illustrates the matching of Security Levels and Protection Classes. PC 1 does not fit to SL 1, as the tool set available to the attacker for PC 1 is too large for a casual or coincidental attack. The low level of risk the attacker is willing to take in PC 1, however, fits nicely to the attacker's low motivation in SL 2. After a comparison of further aspects, PC 1 and SL 2 can be associated. Similar lines of argumentation lead to matching PC 2 with SL 3 and PC 3 and 4 with SL 4.

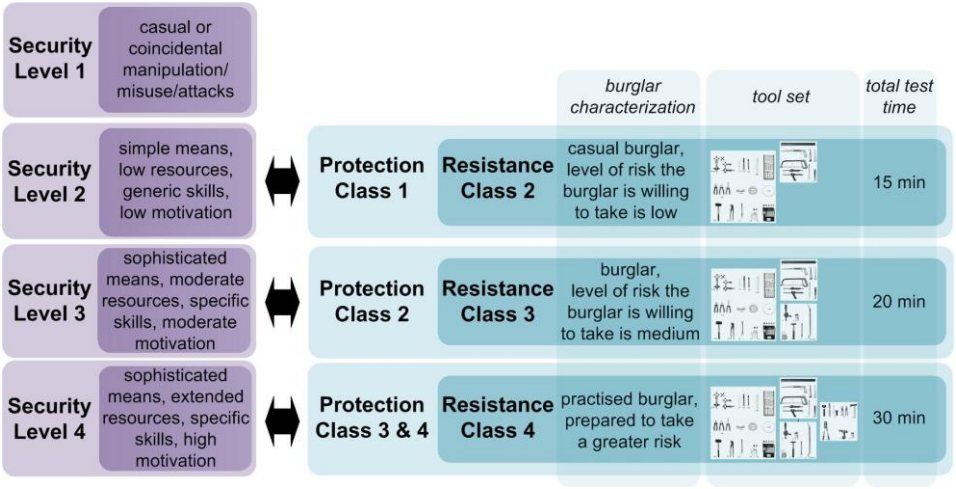

Fig. 3: Matching Security Levels [IEC3-3] and Protection Classes [EN2-5] (and Resistance Classes [EN27, EN30])

One may continue and also specify security grades for technical security systems. EN 50600 requires for most of them only that they shall be compliant with the respective specialized standards, and to choose their security grades according to the risk assessment. However, the above logic can also be pursued further and in this way security grades of technical systems are linked to the Protection Classes and Security Levels. It facilitates the mapping that in many of the associated standards, the security grades are also defined via some sort of characterization of the attacker's means, resources and the like. The results can be found in Tab. 2.

IEC 62443	EN 50600	EN 1627	EN 62676	EN 50131	EN 60839
IT security	physical security	passive elements	video surveillance	intrusion and holdup alarm	access control
SL 1		RC 1 N*	X	X	mechanical key**
SL 2	PC 1	RC 2	Grade 2	Grade 2 (or 1)	Grade 2 (or 1)
SL 3	PC 2	RC 3	Grade 3	Grade 3	Grade 3
SL 4	PC 3 or PC 4	RC 4	Grade 4	Grade 4	Grade 4

* RC 1 N protects mainly against acts of vandalism, such as attempts against forced entry by physical force (kicking, jumping, shoulder slams, lifting up and tearing out). It should thus provide enough protection to prevent an unauthorized person from casually or coincidentally accessing areas that require a minimum of protection against unauthorized manipulation.
** A conventional mechanical key seems perfectly sufficient: no sophisticated options such as unique identification of the user or multifactor authentication are needed. The management and storage of the keys need to be controlled.

Tab. 2: Correspondences between Security Levels, Protection Classes, Resistance Classes and security grades of technical systems

3.2 Type of Attacker

As we have already seen above, different aspects of security are regulated by a large number of different classifications. Most of them entail lists of detailed requirements that need to be fulfilled. This approach is very helpful when one is searching for precise guidance about how to implement the fulfillment of particular security requirements. In a first step, one however often does not want to make all these implications, as the analysis of a system's need for protection is independent of the practical implementation of protection by means of specified measures. A solution for this issue would be the introduction of a generic classification offering the possibility to express solely the level of protection. It should not make any statement on the implementation of that protection, i.e. whether, for example, means of IT, physical or organizational security are used to achieve it. In the previous section, you have seen that characterizing the attacker and his skills, motivation, tools and the like has proved to be a convenient principle allowing for finding links between different classifications. This is also due to the fact that many classifications already use it as an underlying principle. We thus suggest turning this approach into a classification itself. For this purpose, we characterize four Types of Attack(er)s (ToA) that a system can be supposed to be resistant against:

ToA 1	casual or coincidental manipulation or attack
ToA 2	attack(er) with simple means, low resources, generic skills and a low motivation
ToA 3	attack(er) with sophisticated means, moderate resources, specific skills and a moderate motivation
ToA 4	attack(er) with sophisticated means, extended resources, specific skills and a high motivation

Fig. 4: Types of Attack(er)s (ToA)

The above definition of the ToA is strongly inspired by the definitions of the Security Levels from IEC 62443 [IEC3-3]. The difference is that the ToA only expresses that a system is supposed to be resistant against that particular type of attacker. It does not imply anything more.

The approach offers a number of advantages:

- The definitions of the classification are as clear and simple as possible.
- A generic term is created that offers the possibility to talk about the level of protection required for a system without implying the deployment of particular measures.
- As many classifications already use the characterization of the attacker as an underlying principle, finding appropriate counterparts in the various domains of security is easy.
- The approach allows for taking the different aspects of security into joint consideration and is therefore truly holistic.

It is one of the key ideas of the approach that the Type of Attack(er) characterizes the attacker and does not imply anything more. By definition, there are no particular requirements associated with the ToAs. However, we offer guidance by making suggestions for how to achieve a particular ToA by linking different security classifications (see Tab. 2).

Please note that in order to provide comprehensive protection for a system, one also needs to understand how the different kinds of security work together: if they address the same factors and are thus redundant (possibly intended to ensure Defense in Depth), or if they take care of independent gateways that an attacker might exploit. We should thus aim at evaluating the joint effect of physical and IT security measures systematically. The Type of Attack(er) can be useful in that context. For illustrating the results of such an evaluation, we use a similar tool as the holistic security concept (HSC) from [Ko16]. The HSC utilizes a matrix to show which combinations of Security Levels and Maturity Levels result in which so-called Protection Levels. It expresses what kind of process maturity is mandatory to ensure that IT security measures can actually have an effect such that a particular Protection Level is achieved. The Protection Levels correspond to the Security Levels in a direct way and express that the protection targeted by the Security Levels is indeed achieved. We can develop that concept further and also take the physical security aspect into consideration by adding another axis to the matrix. A four-dimensional matrix is the result. For the sake of simplicity, for now, we want to assume that the Process Maturity is on Maturity Level 3 such that the organization is capable of following procedures. In this way, we may focus on IT security and physical security measures. Firstly, we need to ask what measures can actually be implemented to protect the system under consideration (SUC). We are facing three different categories for a *s*ystem's *c*apability of being *p*rotected (SCP) by physical or IT security measures, as illustrated in Fig. 5. Either only IT security or physical security measures, or both IT

and physical security measures can be implemented. In the case of the latter, one can furthermore distinguish the three cases (SCP3-I), (SCP3-II) and (SCP3-III) as indicated in Fig. 5. Those categories elaborate on which measures protect the same or independent ways of intrusion.

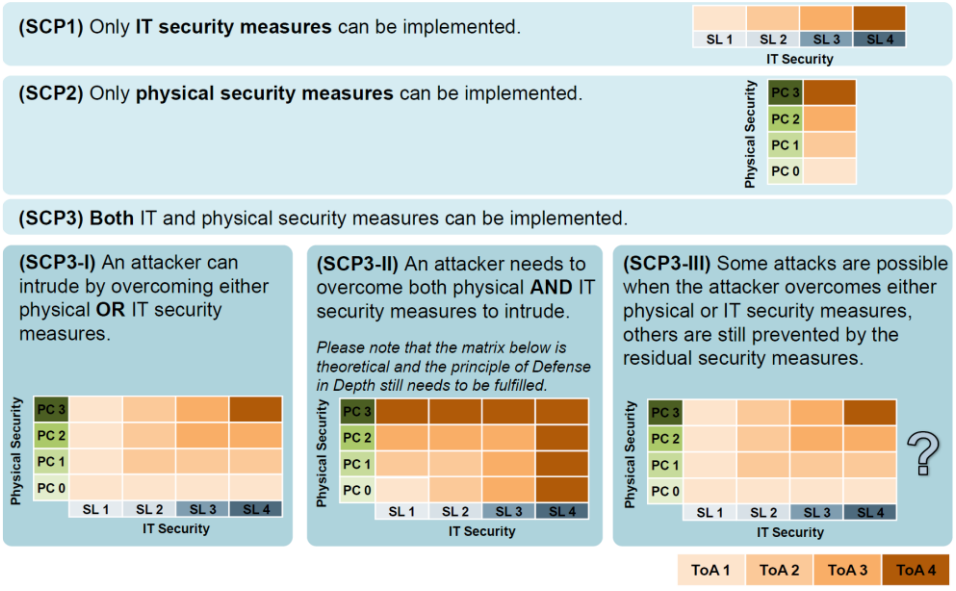

Fig. 5: Joint effect of physical and IT security measures

Fig. 5 also shows the matrices for all those cases. For (SCP3-I), both IT security and physical security measures need to be on an adequate level in order to ensure the security of the system. The measures need to be strong individually and the correspondences in Tab. 2 should be taken into consideration. This relation is also indicated in the matrix. For a system from category (SCP3-II), IT and physical security add up, such that only one of the two needs to be on a high level. Please note that the depicted matrix is purely theoretical, as the Defense in Depth principle still requires the implementation of both IT security and physical security. Systems assigned to category (SCP3-III) are the most complicated and the most common at the same time. As an example, one could think of a server room: if an attacker only overcomes the physical security measures and breaks into the building, he can perform an attack on the availability by destroying the equipment with brute force. In order to intrude into the IT system, the attacker needs to overcome further IT security measures. This situation is too complex to express it in a single matrix. In practice, most systems do in fact belong to category (SCP3-III).

Even if the above matrices thus cannot provide a comprehensive description of the complex issue in many cases, one aspect of the considerations should always be kept in mind: it is recommended to differentiate between the ‘OR’ and ‘AND’ cases (SCP3-I and SCP3-II) when designing the set of security measures for any SUC. In addition, one

should consider that in case of doubt, the Defense in Depth principle always suggests deploying all security measures according to Tab. 2.

4 Example: comprehensive protection of a railway system

In the context of railway systems, critical assets can be found in different kinds of locations thus providing very particular conditions. These may be categorized as trains, tracks and rooms - such as Operation Control Centers and server rooms. Independently of the existing differences in the locational circumstances, we need to aspire to provide the same security for the assets in all locations. This target can be expressed very easily by using the Type of Attack(er) approach: the same ToA shall be assigned to all locations. In order to decide which ToA is suitable, one may recourse to established principles, as they already exist for IT security and the assignment of Security Levels. The ToA that one assigns to a system under consideration shall match these Security Levels. It is convenient to base the decision on the ToA on the analysis for IT security, as such analyses are being performed by most organizations already (for example according to [DIN-04]). This means, for example, that if SL 3 is assigned, the system shall be protected according to ToA 3, as those classifications share the same attacker characterization (see Fig. 3 and Fig. 4). The fact that all locations shall be protected according to a particular ToA, however does not mean that the very same protective measures need to be applied everywhere. The specific conditions in the individual locations shall be taken into account to find the appropriate measures. The Protection Classes from EN 50600 are designed for the description of physical security as it can be implemented for the protection of rooms. If one intends to protect equipment in unusual areas providing special conditions, as trains or tracks, more individual solutions are required. These can be found by analyzing the individual case, consulting specialized standards as depicted in Tab. 1 and combining those mechanical housings and technical systems that are feasible and result in a protection corresponding to the assigned ToA.

5 Conclusion

Physical security measures shall always be part of a holistic security concept; this applies in particular for critical infrastructures. Depending on the individual assets and the particular conditions of their location, different explicit measures shall be taken. A useful tool for choosing the right set of security measures is the Type of Attack(er) that characterizes the attacker a system shall be resistant against. It represents a holistic approach as it allows for taking all aspects of security into joint consideration. In particular, the joint effect of IT security (IEC 62443) and physical security (EN 50600) can be analyzed in this way. In future, our approach may be used to find appropriate sets of protective measures for various specific applications. Furthermore, additional aspects of security may still be added explicitly and links to associated standards could be found.

Bibliography

[DIN-04] DIN VDE V 0831-104: Electric signalling systems for railways – Part 104: IT Security Guideline based on IEC 62443

[EN03] EN 1303: Building hardware – Cylinders for locks – Requirements and test methods, European standard, 2015

[EN-1] EN 50600-1: Information technology – Data centre facilities and infrastructures – Part 1: General concepts, European standard, 2012.

[EN2-5] EN 50600-2-5: Information technology – Data centre facilities and infrastructures – Part 2-5: Security systems, European standard, 2016.

[EN27] EN 1627: Pedestrian doorsets, windows, curtain walling, grilles and shutters – Burglar resistance – Requirements and classification, European standard, 2011.

[EN30] EN 1630: Pedestrian doorsets, windows, curtain walling, grilles and shutters – Burglar resistance – Test method for the determination of resistance to manual burglary attempts, European standard, 2016.

[IEC2-4] IEC 62443-2-4: Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers, international standard, 2015.

[IEC3-3] IEC 62443-3-3: Security for industrial automation and control systems – Part 3-3: System security requirements and security levels, international standard, 2015.

[ISO01] ISO/IEC 27001: Information Technology – Security Techniques – Information security management systems – Requirements, international standard, 2013.

[Ko16] Kobes, Pierre: Leitfaden Industrial Security, IEC 62443 einfach erklärt. VDE Verlag, 2016.

[NE-4d] NERC Standard CIP-006-4d – Cyber Security – Physical Security of Critical Cyber Assets, 2013.[VdS07] VdS 2007: Informationstechnologies (IT-Anlagen) – Gefahren und Schutzmaßnahmen, Publikation der deutschen Versicherer (GDV e.V.) zur Schadenverhütung, 2016.

[VdS33] VdS 2333: Sicherungsrichtlinien für Geschäft und Betriebe, VdS-Sicherungsrichtlinien, 2014.