Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 571

3D Modeling of Selected Assets, Security Zones and Conduits

Simon Seibt[1], Karl Waedt[2], Hans Delfs[3], Simon Odorfer[4]

Abstract: Current critical industrial infrastructure (CII) which uses industrial automation and control systems (IACS) can be a target of cyber-attacks or combined cyber-physical attacks. To ensure the security of the CII, international standards are gradually evolving. The IEC 62443-x-x series is a specialized multipart security standard for IACS. It introduces, among others, the concept of security zones and security conduits [IE09]. The security zones can be defined in a physical sense and for logical grouping. By applying the defense-in-depth concept, both definitions are relevant. The development of a realistic three-dimensional (3D) model of CII can support the subdivision for the zoning and further security analyses. The model includes the locations of security relevant physical assets, which can be grouped into security zones and linked with related security artefacts. By using a 3D model, all relevant two-dimensional views can be derived. This paper addresses the use of a 3D model to support the application of security controls and risk assessments in line with concepts elaborated by IEC 62443-4-2 [IE15].

Keywords: cybersecurity, industrial automation and control systems, physical assets, application security controls, security zones, security conduits

1 Introduction

Industrial automation platform developers and system integrators are gradually deploying commercial-off-the-shelf (COTS) technology for industrial automation and control systems (IACS) while still using legacy components that were initially designed for autarkic use only. This may cause increased vulnerabilities for cyber-attacks against the IACS equipment. The IT technology was initially developed for business systems for their daily processes and is usually not sufficiently robust or the legacy systems were designed for use in a different context. International organizations and committees have already responded to the increased threat level [St14]. Standards relating to the IT Security for control and safety systems are gradually released. Several parts of the multipart security standard IEC 62443 for IACS are already published. Key concepts of the IEC 62443 are Foundational Requirements (FR), System Requirements (SR),

[1] Nuremberg Institute of Technology, Department of Computer Science, Keßlerplatz 12, 90489 Nuremberg, seibtsi47063@th-nuernberg.de
[2] Areva GmbH, Overall & Safety I&C Engineering / Cybersecurity, Henri-Dunant-Str. 50, 91058 Erlangen, karl.waedt@areva.com
[3] Nuremberg Institute of Technology, Department of Computer Science, Keßlerplatz 12, 90489 Nuremberg, hans.delfs@th-nuernberg.de
[4] Nuremberg Institute of Technology, Department of Computer Science, Keßlerplatz 12, 90489 Nuremberg, odorfersi57887@th-nuernberg.de

Component Requirements (CR) and Requirement Enhancements (RE) [IE15]. As compared to generic information security standards, like ISO/IEC 27001/2 [II13a] [II13b], the concepts go along with a grading according to 4 Security Levels (SL) [IE13] and a comprehensive concept of security zones and security conduits.

The identification of physical security zones in a factory or plant or more generic for critical industrial infrastructures (CCI) may be difficult as the physical assets are often distributed over dozens to hundreds of rooms in different buildings on one or multiple sites. Three-dimensional (3D) models are increasingly used, for example to simulate facilities for test purposes or for virtual commissioning. The development of a 3D model can also support the definition of security zones, assignment of security controls as well as security risk analysis. The 3D model represents a hierarchical structure of the CII, which can be used to group the physical assets into correspondent security zones and to assign physical security controls and network interface security controls at the respective position in the model. These security controls, or more precisely Application Security Controls, as will be explained later, are linked to the refined security requirements and the corresponding reference of the security standard in order to assure the correct implementation. The links are bidirectional. Thus, a security auditor will also be able to navigate from the requirements to the security controls, which themselves can be associated to physical assets represented in a 3D model. Later on, these serve as one basis of the risk assessment, e.g. the extraction of attack trees and the prioritized analysis of paths of an attack tree [Wa16].

2 Principle and granularity of the 3D modeling

To model the physical properties of a CII together with the security relevant assets, a hierarchical structure for the 3D modeling is needed. The hierarchical structure is based on a graph of nodes with parent-child relationships. Each node can have an array of children but only one parent. A child of a node can be a single 3D object or another node, which includes further 3D objects or nodes. The structure is composed gradually and begins with the modeling of individual physical assets.

Note: Modeling of complex interrelationships is also an approach currently followed as part of Industry 4.0 in Germany [BM40] and similar approaches in other countries.

Note: The following figures show a part of a power plant as an example of a hierarchical structure. This example contains extreme simplifications and does not correspond to the reality.

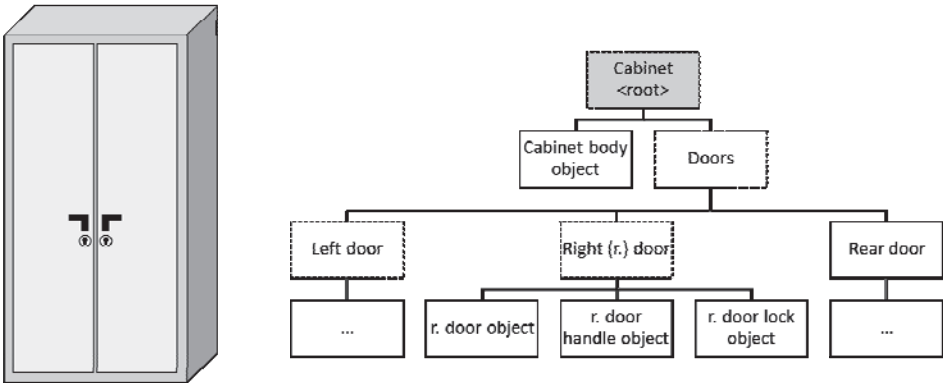

Fig. 1: Artefacts of an instrumentation and control cabinet

Fig. 1 shows an instrumentation and control (I&C) cabinet, which is an example of a security relevant asset. By modeling this cabinet, the root node is the "cabinet" element as indicated in Fig. 1. This node is linked to two children. One of them is a 3D object, which represent the body of the cabinet. The body is a modified standard cube mesh. The other child is another node with "Doors" as its name. This node groups the three door elements, two of which are positioned in the front of the cabinet and one at the rear of the cabinet (not visible in the 2D view at the left hand side of the figure). Each of the three door elements is a node that consists of a door object, a door handle object and a door lock object as part of the 3D mesh. These three downstream elements are simplified in this example because the elements could also be nodes, which further 3D objects. The door lock object is an example of security control (security counter measure) against unauthorized access to the cabinet.

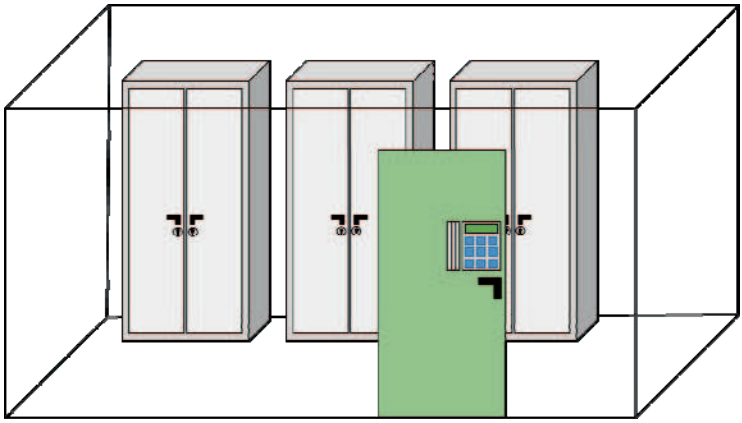

Fig. 2: Artefacts of an instrumentation and control room

In Fig. 2 the hierarchical structure is traced to the room level. The room is an example for an I&C room and consists of three cabinets that were modeled earlier. Furthermore,

the room has a door that also features an access control as a security counter measure. This access control could be a smart card reader with an additional PIN.

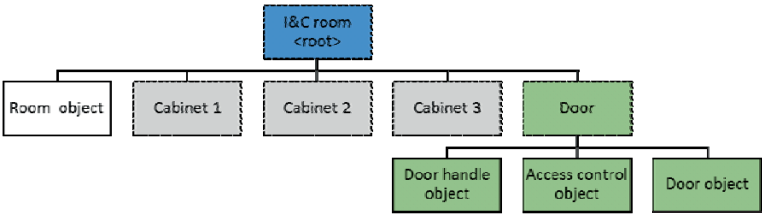

Fig. 3: Room level hierarchical representation of securiy relevant artefacts

By modeling this room, the root node is set to the “I&C room” as indicated in Fig. 3. This node consists of four other nodes and a 3D object, which is the “Room object”. The cabinet, which was grouped as a node, is tripled to new unique nodes in a child relation to the “I&C room”. The access-protected door is also another node with three child objects.

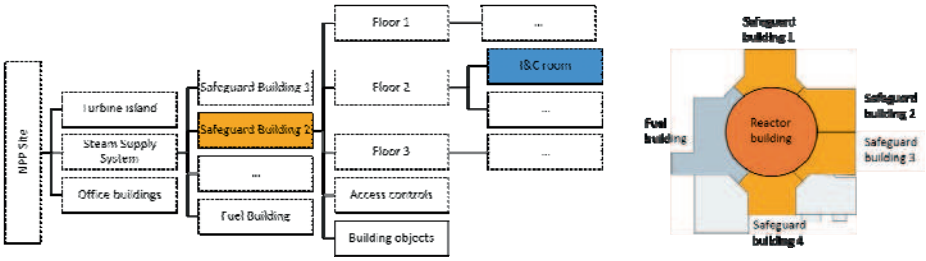

Fig. 4: Plant level hierarchical representation of security relevant artefacts

The next step is to expand the hierarchical structure to the buildings level or if there are more security relevant floors, each floor has to be modeled separately first. For this example, only floor 2 is considered as a relevant part. So the root node is set to “Safeguard Building 2”, as indicated in Fig. 4. To complete the safeguard building model, the procedure is the same as the modeling of the “I&C room” or the relevant assets.

By finishing the 3D model of a Power Plant with the introduced procedure, a scene graph with a hierarchical structure is created. This graph can be used to place security controls at their effective positions and to group the graph into security zones.

3 Application Security Controls

The security relevant assets should be protected by security controls such as physical entry controls or access controls. By modeling the assets, the security controls can be placed at their effective positions. The security controls describe measures to prevent an attack, detect an attack or initiate corrections/mitigations after an attack [WD15]. To assure that all security controls are correctly implemented, the security controls are linked to the description and implementation guidance from IEC 62443-x-x and ISO/IEC 27002:2013 [Wa16]. Another link can also be set to the initial requirements. Thus e.g. a RE according to IEC 62443-4-2 may be to have two authentication means. A further project-specific guidance may be to have iris scanners as additional access controls for each main security zone. From the Security Controls depicted in the 3D model it will be possible to navigate to the respective source requirements. However, this is beyond the focus of this paper. Furthermore, by using this linking method, weak points can be early identified on this level and potential physical intruder paths can be discovered by attack trees [WD15].

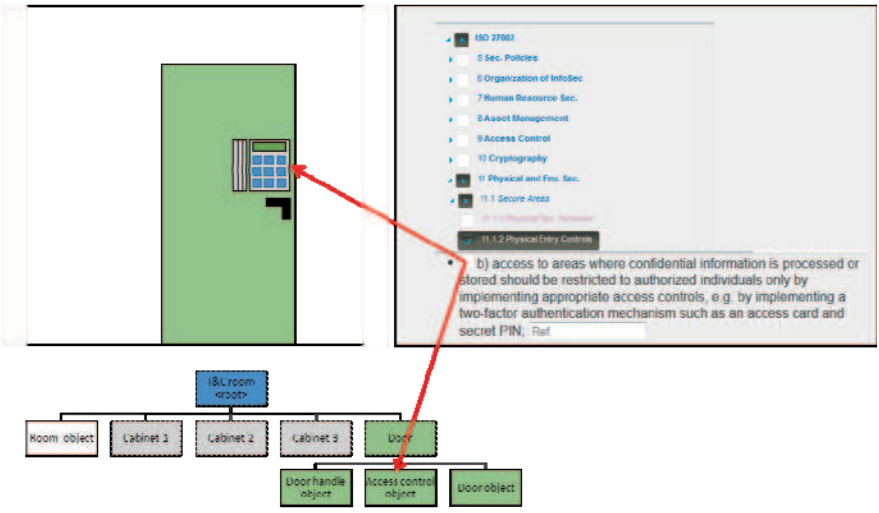

Fig. 5: Linking security controls

Fig. 5 shows an example for the security controls linking. The smart card reader with an additional PIN, which is a child object of the “Door” node, can be linked to the description and implementation guidance of the physical entry controls section of the ISO/IEC 27002:2013. The smart card reader can be used with cryptographic smart cards. The DES is a symmetric-key encryption and the RSA is a public-key cryptography [DK15]. Both methods are mostley used for the cryptographic smart cards. These smart cards can also be linked to cryptograpic controls section of the ISO/IEC 27002:2013 to assure the correct implementation.

The general security standards like ISO/IEC 27002:2013 are structured hierarchically with different levels of detail. This can be modeled as XML tags or as JSON objects. Each section of the standard should get a unique ID for the linking. The file format for the 3D models is typically also based on XML or JSON. By modeling the 3D models with a scene graph, each object also get a unique ID for the identification.

To get a relation between the 3D object and the corresponding section of the standard, the Application Security Controls (ASCs) [II11] can be applied. The ASC is a data structure, which contain a precise enumeration and description of a security activity and its associated verification measurement to be performed at a specific point [II15]. An ASC data structure can also be created as XML tag or JSON object in a separate file or later in a database for each project or corresponding 3D model.

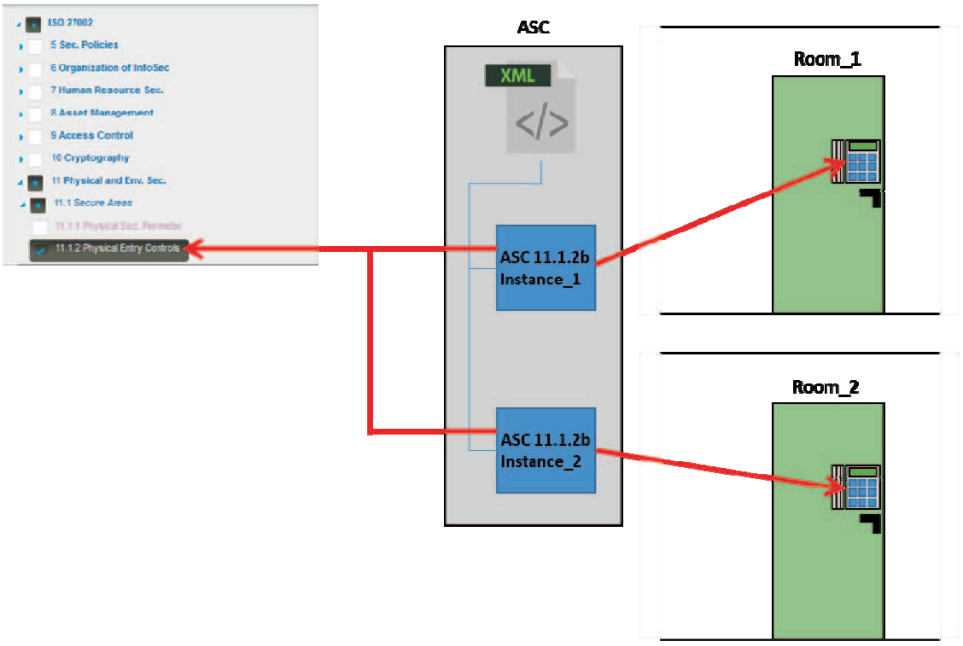

Fig. 6: Linking with ASC instances

Fig. 6 shows an example for a separate XML file with two ASC instances. For each security control linking, a new instance of the XML tag of the ASC is needed. In the example, two doors with their smart card reader as access control are indicated. The access control objects must be linked with the same corresponding section of the security controls standard (or guidance according to which the security controls are structured). Therefore, two instances of the ASC are needed. Each ASC also features additional information for the correct implementation of the security control. The listing example (Listing 1.) below shows a XML tag entry of an ASC.

```
<ASC ASC_ID="ASC_11_1_2_b_Instance_1">
        <ThreeDimensionalObject>
                <ID>AccessControl01_Door01_Room01</ID>
                <Filename>I C Room Scene</Filename>
        </ThreeDimensionalObject>
        <Standard>
                <ID>ISO_27002_11_1_2_b</ID>
                <Filename>ISO_27002</Filename>
        </Standard>
        <VerificationProcedure>...</VerificationProcedure>
        <SecurityTestCases>...</SecurityTestCases>
        <SecurityTestProcedure>...</SecurityTestProcedure>
        <Accountable>...</Accountable>
        <Responsible>...</Responsible>
        <Consulted>...</Consulted>
        <Informed>...</Informed>
        <ANF>...</ANF>
        <SecurityLevel>...</SecurityLevel>
        <SecurityZone>...</SecurityZone>
</ASC>
```

Listing 1: ASC instance as XML tag

Each ASC instance is also assigned a unique ID, which is a property of the start tag. The ID and Filename (or later file-path) of the 3D object and the corresponding section of the standard is integrated in a sub-tag of the ASC tag. After these entries, the additional ASC details are listed as own tags.

For example, the “SecurityTestCases” tag include different scenarios or use cases, which the security auditor wants to consider during the audit of the ASC. The tags “Responsible”, “Accountable”, “Consulted” and “Informed” base on the RACI model to store the role-based information of the involved persons. Furthermore, a link to the respective securtiy zone can also be stored in the ASC instance.

While the concepts of Organization Normative Framework (ONF) and Application Normative Framework (ANF) [II15] will not be further evaluated here, the above example already indicates, that for complex industrial facilities, it is beneficial to use semi-formalized definitions of Application Security Controls (ASCs). Thus, interrelations between ASCs as well as links between ASCs and modeled objects become possible, together with commercial project relevant role assignments, activity planning and activity tracking, like the scheduling of security test activities and the currently achieved progress.

4 Security Zones and Security Conduits

Security Zones and Security Conduits are introduced as key concept in the IEC 62443-x-x. The zones can be defined in a physical sense and for logical grouping. By developing of a 3D model of a critical industrial infrastructure, multiple cybersecurity related activities are supported, starting from the Security by Design up to the virtual inspections. As part of the Security by Design, the security zones can be defined by navigating through the 3D model and by assigning the physical 3D container objects to Security Levels, e.g. SL1 to SL4 according to IEC 62443. Thus, the physical composition of Security Zones is defined.

Similarly, the logical Security Zones are defined starting from the business needs (business domains) and the network architecture. Note: This second part of logical definition of Security Zones as well as the combination of Physical Security Zones and Logical Security Zones is not addressed in this document.

Security Zones provide an effective means to design and provide Application Security Controls that are applicable to all assets contained in the respective Security Zone. At the modeling level and the (XML/ JSON) data representation level, this is similar to the inheritance of security controls to all assets in a Security Zone.

Beyond supporting an efficient representation (with less redundant repetitions), this also supports the effective demonstration of compliance with regulatory requirements, e.g. on how a requested Security Level is achieved by the contribution of multiple Application Security Controls, that are either inherited or explicitly assigned to the evaluated primary or supporting assets.

Security Zones can also support dynamic security analyses. As part of a security risk assessment scenario it can be assumed that one of the predefined threat agents is located in a specific Physical Security Zone. Based on the assumed threat agent characteristics, like general IT skills, general knowledge level of process engineering, knowledge level of automation platforms, knowledge of the specific configuration of the targeted industrial process, knowledge of security vulnerabilities etc., the threat agent may be able to traverse along different branches of an attack tree. The ability to traverse a path in an attack tree will not be only according to the treat agent capabilities but also according to the strength of the implemented application security controls.

In many cases, the strength of the application security controls can be assessed by security tests, like penetration and fuzz tests. Based on the detail of the 3D specification of cybersecurity relevant assets and artefacts, the benefit of cybersecurity tests expressed as expected effort to potential impact ratio can be prioritized. Note: “Smart” (as model based) cybersecurity testing is part of a joint project (SMARTEST) by multiple German universities, partially sponsored by the German Ministry BMWi. The primary focus of the modeling for the cybersecurity testing is on the modeling of network protocols and state machines of the automation devices which allow more targeted attacks. However,

information from these behavioral models can be linked to the 3D and 2D models addressed in this document (e.g. link from an industrial network protocol model to a Security Conduit).

5 Conclusion

For complex industrial facilities, 3D modeling can effectively support multiple security activities, starting from the Security by Design up to the support of security audits. The 3D representation serves as unique source for deriving multiple 2D views. Traditionally, multiple 2D perspectives are used that may become inconsistent after manually modifying one 2D view. Nevertheless, objects in the 3D scenes can be linked to objects in unique (source) 2D representations, e.g. of network architectures. Similarly, objects in 3D scenes, can be linked to objects in unique 2D representations, e.g. a physical network interface card port in a 3D view of a network switch located in an electronics cabinet can be linked to the respective connection point in a 2D network architecture diagram.

Equipment from 3D representations of supporting automation and IT assets (e.g. a processing unit) can be linked to other 3D physical equipment, e.g. pumps, valves, smart sensors or actuation equipment which may be supporting or primary assets. While this is not elaborated in the current paper, it is a key step for evaluating the potential (graded) impact of a threat agent to the primary assets (e.g. a chemical process).

Summing up, this paper showed some modeling approaches that support the graded security levels, zones and conduits concepts of IEC 62443 in general and more specifically the risk assessment approaches being developed in IEC 62443-4-2. As indicated, several extensions have to be explored in order to make full benefit of the potential provided by an intuitive, semi-formal and, extensible modeling.

6 References

[BM40] BMWi: IT-Sicherheit für die Industrie 4.0 - Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten - Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, 2016.

[DK15] Delfs, H.; Knebel H.: Introduction to Cryptography: Principles and Applications, 3rd ed., Springer, 2015.

[IE09] IEC 62443-1-1:2009 Security for industrial automation and control systems – Part 1-1: Terminology, concepts and models, 2009.

[IE15] IEC 62443-4-2:2015 [Draft] Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components, 2015.

[IE13] IEC 62443-3-3:2013, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels, 2013.

[II13a] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements, 2013.

[II13b] ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls, 2013.

[II11] ISO/IEC 27034-1:2011, Information technology - Security techniques - Application security - Overview and concepts, 2011

[II15] ISO/IEC 27034-2:2015, Information technology - Security techniques - Application security - Organisation normative framework, 2015.

[St14] Störtkuhl, T.: IT-Sicherheit auf Basis IEC 62443 für elektrische Signalanlagen, Signal + Draht 10/2014, 10-12, 2014.

[Wa16] Waedt, K.; Parekh, M; Tong X.; Gao, Y.; Ding, Y.; Xie, X.: Nuclear Safety and Risk-based Cybersecurity Testing, 47th Annual Meeting on Nuclear Technology, Hamburg, 2016.

[WD15] Waedt, K.; Ding, Y.: IT Security / Interoperability, 1st Sino-German Intelligent Manufacturing/Industry 4.0 Standardization International Summit Forum (SGSF), Shanghai, 2015.