Human-Centered Design and User Experience, Vol. 114, 2023, 313–321
https://doi.org/10.54941/ahfe1004249

Human-Centric Introduction to a Complex Cybersecurity Standard

Jan Eißler, Marko Schuba, Tim Höner, Sacha Hack, and Georg Neugebauer

FH Aachen University of Applied Sciences, Aachen, 52066, Germany

ABSTRACT

Industrial automation and control systems (IACS) operate in complex and increasingly networked environments of industrial plants. Due to the increasing number of cyberattacks, these systems are also exposed to the growing threat of being attacked. IACS are often found in critical infrastructure such as power supply or water treatment plants, as well as in industry, so their compromise can result in devastating consequences. To prevent this, the IEC-62443 series of standards was developed to address the cybersecurity of IACS. In order to achieve cybersecurity in accordance with the IEC-62443 standard, the human factor plays a major role, as it is humans that need to implement and manage the cybersecurity controls. To help those users to get started and gain a basic understanding of important IEC-62443 concepts such as zones and conduits, defense in depth, and security levels, this paper defines an experience-based practical approach to train users w.r.t. application and implementation of the standard.

Keywords: Cybersecurity, Industrial automation and control systems, IEC-62443, Competence, Training, Human factor

INTRODUCTION

Industrial automation and control systems (IACS) operate in complex and increasingly networked environments. Due to the increasing number of cyberattacks, these systems are also exposed to the growing threat of being attacked. One of the main roles in the security of these systems is played by humans. It is through them that equipment and systems are planned, installed, configured and maintained. IACS are often found in critical infrastructure such as power supply and water treatment plants, as well as in industry. A compromise of these systems can have devastating consequences. IEC-62443 was developed to address this threat situation (Franceschett, 2019).

IEC-62443 is a series of standards dealing with the security of IACS. It provides support to organizations and businesses to design and operate secure, networked IACS. Its aim is to ensure the availability, integrity and confidentiality of these systems and to reduce the risks of sensitive information being compromised, equipment (software or hardware) being damaged or the environment being destructed (Franceschett, 2019).

IEC-62443 builds on other IT security standards, such as the ISO/IEC 27000 family of standards, but also addresses the specific requirements and differences of IACS. IACS differ from IT systems because they interact

strongly with their physical environment (Colbert, 2016). Therefore, the IEC-62443 standard includes the potential threat from cyberattacks to life and the environment in a risk assessment phase. It also focuses on the availability of IACS by ensuring that security controls do not result in the impairment of essential functions and emergency processes. Another special feature of IACS is their long lifetime of sometimes more than 20 years (Colbert, 2016). This fact requires special handling of these systems, as the systems themselves or their cybersecurity controls may have vulnerabilities and thus could be easily attacked (Franceschett, 2019).

With the help of the procedures described in the standard, system integrators and operators of industrial plants can ensure that their systems meet the required security requirements or they can identify controls to achieve this goal (Franceschett, 2019).

The implementation of the IEC-62443 standard is done by humans. How these controls are implemented plays a decisive role for security and safety of the entire plant and company. In the underlying work of this paper, an environment is created in which people can practically implement and test the central points of the standard. This is to create a better understanding of the concepts and to identify and correct errors in real implementations.

Basic Concepts of IEC-62443

The IEC-62443 standard defines several basic concepts that are used for security assessment and security improvement. These are, among others:

- Defense in depth
- Least privilege
- Security levels
- Security requirements
- Zones and conduits

Defense in Depth

Defense in depth is a procedure in IT security in which several different defense controls are used to protect a system infrastructure. An attacker must overcome all controls one by one in order to cause damage. Ideally, controls are chosen in such a way that possible vulnerabilities of one control are mitigated by a subsequent control. A mature defense in depth architecture can prevent a large part of the often automated attacks (Cleghorn, 2013).

Least Privilege

A fundamental principle of IT security is the principle of least privilege. It states that a user of a system only receives authorization for the actions that they must perform within the scope of their work. Authorizations that go beyond this are withdrawn from the user. This principle can be enforced by a default deny policy. Only explicitly assigned authorizations are granted, all other actions are not permitted.

Security Levels

A basic tool for assessing the security of systems in the IEC-62443 standard is the use of security levels. The standard defines five security levels (SLs 0, 1, 2, 3, and 4) (IEC 62443-1-1, 2016).

- SL 0: No specific requirements or security protection necessary
- SL 1: Protection against casual or coincidental violation
- SL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation
- SL 3: Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
- SL 4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Security Requirements

To determine the level of security of a system, the standard defines seven foundational requirements (IEC 62443-1-1, 2016). These requirements are

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability

These requirements are used to check which security level a system achieves when applying the standard (IEC 62443-1-1, 2016).

Zones and Conduits

Different components have different acceptable risks and their security requirements differ accordingly. To map these different requirements, the concept of zones exists. Components with the same security requirements are grouped together and thus allow the bundled application of security controls (ISA 62443-1-1, 2016). Attackers often try to bring systems that can be easily compromised under their control and then move laterally, i.e., they compromise further systems in the same network and thus expand their foothold (NSA, 2022). Segmenting the network into zones makes it much more difficult to move laterally, as, e.g., firewalls prevent the attacker to directly attack a system (NSA, 2022).

Zones can be physical or logical. Physical zones group components based on their physical location. Logical zones, on the other hand, group components based on logical factors such as their function, affiliation to a network, etc (ISA 62443-1-1, 2016).

Zones can also be part of other zones to support the concept of defense in depth. In addition, zones can be classified as trusted or untrusted (ISA 62443-1-1, 2016).

Conduits exist for grouping and controlling the communication flows with components in other zones. Examples for conduits area network cables or multiple connections over different communication paths (ISA 62443-1-1, 2016).

Practical Environment

In the practical environment, the user, who is to be trained in the implementation of the standard, needs to apply the presented concepts himself. For this purpose, an initially unsecured network shall be separated into zones and conduits according to the IEC-62443 standard. In addition, security controls shall be introduced to minimize threats.

In the unsecured network – the training starting point – each device is simulated using a virtual machine (VM). The simulated devices and applications are similar to typical systems that occur in a real company network. The respective network architecture is depicted in Figure 1.

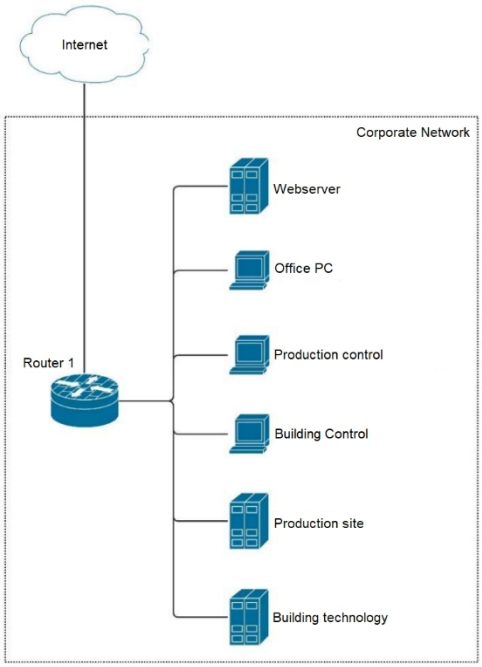

Figure 1: Initial network that needs to be secured.

The VMs simulate the following applications:

1. Router 1 - The only router in the network, which has a firewall and allows the devices to access the Internet.
2. Webserver - Web server that is publicly available on the Internet and provides a website. It is assumed that the company's Internet presence and an online shop are operated via this.
3. Office-PC - A computer used for general office tasks. In addition, this system can be used as an operator terminal for production control and

building automation. Users can access the VMs production control and building control via remote desktop connection. It is assumed that this option will be used to store production data, enter control commands or perform other activities directly from the workstation.

4. Production Control – A computer that controls the production plant. A control software is installed on this system, which communicates via Modbus protocol with a Modbus simulation software installed on the VM production plant (Modbus is a widely used protocol in industrial plants). The control software corresponds to the role of the client in the Modbus protocol.
5. Building Control - A computer that used for administration of a BACnet building network (BACnet is a protocol used frequently in building automation systems). A control software is installed on this VM, which communicates via BACnet protocol with the simulation software on the VM building technology. In the BACnet protocol, the control software corresponds to the role of the client.
6. Production Plant - This system simulates a programmable logic controller (PLC) to which a production plant is connected. The PLC is simulated by software that can be addressed via the Modbus protocol. This software corresponds to the role of the server in the Modbus protocol. Software on the VM production control is used for sending control commands to the plant. The production plant can be run safely even without a connection to this control software.
7. Building technology - This VM simulates sensors and actuators in the building automation technology network. For this purpose, a simulation software is used which simulates two rooms with temperature sensors and air conditioning systems. This software can be addressed via the BACnet protocol. In the BACnet protocol, this software takes on the role of the server. The building technology can also be run without a connection to the control software.

In the initial state, the devices only have basic security features such as a simple, password-based user authentication with default login data and preset firewall rules that allow all outgoing connections. Incoming connections from the Internet are only possible to the VM web server. Within the network, communication is not restricted.

Training Tasks for the User

In order to complete the training, the user must edit this initial state according to the basic concepts presented to secure the example network.

Introduction of Zones and Conduits

The standard IEC-62443-3-2 defines a process for dividing a system into zones and conduits (IEC 62443-3-2, 2016). This process consists of four steps, which must be carried out for all existing devices or systems.

1. Identification of the "system under consideration" (SuC). In this step, the system or group of systems to be considered is determined.

2. Risk analysis of the SuC. In this step, a detailed risk analysis of the previously selected system is carried out. A risk is the combination of the probability that a particular threat will exploit a particular vulnerability and its impact. To assess the risk a so-called risk matrix is used. Each company is encouraged to design their own risk matrix, as the effects in particular, for example, the loss of reputation or business, are very individual and cannot be quantified in general. In the context of this paper, the participants of this practical task work with the matrix included in the standard. In this matrix, the effects are divided into four categories, low, medium, high, critical, whereby the classification refers to the percentage of financial damage in relation to the annual turnover of the company. The probability of occurrence is determined with the help of the security levels of the standard and divided into four categories.
   The matrix can be used to risk assess the individual systems.
3. Division into zones and conduits. The division of assets into zones and conduits is a central concept of the IEC-62443 standard to increase security in IACS environments. Assets are grouped based on risk assessment results, common security requirements, location, or other characteristics. Organizations need to determine individually which criteria they find useful (IEC 62443-3-2, 2016). The aim of grouping is to find commonalities in the security requirements of the assets and to identify controls that can fulfil these common security requirements. This allows an individual security level to be set for each zone, as the same level of security does not need to be achieved everywhere. Zones that are less security-critical can be given a lower security level accordingly. This reduces the effort and thus also the costs for the implementation and operation of security controls (IEC 62443-3-2, 2016).
4. Documentation of the zone properties. Each of the zones and conduits created and their properties must be documented. IEC-62443-3-2 specifies which points should be included in the documentation. In the context of this paper, properties that cannot be defined due to the virtual simulation environment are excluded, e.g., physical access to zones. In addition, the conduits are represented by the firewalls at the router interfaces. Therefore, the conduits are already represented by the logical access points of the zones. However, in a practical application of the standard, these properties should be part of the documentation (IEC 62443-3-2, 2016).

Detailed Cybersecurity Risk Assessment

In a next step a detailed cybersecurity risk assessment must be carried out for each zone. The aim of this detailed risk assessment is the exact identification of the risk that exists for the systems within the zone. This assessment is carried out in twelve steps, which are defined in the standard. Subsequently, it must be assessed whether the controls introduced have reduced the risk to an acceptable level. If this is not the case, a new iteration of the risk assessment with subsequent definition of controls must be carried out (IEC 62443-3-2, 2016).

Countermeasures in the Practice Environment

The defined controls of the last steps should also be implemented in the practical environment by the participants. This enables a deeper dive into the necessary steps in the implementation of the standard. The controls are directly related to the IEC-62443 system requirements (SR) which are specific technical requirements linked to a higher level foundational requirement. Security controls that are to be implemented by the participants are as follows

1. Establish separate user accounts with minimal permissions. Each user account can be assigned to a person in order to give the system the ability to uniquely identify and authenticate human users according to SR 1.1 RE 1 (IEC 62443-3-3, 2020). In order to apply the principle of least privilege, each account is given the minimum permissions necessary to function.
2. Introduction of strong credentials. Requirement SR 1.7 - Authenticator management requires the enforcement of a certain complexity in the assignment of passwords in terms of minimum length and diversity of their characters, furthermore, passwords must not correspond to user names. In the practical environment, the operating systems used are configured to enforce these properties when assigning passwords.
3. Restriction of allowed connections. Zone boundary protection requires the ability of the system to monitor and control communication at the zone boundaries (IEC 62443-3-3, 2020). This ensures that only those connections are allowed that are necessary for the system to function. All other connections are prevented or rejected.
4. Authentication when establishing a connection. In addition to human users, software processes must also authenticate themselves. This ensures that only authorized connections can be established. Together with encryption of a connection, this control offers protection against spoofing (manipulated identities) and man in the middle attacks (for message sniffing and manipulation). (BSI) (IEC 62443-3-3, 2020).
5. Encryption of the communication. It must be ensured that the integrity of the transmitted information is protected. Therefore, the connections of the practical environment need to be encrypted.
6. Reduce feedback on failed login attempts. The control software on one of the systems provides unnecessary information about the reasons for failed login attempts. This data needs to be suppressed (IEC 62443-3-3, 2020).
7. Limitation of the number of failed login attempts. The number of consecutive failed login attempts via the control software on the production control device needs to be limited (IEC 62443-3-3, 2020).
8. Display of a notice of use. A notice of use concerning the rights and obligations associated with the use needs to be displayed before registration (IEC 62443-3-3, 2020).

Final State of the Practical Environment

After carrying out the steps described above, the network should look similar to the one shown in Figure 2:

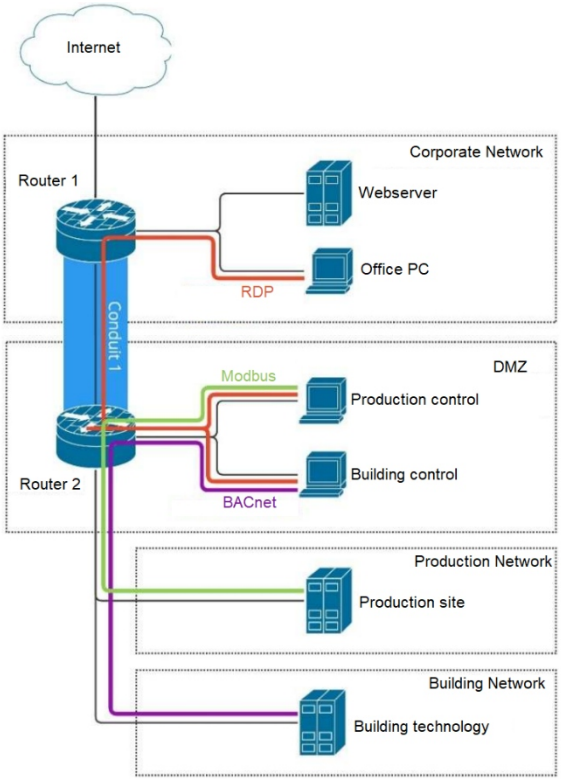

Figure 2: Optimized network including zones, conduits, and security controls.

Through the users' changes to the network, an increase in security according to IEC-62443 could be achieved. Attacks that were successful in the initial network can no longer be carried out in the optimized network. Such attacks should be tested by training participants before and after applying the security changes to further enhance the learning experience.

CONCLUSION

For a successful implementation of the cybersecurity standard IEC-62443, the human factor, i.e., the competence to implement the complex standard is crucial. In this paper, the application of the IEC-62443 standard was carried out on a virtual network as a training example for technical personnel responsible for cybersecurity in an industrial environment. For this purpose, the steps described in the document IEC-62443-3-2 were used to determine the risks of the network and to identify and implement security controls. In this context, the concepts of zones and conduits, security levels and defense in depth were explained and applied to practical examples.

With the help of practical implementation, training participants can try out the technical implementation of the standard independently and based on experience. By dealing with the central concepts of the standard and their real-life manifestations, the standard becomes more tangible.

REFERENCES

A. L. Franceschett, P. R. A. de Souza, F. L. Pereira de Barros und V. R. de Carvalho (2019), A Holistic Approach - How to Achieve the State-of-art in Cybersecurity for a Secondary Distribution Automation Energy System Applying the IEC 62443 Standard.

BSI - Bundesamt für Sicherheit in der Informationstechnik, "IT-Grundschutz-Kompendium."

E. J. M. Colbert und A. W. Kott (2016), Cyber-security of SCADA and other industrial control systems (Advances in information security 66).

IEC 62443-1-1: Models and Concepts, International Society of Automation (2016).

IEC 62443-3-2 (2016): Security risk assessment for system design, International Society of Automation.

IEC 62443-3-3: System security requirements and security levels (2020).

L. Cleghorn (2013), "Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth.

NSA - National Security Agency (Dec 2022) National Security Agency Cybersecurity Technical Report: Network Infrastructure Security Guide.