NATIONAL ELEVATOR INDUSTRY, INC.

Elevator and Escalator Industry Cybersecurity Best Practices

Provided by the National Elevator Industry, Inc. (NEII)

This guideline was originally written and produced by NEII's Cybersecurity Committee, which includes cybersecurity and codes experts from NEII member companies. Thank you to these experts and the other experts from Europe, the Pacific Asia Lift and Escalator Association (PALEA) and the China Elevator Association (CEA) for their support and expertise.

Issued: April 1, 2019

The July 1, 2020 revision reflects further updates based on input received from other technical experts, including Symantec, A Division of Broadcom. Thank you to all of the experts for their support and expertise.

Revised: July 1, 2020

NEII's commitment to improving cybersecurity defenses for elevator and escalator cybersecurity control systems is essential to aiding manufacturers in the designing of systems that protect against network based cyber-attacks.

- Symantec, A Division of Broadcom

Elevator & Escalator Industry Cybersecurity Best Practices

Table Contents

1 Preface

This guideline is to address best practices for elevator and escalator cybersecurity when the conveyance has the potential to be connected to untrusted systems or the internet.

2 Introduction

Cybersecurity protection for elevators and escalators has become a necessity. At one time isolated, building conveyances have become an integrated part of complex modern building systems with multiple controllers and processors, remote interaction systems accessing the internet, wireless communication to general purpose computers and mobile device-based service tools. Elevators and

escalators have also become enriched with new user enhancements and features, a key component in emergency situations with voice, real-time in-car video displays and complex interaction with fire and life safety systems for building evacuation situations. The ability to deliver real-time data to service personnel as well as software updates on demand electronically is the norm. While connectivity takes elevators and escalators to new levels in availability, efficiency and general building safety, it also presents exposures to the world of cyber threats such as denial of service attacks.

3 Scope

This guideline provides a path to aid elevator and escalator manufacturers in designing their products that provide a measured protection and management against network based cyber-attacks. The objective of this guideline is to focus on the interfaces between the elevator or escalator and the Internet, building area networks and untrusted systems. Portable maintenance and service tools used by technicians are included and should be evaluated as an untrusted system. The approach is to use industry best practices as the guidance for national norms, standards (e.g. ASME A17.1/CSA B44), and regulations relevant to the elevator and escalator industry. This document focuses on the role of the manufacturer and maintenance provider of elevator and escalator equipment and not on the manufacturer's customers, partners, general service providers or the roles of those who may have other responsibilities regarding cybersecurity and/or the interfaces with the manufacturers, nor a complete ecosystem's end to end cybersecurity view.

3.1 Definitions

3.1.1. Terms defined in this document

Asset:	Anything with a perceived or actual value to the organization. This Includes physical asset such as a piece of equipment.
Conduit:	The channel through which components in a system communicate with each other. Note: future potential standardization work may consider alternative definitions such as [IEC/TS 62443-1-1 3.2.27] including notes.
Defense in depth:	The notion of applying multiple defense mechanisms/controls rather than relying on a single mechanism/control. Note: future potential standardization work may consider alternative definitions such as [IEC/TS 62433-1-1 3.2.40] including notes or explanations such as described in [NSA].
Product:	Elevator system or escalator system and all associated subsystems and services provided by the manufacturer.
Security control:	Specific processes and installation and organization controls that need to be implemented to keep up the overall cybersecurity health of the system. They include, but are not limited to, periodic security audits, continuous security monitoring and incident management processes.
Security level:	Analogous to SIL levels used in safety, security levels denote the level of protection against unauthorized or bad actors with increasing complexity Note: future potential standardization work may consider alternative definitions such as [IETC/TS 62443-3-3 3.1.38] including notes.
Security measure:	Specific techniques that have been implemented to meet specific product technical requirements. These include use of state-of-the-art authentication protocols, cryptographic routines of encryption, session keys, secure boot, code signing, firewall settings, etc.

Security zone: A set of component(s) in a system architecture that can be assumed to co-exist in a secure manner; the components however that communicate outside of the zone and corresponding conduits are not considered secure.
Note: future potential standardization work may consider alternative definitions such as [IEC/TS 62443-1-1 3.2.117] including notes.

Trusted zone: A security zone as per above.

3.1.2 Abbreviations

BMS:	Building Management System
DDS:	Destination Dispatching System
EMS:	Elevator/escalator Management System
F&LS:	Fire and Life Safety System
IACS:	Industrial Automation and Control System(s)
IT:	Information Technology
MRL:	Machine room-less elevator
OT:	Operational Technology
PSTN:	Public Switched Telephone Network
SPOF:	Single Point of Failure
SuC:	System under Consideration

3.2 Architectures Considered

The guideline is targeted primarily at interface points where the elevator or escalator has communications with the Internet, building area networks and untrusted entities. While the guide addresses interface points to other systems, best practices should also consider communications between internal functions. Figure 1, Figure 2 and Figure 3 depict some typical examples of elevator system architectures and the parts of the control system at risk; these examples apply equally to escalator control systems. These are examples and hence should not be construed as actual implementations or exhaustive. Interfaces from the examples include:

- Connection points that interface to the internet either physically or wirelessly;
- Connection points that interface to a physical or wireless building network;
- Serial communication interface to Fire and Life Safety (F&LS) system (physically isolated wire interfaces are exempt);
- Connection points to intelligent service tools, wired or wireless;
- Intelligent service tools themselves (e.g. PCs);
- Trapped passenger alarm system if it can accept downloaded software or elevator interaction; and
- Communication links that connect outside the elevator and escalator.

Note that in the above list:

- Serial communication links and trapped passenger alarm systems can typically be considered part of a trusted zone.
- Communication links are represented in this document as conduits.
- Interfaces will be considered endpoints on any termination point of the conduits.

3.3 Examples of Trusted Zones

The trusted portions of the system are not considered in this guideline, and they are depicted by the semi-transparent green areas in Figures 1, 2, and 3 below. While a cybersecurity architecture should consider a layered approach in the trusted zones, this topic will be deferred to a more comprehensive standard. It should also be noted that most systems will contain multiple trusted zones. As a reminder from 3.2 each conduit is terminated by endpoints which are the interfaces under consideration in the scope of this document.

Figure 1

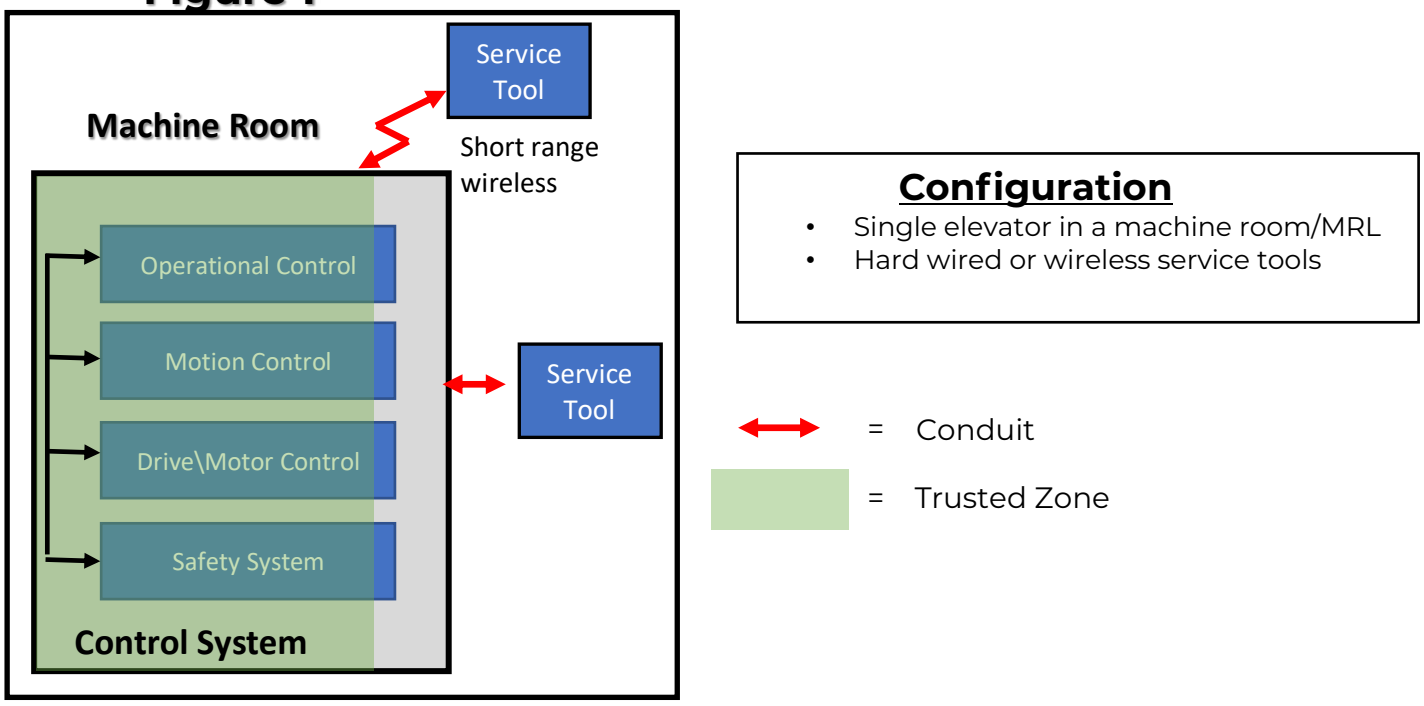
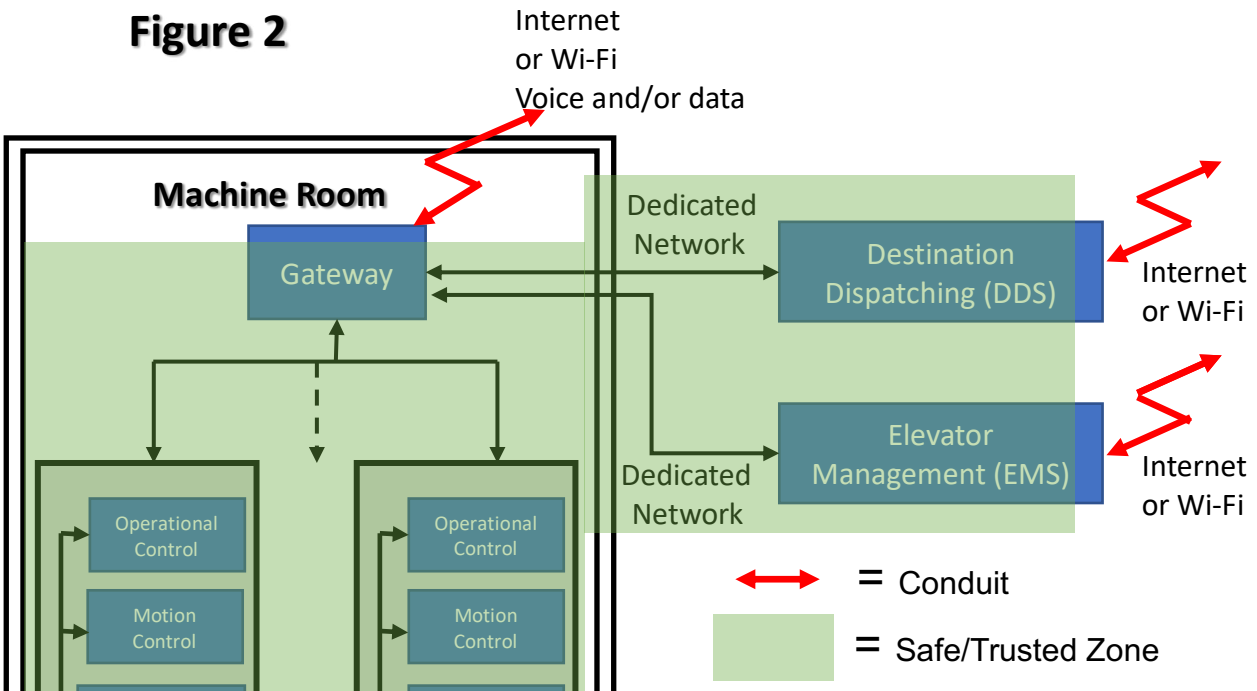


Figure 1 is a single elevator installation, with short range wireless communications to service tools.

Figure 2



Configuration

- Single or multiple elevators in a machine room / MRLs
- Remote interaction or gateway voice and data communication out of the machine room
- Hard connect or wireless service tools
- DDS on dedicated wired network
- EMS on a dedicated wired network
- Communication dedicated wired to a "untrusted system"
- DDS and/or EMS communicate out of the building

Figure 2 is a more complex installation in which the destination system and the management systems communicate over a network via a gateway which interacts with a backend system. In this example, a backend system refers to different kinds of servers, databases, and other infrastructural elements typically not on site that provide additional compute power and storage for the products. It can be instantiated in different ways, including on-prem and Cloud, public and private.

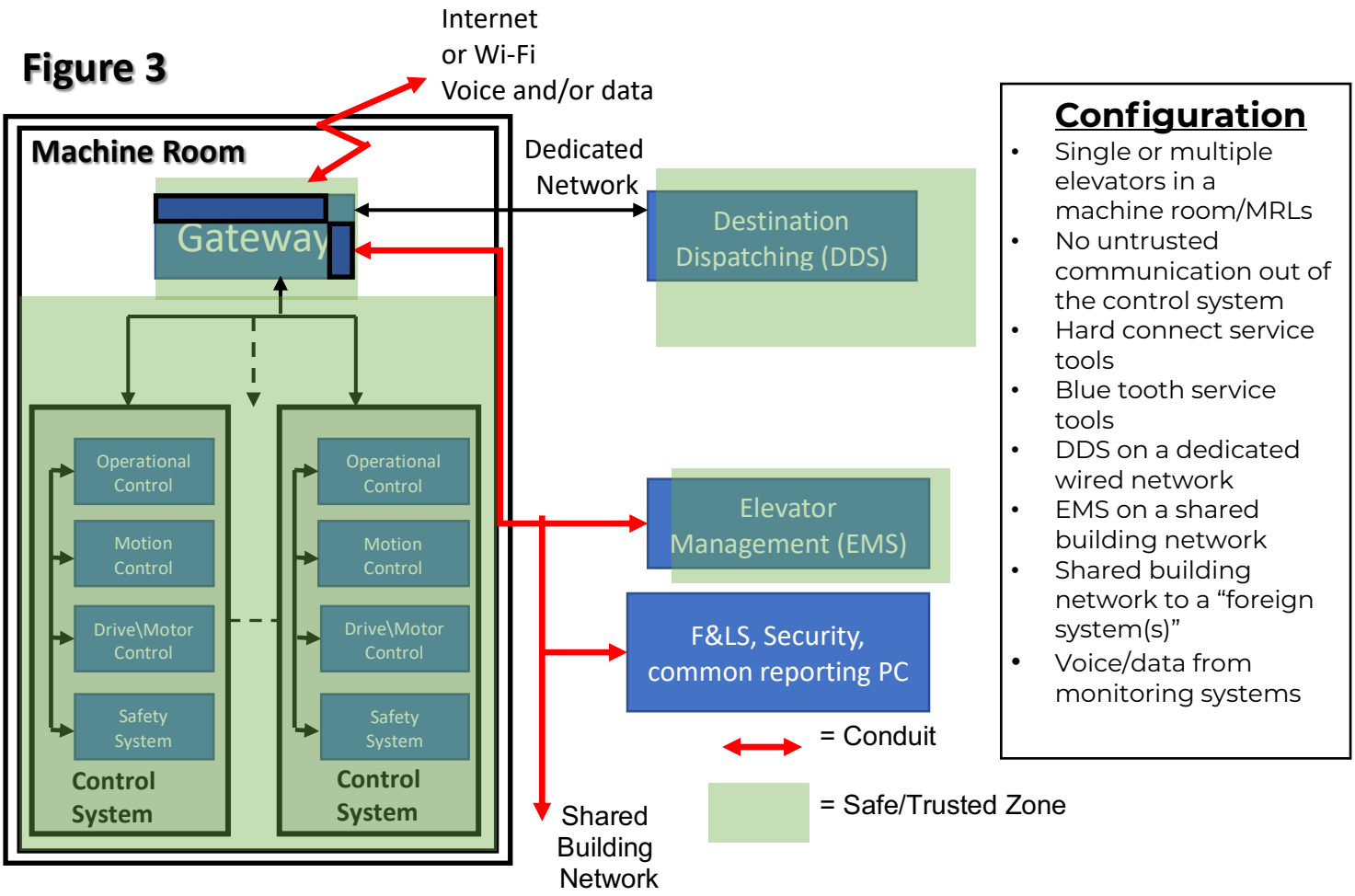


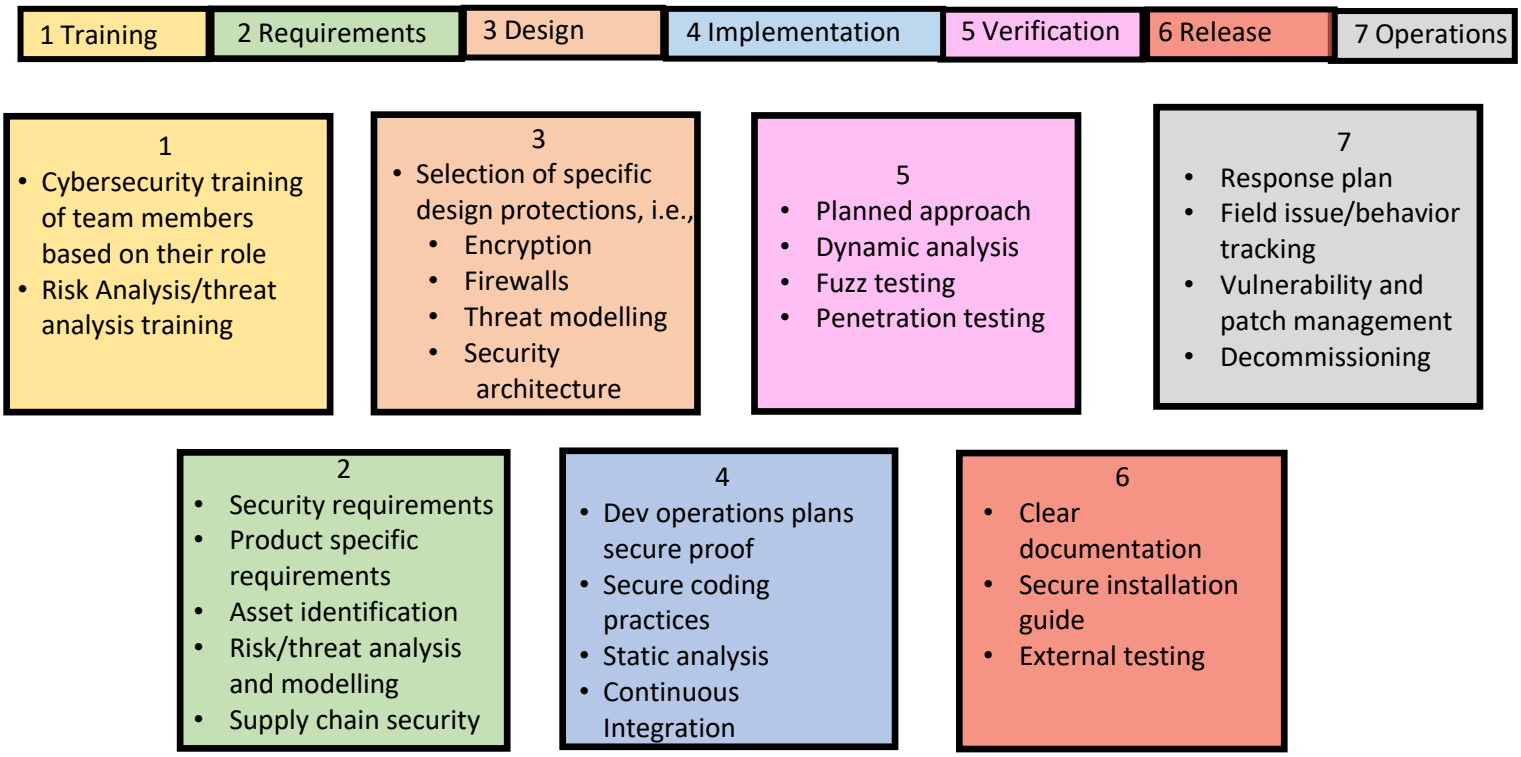
Figure 3 covers the case of an untrusted building network and the connection of the elevator and escalator system to other building systems such as a Fire & Life Safety System or a Physical Access Control system.

4 Cybersecurity Process Life Cycle

The fundamental recommendation of this guideline is a strong cybersecurity process lifecycle. This lifecycle needs the manufacturer to commit adequate training, tools, resources, and processes to harden and maintain the elevator and escalator from cyber-attacks. The lifecycle approach is also a fundamental premise of best practices utilized for all cybersecurity standards and approaches.

The lifecycle approach recommended is shown below and contains seven (7) distinct functions. These seven functions are then further described in following sections and are to be considered in a cybersecurity plan, no matter how many steps they are combined in.

Steps



4.1 Training

Each employee participating in the cybersecurity lifecycle requires adequate training to ensure an appropriate level of security of an elevator or escalator installation. This includes but is not limited to developers, line and upper management, maintenance staff, and procurement.

Cybersecurity training of the relevant employees should be tailored to their role and give general information as well as role-specific expertise not necessarily required by other parties. For example, all employees participating in the cybersecurity lifecycle need to generally understand what cybersecurity is about, what the current best practices are and how to apply them and understand the product to be secured as well as the risks induced by cybersecurity threats. It is recommended that the training team includes cybersecurity specialists or subject matter experts (SMEs).

The specific training might differ significantly by role. While developers require the expertise on how to implement functionality securely (see also Section 4.3 Design) and should be trained so they know the relevant best practices for their respective tasks, elevator and escalator maintenance staff requires another kind of training. They should primarily understand the reasons for dealing with cybersecurity and be trained to maintain the security of an installation by following given policies.
As in normal IT security, upper management needs to understand how important cybersecurity is for elevator and escalator installations and should support all efforts by establishing and maintaining an industrial security lifecycle process and allocate the resources necessary to get the cybersecurity resilience of installations to a reasonable level.

In addition to the above-mentioned cybersecurity training it is also essential that the team performing the risk or threat analysis has up-to-date knowledge about the relevant standards, such as ISO 14798, and is able to work according to the relevant best practices.

4.2 Requirements

4.2.1 Introduction

The process of managing cybersecurity requirements of an elevator and escalator is effectively a process of managing risk.

To achieve a product with an acceptable level of security, it is necessary to create a set of meaningful measures and controls, which mitigate the various risk events threatening the elevator and escalator.

Since identifying assets and gathering possible security risks is a creative and cooperative process, seeking professional external support (e.g., for the facilitation of workshops) might be a valuable addition when no internal expertise is available.

Like in the hazard and risk analysis of functional safety, it is essential to form a diverse team for the risk analysis. By combining the different perspectives on the subject to be assessed, the lists of both the identified threats and risks will eventually become increasingly complete.

Cybersecurity requirements for an elevator and escalator can be divided in two categories:

1. **Baseline security requirements.** These are the best practice security measures that the organization should apply to all systems. Part 6 of this guideline gives a proposed baseline of requirements. Requirements should consider the multi-dimensional requirements for equipment that the target system will be interfaced with.
2. **System-specific security requirements.** When designing new systems or when analyzing security of existing systems, risk-threat analysis should be done to identify threats to the system and countermeasures for the threats should be defined. The security should not solely rely on implementing a baseline of controls (although in some cases, the baseline can be determined to be adequate).

4.2.2 Requirements Process

The following process should be followed for determining the security requirements:

- Identify assets and the level of tolerable risk for both
  - Systems, software, supply chain etc., and
  - Information
- Initial risk assessment:
  - Identify threats and risks to the assets.
  - Determine likelihood and impact of risk events.
  - Determine unmitigated cybersecurity risk.
  - Define security level target for the system.
- Create Initial set of cybersecurity requirements.
- Further iteration of risk assessment:
  - Evaluate existing countermeasures.
  - Reevaluate likelihood and impact of risk events.
  - Determine residual risk.
- Document complete cybersecurity requirements, assumptions, and constraints.

The risk assessment should be updated every time that changes are made to the system or when the threat landscape changes significantly (e.g., new software vulnerabilities are published) and based on test results.

Guidelines to each step of the requirements process follow.

4.2.3 Identification of Assets and Systems under Consideration

- Assets should be identified to know which parts of the system should be protected, or in other words, which parts justify the additional cost of securing them.
- Everything that has a perceived or actual value to the organization is an asset from a security perspective. The assets might be logical, physical objects or information. Examples include availability of service, safety of passengers and service personnel, and the integrity of the safety system.
- It might be necessary to identify additional assets which are present in the specific System under Consideration (SuC).
- For elevator and escalator systems, the safety of passengers and service technicians should be considered as a protected asset, and take precedence over other protection aspects. Security measures should not adversely affect the safe functioning of the elevator and escalator system.
- During asset identification, the level of tolerable risk should be determined. What is considered tolerable depends on the organization and local regulation and societal values such as is the elevator or escalator system installed in a low-risk residential building or installed in a hospital or embassy. Assumptions have to be made about the typical use of the elevator or escalator systems if a generic risk assessment is required.

4.2.4 Initial risk assessment

- During risk assessment, risk events/threats which threaten the assets should be identified.
- Initial risk assessment begins with the identification of the risks without any mitigating measures in place.
- Security threats for elevators and escalators include, but are not limited to:
  - Exploitation of vulnerabilities due to software errors
  - Malware, such as worms and viruses via the network, transportable media (e.g. USB sticks), and via temporary connections (e.g. service tools)
  - Unauthorized access
  - Unauthorized actions by employees or by others
  - Unintended employee actions
  - Denial of service attacks
  - Botnets (e.g. Mirai)
  - Targeted attacks
  - Social engineering (see [IEC 62443-1.1 5.6.5.3.6])
- Additional input for possible threats is given in NIST SP800-30, BSI Top 10, OWASP Top 10, CAPEC, MITRE ATT&CK for IT and for Industrial Control Systems (ICS) (see References) or other threat catalogs, which are kept up-to-date and are distributed by several relevant organizations.
- To assess the probability of the threat events occurring, the assessment should consider the capability and intent/motivation of the adversary and the vulnerabilities that exist in the system, in particular but not limited to:
  - Adversary capability: How skilled and well-resourced is the adversary?
  - Adversary intent: Is the adversary specifically targeting your organization or is the adversary just looking for an arbitrary system to exploit?
  - System vulnerabilities and accessibility:
    Is the system exposed over the Internet or is it operated in closed network (e.g. internal elevator and escalator control system network)?
    Are there any inherent single points of failures (SPOF) in the architecture of the assets themselves introduced by the architecture of the security solution?
    Is the new architecture showing any residual risks, e.g., new single point of failure (see [IEC 62443-1-1] 5.6.4.2 second clause)?

- A security risk assessment can be challenging when compared to a hazard and risk analysis of functional safety. There is not only one dimension of risk (harm to persons or the system), but rather several are possible. Depending on the specific risk event, the consequences may be:
    - Passenger or service technician injury, e.g. by unexpected motion of the elevator or door drives;
    - Elevator and escalator availability or degradation of transportation capacity;
    - Bypassing of access control, e.g. gaining unauthorized access to a floor; and/or
    - Loss of company assets, e.g. losing intellectual property or internal knowledge.
- When assessing risk to elevator and escalator, the probability and severity may be mapped against ISO 14798:2009 (See Table 4a and 4b) and the risk categories of that standard may be used.

Other risk mapping methods are acceptable if done methodically. Additional guidance regarding the conduct of a risk or threat assessment can be found in IEC 62443-3-2, ISO 27005 and NIST SP 800-30, Guide for Conducting Risk Assessment.

Table 4a – Example of risk probability aligned with ISO 14798:2009

Level of probability	Probability per system	Description of adversary capability and intent vs. system vulnerability
A — Highly probable	Likely to occur frequently in the life cycle	System is exposed over the network and security controls are not implemented and not planned; exploitable by a casual attacker with limited resources and expertise.
B — Probable	Likely to occur several times in the life cycle	System is exposed over the network, minimal security controls are implemented and minimally effective; exploit requires low resources, expertise, and motivation.
C — Occasional	Likely to occur at least once in the life cycle	System is exposed over the network, security controls are partially implemented and somewhat effective; exploit requires moderate resources, elevator or escalator system specific skills and moderate motivation.
D — Remote	Unlikely, but may possibly occur in the life cycle	System is exposed over the network, security controls are mostly implemented and effective; exploit requires significant resources, elevator or escalator system specific skills and high motivation.
E — Improbable	Very unlikely to occur in the life cycle	System is exposed over the network, security controls are fully implemented and effective; exploitation requires a very sophisticated level of expertise, significant resources, high motivation and coordination.
F — Highly improbable	Probability cannot be distinguished from zero	No concern, security controls or other measures fully implemented, assessed, and effective.
• Lower the probability by one category if the system is operated in closed network. • Lower the probability by two categories if the system is operated in a physically secure location and only accessible in that location.		

Table 4b – Example of risk severity aligned with ISO 14798:2009

Level of severity	Impact on safety, system, or environment	Impact on service availability (to users)	Impact on information (to operator)
1 - High	Death, system loss, or severe environmental damage		
2 - Medium	Severe injury or major system or environmental damage		
3 - Low	Minor injury or minor system damage	Service disruption (e.g. elevator and escalators out of use when no alternate means of transport or loss of access control) [A, B]	Data integrity compromised (e.g. elevator and escalator management system data tampered with) [A, B]
4 - Negligible	Does not result in injury or system or environmental damage	Minor service disruption (e.g. transport capacity reduced) [A ,B]	Loss of non-critical data (e.g. elevator and escalator management system data)[A, B]
A Raise the severity by one category if the impact is to multiple sites. B Raise the severity by two categories if the impact country-wide/global.			

- As a result of the initial risk analysis, the unmitigated risk to assets has been determined. Based on an appropriate risk matrix, it should be determined what risks require additional mitigation.
- While the risk matrix of ISO 14798-2009 might be utilized for this purpose, other risk assessment processes (e.g. IEC 62442-3-2, ISO27005 or NIST SP800-30) also can be utilized.
- Security levels that are targeted to mitigate the risks are described in Section 5.

4.2.5 Selection of Security Requirements

- After the initial risk assessment, meaningful countermeasures have to be chosen in order to mitigate the assessed risks exceeding the previously defined acceptable level of risk.
- A commonly used best practice when creating/choosing countermeasures is the so called “defense in depth” approach. Depending on the risk, countermeasures should not rely on a single line of defense but utilize multiple layers of protection. If one line of defense breaks, the asset is still defended by at least another layer.
- Defense in depth is agnostic towards IT or OT.
- In general, some of the countermeasures that can be relevant to these guidelines consist of
  - Embedded device security such as secure boot, etc.
  - Identity and Access solutions to manage authentication and authorization measures
  - Endpoint security solutions to harden and protect both ends of the communication (controllers, gateways, maintenance equipment and tools, and any backend models)
  - Network security solutions to secure communications
  - Information security solutions to protect data and data leakage
  - Other security solutions, e.g., platform (and cloud) as per US-CERT
- For those countermeasures to be efficiently used and introduced in the overall design, they may rely on some or all the below conditions:
  - Good architectural best practices (appropriate architecture documentation at least at general and detailed level including flow diagrams, allowing attack surface minimization, layering, decrease of architecture SPOF, etc.)
  - Good operational best practices (appropriate patching strategy, planning and implementation, working managed backup and validated restore capabilities, monitoring, etc.)

    - Well trained cybersecurity staff that may work from a Product Security Incident Response (PSIRT) for product matters and Cyber Security Incident Response Team (CSIRT) for anything else (see US-CERT ICS Incident Response Capability)
    - Security Playbooks prepared by the above staff
    - Integration of security capabilities between the zones should be encouraged
    - Security orchestration may be required
- Considering the above, defense in depth application of countermeasures for elevators and escalators would apply as follows:
    - Embedded security should be applied from design to operations in the trusted zone
    - Identity and Access solutions consistently apply to each trusted zone, conduit, backend and maintenance operations
    - Endpoint security (in particular hardening) applies to any device at the interface to the conduit which includes
        - Gateways and controllers in the trusted zone
        - Maintenance equipment and connected devices (service tools)
        - Backend solutions may be required for some implementations (see US-CERT)
    - Network security solutions apply to conduits that are connecting to the backend systems.
    - Information security solutions apply consistently to what the risk management assessment for information has highlighted more likely to be in backend systems.
- Compensating countermeasures, such as physical access control or detective controls, may also be used to satisfy one or more security requirements.
- Service tools, including portable tools that are used for servicing elevators or escalators, should employ effective security measures. Service tools can broadly be put into the four following conduit types:
    - Those that can communicate with the elevator and escalator remotely from anywhere on the Internet;
    - Those that can communicate with the elevator and escalator remotely from a trusted backend system;
    - Those that are based on low/moderate range proximity wireless technologies such as Wi-Fi and Bluetooth; and
    - Those that require physical presence close to the equipment and a cable/wire to be plugged in such as USB or serial cable.
- Good cybersecurity practices involve a defense indepth strategy that implements multiple security measures based on the level of accessibility to the device and the potential impact if the system is compromised. In this regard, the accessibility in the above four cases would require different types of security controls depending on the extent of system control that is capable through the service tools.

4.2.6 Further Iterations of Risk Assessment

- Each further iteration of risk assessment is carried out like the initial one, but under the assumption that the previously chosen countermeasures are in place.
- Check that the previously defined countermeasures mitigate the identified cybersecurity risks to the level previously defined as acceptable. Check also if the countermeasures introduce new security threats (e.g. denial of service or a new attack surface).
- If not, add additional countermeasures/mitigations and repeat the evaluation of the risks in question.
- If assessing an existing product, at the end of the risk assessment the required mitigations are identified to minimize the risks identified during the initial assessment.

4.2.7 Documentation of Cybersecurity Requirements, Assumptions and Constraints

Cybersecurity requirements should be documented and contain all technical security measures in the form of requirements which have to be implemented during development. The requirements should be traceable as mitigations to the previously identified security risks. The cybersecurity requirements should also be tracked and at the end of the development verified and validated like all other requirements.

4.2.8 Externally Developed Component Security

The methods described above should also be extended to components developed by external sources, whether they are commercial off-the-shelf (COTS) software, open source software (OSS), or components specifically developed for the company.

- No matter how thorough the risk assessment, the selection of countermeasures, and the security concept is, it can be jeopardized by insecure elements among the externally developed components.
- Best practices include audits of the suppliers, only buying from reliable suppliers and only outsourcing to trustworthy service providers and demanding contractual assurance of processes to be adhered to.
- Further information can be found in ISO/IEC 27036-3 and IEC 62443-2-4 which gives examples of what you could demand from your suppliers/service providers from a security perspective.

In parallel to the development of the system's architecture and the assignment of its functionality, it is good practice to review and update the base threat modelling. Several approaches are practicable, e.g., Microsoft's STRIDE approach. This methodology answers the question "what can go wrong with my system?" by systematically screening each component of your system for the possibility of:

- Spoofing -- pretending a false identity
- Tampering -- the unauthorized modification of data or a system
- Repudiation -- obfuscating one's responsibility for an action
- Information disclosure -- the unauthorized disclosure of valuable data
- Denial of service -- reducing the availability of a service to possibly zero
- Elevation of privileges -- gaining higher privileges than intended by exploiting a design flaw or vulnerability

If the threat model is kept up to date with the evolving architecture of the system, a comprehensive catalogue of possible threats is available. Its threats can then be mitigated by choosing appropriate countermeasures, which can be incorporated into the next iteration of the system's architecture.

4.3 Design

The goal of the design phase is the development of the system's architecture. In this phase, all decisions regarding the high-level design choices and key components to be used are made. Furthermore, during this development of the architecture, the product's complete functionality should be outlined to the degree necessary in order to achieve an architecture which fits to the required functionality. This outline could, for example, consist of the involved entities, the resulting flow of data and important security or non-security properties already assignable.

Due to the far-reaching effects of the choices made during the design phase, this phase is especially prone to the introduction of security vulnerabilities. Flaws in the developed architecture might lead directly or indirectly to vulnerabilities which might be hard to identify at this high-level stage, since they might be very specific or only recognizable on a much lower level.

Fixing these security issues is most efficient if identified as early as possible, preferably during the design phase. If security flaws are only discovered in later phases, such as during testing or operations, it becomes increasingly complex and expensive to deal with them. It is therefore very important to try to detect the vulnerabilities already in the design phase and use industry standard best practices for reducing the attack surface exposed.

Best practices include:

- The principle of least privilege, meaning a process or a user should by design not have higher privileges than necessary for the fulfillment of its task.
- Attack surface identification and minimization.
- Modular design methodology to reduce the impact of security threats.
- Defense in depth, meaning that no risk should be mitigated by a single measure but by a set of layered measures still effective if one of the individual measures fail (also described in the requirements phase).
- Restricting the access of a user, interfacing system or task to just the data which is required for the respective functionality.
- Preferring simple, proven, in use concepts or components over unnecessary complex, proprietary or inadequately tested ones.
- Performing security design reviews on a regular basis in order to detect security requirements that are not yet addressed by the present design and check whether the system's current architecture is in conformity with the best practices.

Additional information regarding security best practices in the design phase can be found in IEC 62443-4-1 Practice 3, NIST SP 800-82 Chapter 5, or in the BSI ICS Security Compendium Chapter 5.6.

4.4 Secure Coding Guidelines Implementation

At a minimum the following main attributes associated with secure implementation should be followed:

- The use of secure coding guidelines
- The use of static analysis tools
- Unit testing of critical functions
- Analysis of third party and open source software

The use of secure coding guidelines: In addition to good coding practices for different languages, the guidelines should list potentially exploitable coding constructs or designs that should not be used and these should be from real world examples. Typically, they should also include a list of banned/deprecated functions.

The use of static analysis tools: At a minimum, code that meets the following criteria should be analyzed using static code analysis tools:

- Code listening on or connecting to a network that may be connected outside the Trusted/Security Zone of the device, system or application under consideration.
  Code with prior vulnerabilities identified.
- Code executing with high privilege (for example SYSTEM, administrator, root) unless all code executes with high privilege. Code running with higher privileges should have valid reasons for doing so.
- Security related code module (for example, authentication, authorization, cryptographic and firewall code).
- Code that parses data structures from potentially untrusted sources.
- Setup code that set access controls or handles encryption keys or passwords.

All risks identified by the static analysis tool in violation of the coding standard should be mitigated unless the risk can be shown to be not relevant.

A best practice is to carry out continuous source code analysis during the development process, rather than towards the end of the code development phase. When developer's check-in the code, the code can be automatically analyzed for any possible security issues.

4.5 Verification, a Planned Approach

In addition to the normal testing and validation processes which are a part of product development, cybersecurity verification and test plans should be a formalized process in the product verification phase. The following key activities related to security are important:

Dynamic Analysis

- Dynamic analysis should be performed on the application to identify any memory corruption, race conditions, user privilege issues and any other critical security problems.

Fuzz Testing

- Fuzz Testing should be performed on all components that process data originating external to the security zone or component.
- A Fuzz Testing Plan should be created documenting the fuzz testing that will be done. The plan should include a list of all components that will be fuzzed, a description of how the fuzzing will be done, whether smart fuzzing or dumb fuzzing will be done, and the pass/fail criteria for the tests.

Penetration Testing

- In addition to the use of fuzz testing tools, various penetration testing tools are also recommended for use during testing. The test plan should have specific line items relating to the use of penetration testing tools.
- Independent (third party) penetration testing should be considered on a periodic basis.

Verify countermeasures of threat modeling findings are properly implemented

- Abuse case tests and known vulnerability testing should be performed on all components and attempt should be made to exploit all threats identified in the threat model that have been mitigated.
- Identify any attack surface not captured in threat modeling process.
- Results should be carefully documented.
- The effectiveness of the implemented security countermeasures should be verified through testing and the risk assessment should be updated based on test results.

Independent third-party analysis

- It is recommended that independent third-party security risk analysis and testing be carried out for high risk application. This analysis should be carried out by a company who is known to be skilled in performing such an analysis.

Red Teaming / Blue Teaming

- Red Teaming and Blue Teaming should be considered as appropriate testing methods to qualify the entire defense as planned by the best practices described in this document (see References on MITRE Cyber Exercise Playbook).

4.6 Release

The documentation listed below, and the risk acceptance are suggested deliverables to be completed before product release.

Documentation

- Threat Modeling and Risk Assessment
  The threat model with residual risks identified.

- Security Requirement and Secure Design
  The design document, identifying each security requirement and associated security control.

- Security Test Plan
  Testing Plan showing how each security control has been tested to ensure it meets the security requirement.

- Analysis Reports
  Reports summarizing the results of performed analyses and highlighting any found issues and insufficient security controls.
  - Third Party Code/Library Analysis Report
  - Dynamic Security Analysis Report
  - Static Code Analysis Report

- Test Reports
  - Fuzz Testing Report
  - Internal Penetration Testing Report
  - External Penetration Testing Report

- User Manual
  User documentation including user, operation, and maintenance manuals should be reviewed by relevant experts and should include a security guidance section for users and administrators, including actions and constraints that are necessary to prevent security breaches.

  Administrator guidance should include all administrator responsibilities necessary for secure operation of the product, including those related to assumptions regarding administrator behavior found in the statement of product security environment.

  If an Application Programming Interface (API) or set of classes or objects that developers can use to build applications is provided, security information and best practices should be provided for each applicable function or method call.

  The security guidance section in the user manual should contain procedures for reporting security vulnerabilities.

  Documentation should include the threat profile assumed in the design and the high level security functionality as relevant to the user, including authentication mechanisms, default policies for authentication and other functions, and any security protocols that are mandatory or optional.

- Secure Installation Guide

  Installation guidelines should list and explain all security configuration options present in the product and make note of their default and optional settings. By default, the installation should be secure so that the default configuration is considered secure without any additional configuration changes. All default passwords need to be removed.

Additionally, the installation manual should contain all field/external testing requirements to be performed before commissioning to create a secure installation.

- Incident Response Plan

  Documented procedures for structured reaction in case of an incident, including a responsible, accountable, consulted and informed (RACI) matrix with contact details (see also Section 4.8).

4.7 Threats to Equipment Operation

Threats to equipment operation require measures such as keeping track of all exposed hardware and software, monitoring of the installations, and response plans.

Evaluating the current risk of installations requires knowledge about all components that are possibly exposed to an attacker. This asset inventory includes hardware as well as software.

- Keep inventory and version control of hardware/software in use.
- Continuously monitor vulnerability databases and field issues
- If a vulnerability in a hardware or software asset is detected, it is necessary to analyze if the vulnerability has any impact to the asset.

If assets are affected by vulnerabilities, a further process for fixing the issue by either updating, replacing, mitigating or accepting the risk, for this vulnerability should be implemented. It would be advisable to use a scoring system to prioritize and assess any identified security issue.

4.8 Incident Response Plan

Written procedures, also called security playbooks, should be developed, tested and made available to execute the necessary next steps in case of an incident ("Incident Response Plan"). The response plan should contain the necessary information to deal with all kinds of conceivable incidents and is highly dependent on the specific assets.

Manufacturers will consider different aspects of the incident response plan for their products

At a minimum the response plan should contain the following:

- Contact details, responsibilities
- Asset components
- Place of installation, if applicable
- Predefined procedures

Additionally, the response plan could cover for example incidents such as

- Abnormal network traffic
- Unexpected shutdown due to a security breach
- Defacement of an elevator and escalator display
- Unavailability of any elevator/escalator service due to a denial of service attack

The manufacturer and maintenance provider should develop emergency procedures regarding the before mentioned and additional requirements. A process should be in place to properly maintain the response plans in case of changes or updates.

The company should also consider how to handle the decommissioning of the elevator or escalator since sensitive information might be stored on some components (e.g., IDs, credentials, parameter sets, etc.) which might be used maliciously or provide insight into the asset and other linked assets if disclosed. Erasing the information or destroying the asset physically might be necessary. Decommissioning of an asset should be reflected in the asset inventory.

FIRST defined both PSIRT and CSIRT as two good practices for manufacturers and maintenance providers to cover both incident response plan aspects of their product when delivered.

FIRST deliverables can be leveraged through its collaborative work with ISO (ISO 27035) and ITU[1].

- CISA for ICS as well noted that in Risk Management and Cybersecurity Governance to "develop and practice incident response procedures that join IT and OT response processes."
- US-CERT ICS Incident Response Capability recommends the framework of interlocking the OT side.

5 Levels of Security

As described in Section 4.2 of this guideline, the Security Level target of the system or component should be defined during risk assessment, and the achieved Security Level of the system or component should be verified through testing.

A review to verify the Security Level should also be redone during the lifecycle of the system when:

- Changes are made to the system;
- New vulnerabilities relevant to the system are detected;
- New security patches to the system components are published by vendors or the open source community; and/or
- Periodically, as determined by the organization's policy.

Security Levels (SL) can be described as the skill level and motivation of the attacker that the SL protects against:

SL 0: No specific requirements or security protection necessary

Through risk assessment, it has determined that the system does not require specific security requirements, for example, because consequences of misuse are determined to be negligible.

When assessing if a security level has been achieved, SL 0 can indicate that a subset of countermeasures for SL 1 have been implemented, but full SL 1 is not met.

SL 1: Protection against casual or coincidental violation

The system should be protected against casual attackers with low skills or against unintentional misuse. Protection requires a basic level of security controls to ensure confidentiality, integrity, and availability of data and to enforce authentication, authorization, and accounting of access. For example, security controls according to SL 1 do not require unique authentication of users and devices.

[1] This document is meant to be used globally, and as skills are a general issue, the ITU role can help support the interests of manufacturers as it is recognized for its capacity building.

A recommended set of controls for SL 1 is provided in the ISA/IEC 62443-3-3 Standard referenced in this guideline.

SL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation

The system should be protected against attackers that have tools and skills to misuse generic information technology systems, such as web-based applications, but do not have specific knowledge on elevator and escalator systems and are not specifically targeting these systems. The motivation of the attackers can be reputation gain, for example. As a difference to SL 1, protection according to SL 2 requires security controls that are implemented in a more granular manner. For example, users and devices should be authenticated uniquely.

A recommended set of controls for SL 2 is described in Part 6 of this guideline.

SL 3: Protection against intentional violation using sophisticated means with moderate resources, elevator and escalator system-specific skills and moderate motivation

The system should be protected against highly skilled attackers that are knowledgeable about security and elevator or escalator systems and who are specifically targeting those systems. An attacker going after a SL 3 system will likely be using attack vectors that have been customized for the specific target system. The motivation of the attackers may include blackmail, revenge (disgruntled former employee), or sabotage (industrial competitor).

Controls for SL 3 are out of scope of this guideline.

SL 4: Protection against intentional violation using sophisticated means with extended resources, elevator and escalator system-specific skills and high motivation

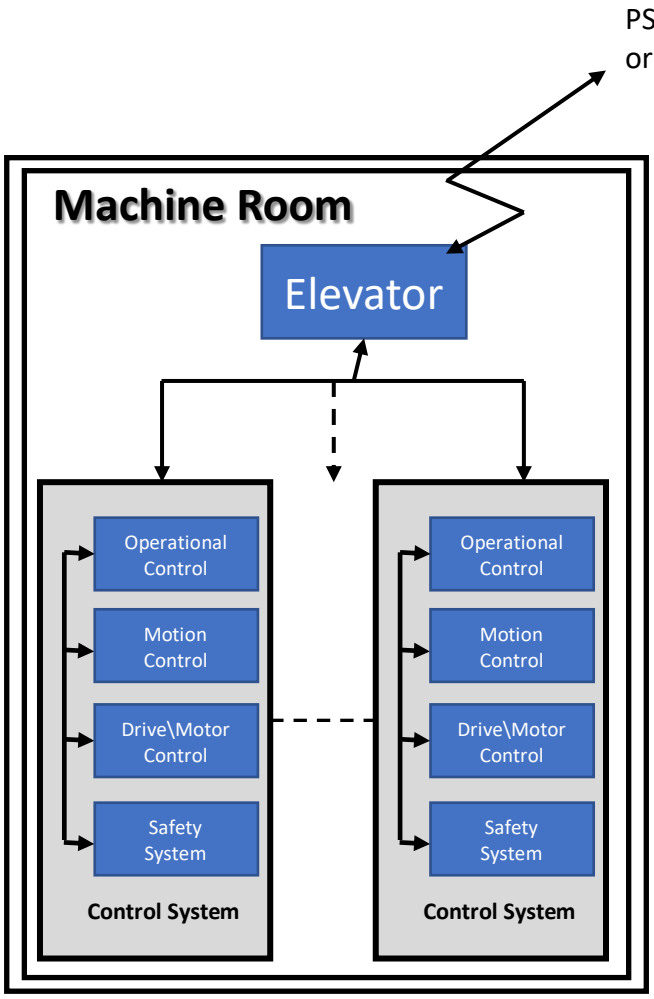
The system should be protected against highly skilled attackers that are knowledgeable about security and elevator or escalator systems and who are specifically targeting those systems with extended resources and high motivation. This is similar to SL 3, but with SL 4, the attacker is even more motivated and is prepared to spend extended periods of time and resources to plan and execute the attack.

Controls for SL 4 are out of scope of this guideline.

More detailed description of the Security Level process can be found in IEC 62443-3-3.

6 Example

The following example presents a simplified version of risk assessment and selection of security requirements for a remote interaction system integrated to the elevator control system.



Configuration

- Single elevator or a group of elevators.
- Elevator Remote interaction/Gateway communicating via the Internet.
- The Gateway is embedded in the control system.
- The elevator and escalator remote interaction system cannot modify the control system by design.
- 10,000 remote interaction systems deployed.

Requirement Process

1. Identify assets:
   Functions of the control system cannot be modified from the remote interaction system
   Integrity of the remote interaction system
   Integrity of the data sent by the remote interaction system
   Availability of the remote interaction system
2. Tolerable Risk
   Scalable attacks over the internet are not tolerable
   Local attacks with physical access do not need to be considered, as they only affect a single unit.
3. Initial risk assessment
   a. Identify threats and risks to the assets.
      i. Denial of service attack on the remote interaction system
      ii. Tampering with the data sent from the remote interaction system
      iii. Spoofing the endpoint for data sent from remote interaction system
      iv. Taking ownership of remote interaction system
      v. Attacking the control system through the remote interaction system
   b. Determine likelihood and impact (see Table 7.1 below).

See example presented below including in Tables 7.1 through Table 7.4.

Table 7.1 Threat and Risk Assessment before security controls are applied

Risk event	Probability	Impact	Note
i. Denial of service attack on the remote interaction system	A	4 (single), 3 (scalable)	Tools are commonly available to carry out DoS attacks and they occur frequently against systems exposed over the internet. Impact is likely to be negligible for single site as the temporary loss of remote interaction data is not serious.
ii. Tampering with the data sent from the remote interaction system	D	3 (single), 2 (scalable)	Modifying the data so that it is actually meaningful will require skills. If successful, the impact is low for single site, as a legitimate service need may go unnoticed leading indirectly to safety risk.
iii. Spoofing the endpoint for data sent from remote interaction system	B	3 (single), 2 (scalable)	Spoofing attack is easily carried out for unprotected communications. Theft of data will have low impact for single site.
iv. Taking ownership of remote interaction system	C	3 (single), 2 (scalable)	If the remote interaction system is unprotected, taking ownership will not be hard. However, remote interaction is not considered critical function so the impact will be low for single site.
v. Attacking the control system through the remote interaction system	E	2 (single), 1 (scalable)	Attacking the control system requires extensive skills even after the remote interaction system is breached. If attack is successful, impact can be medium on single site.

c. Determine unmitigated cybersecurity risk

As the remote interaction system will be connected over the Internet, scalable attacks are a valid concern. Thus, the risk assessment has to assume that the attacker can attack multiple sites at once.

Table 7.2: Risk heatmap before security controls are applied

Probability Level	Level of Severity			
	1 - High	2 - Medium	3 - Low	4 - Negligible
A – Highly probable			i	
B – Probable		iii		
C – Occassional		iv		
D – Remote		ii		
E – Improbable	v			
F – Highly improbable				

d. Define security level.
   Several of the risks are on unacceptable level. Thus, security measures are required to reduce the risk. For the purposes of the example, we select to implement Security Level 1 requirements according to IEC 62443-3-3. Security Level 1 should be adequate to block casual attackers.

e. Create security requirements.
   Out of SL 1 requirements, the following will mitigate the initial risk:

   i. 7.1 Denial of service protection
   ii. 3.1 Communication integrity
   iii. 3.1 Communication integrity, 4.1 Information confidentiality
   iv. 1.1 Identify and authenticate human users, 2.1 Authorization enforcement, 2.8 Auditable events, 3.4 Software and information integrity
   v. 5.2 Zone boundary protection, 5.4 Application partitioning

f. Further iteration of risk assessment.
   After applying Security Level 1, the risk assessment will be redone.

Table 7.3 Threat and Risk Assessment after security controls are applied

Risk event	Probability	Impact	Note on mitigation
i. Denial of service attack on the remote interaction system	C	4 (single), 3 (scalable)	Implementing DoS protection (e.g., packet filtering) will make successful attacks harder.
ii. Tampering with the data sent from the remote interaction system	E	3 (single), 2 (scalable)	Implementing communication integrity (e.g., using TLS) will make tampering attacks improbable, but not completely impossible as new and unknown vulnerabilities may appear. In addition, since TLS1.3 introduces a ban of passive/offline decrypt it is making debugging much harder.
iii. Spoofing the endpoint for data sent from remote interaction system	E	3 (single), 2 (scalable)	Implementing communication integrity and confidentiality (e.g., using TLS with mutual authentication) will make spoofing attacks improbable, but not completely impossible as new and unknown vulnerabilities may appear. In addition, since TLS1.3 introduces a ban of passive/offline decrypt it is making debugging much harder.
iv. Taking ownership of remote interaction system	E	3 (single), 2 (scalable)	Implementing authentication and accounting and auditing on the remote interaction system will make remote attack to take ownership improbable.
v. Attacking the control system through the remote interaction system	F	2 (single), 1 (scalable)	Partitioning the remote interaction system from the control system will make attacks highly improbable.

Remote Interaction Table 7.4: Risk heatmap after security controls and applied and tested as per SL 1 mitigations

Probability Level	Level of Severity			
	1 - High	2 - Medium	3 - Low	4 - Negligible
A – Highly probable				
B – Probable				
C – Occassional			i	
D – Remote				
E – Improbable		ii, iii, iv		
F – Highly improbable	v			

The risk assessment indicates that some of the risks still require review by the organization stakeholders. If the risks are not considered acceptable, additional layers of protection need to be defined.

8 Referenced Documents

ASME A17.1/CSA B44	Safety Code for Elevators and Escalators
BSI ICS Security Compendium V1.23	Federal Office for Information Security P.O.B. 20 03 63 D-53133 Bonn (Germany) BSI
BSI Top 10	BSI Analyses about cyber security BSI
CAPEC V 3.0	Common Attack Pattern Enumeration and MITRE Corporation
CISA	Cybersecurity Practices for Industrial Control Systems https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf
FIRST CSIRT2.0 Framework	Computer Security Incident Response Team (Services) FIRST.org
IEC 62443-1-1	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
ISA/IEC 62443-2-4 2017	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers ISA/IEC
ISA/IEC 62433-3-3: 2013	Industrial Communication Networks – Network and System Security- Part 3.3: System Security Requirements and Security Levels ISA/IEC
ISA/IEC 62443-4-1:2018	Security for industrial automation and control systems – Part 4-Secure product development lifecycle requirements ISA/IEC
ISO/IEC 27036-3:2013	Information technology -- Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security ISO/IEC
ISO 14798:2009	Lifts (elevators), escalators and moving walks – Risk assessment and reduction methodology ISO
ISO 27005:2018	Information technology -- Security techniques – Information security risk management

ISO 27035	Information Security Incident Management ISO
MITRE ATT&CK for Enterprises	MITRE ATT&CK for Enterprises https://attack.mitre.org
MITRE ATT&CK for ICS	MITRE ATT&CK for ICS https://collaborate.mitre.org/attackics/index.php/Main_Page MITRE
MITRE Cyber Exercise Playbook	Cyber Exercise Playbook https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf MITRE
NIST Building Blocks	Building Blocks https://www.nccoe.nist.gov/projects/building-blocks NCCOE – NIST
NIST Defense in Depth	NIST Defense in Depth definitions https://csrc.nist.gov/glossary/term/defense_in_depth NIST Computer Security Resource Center
NIST SP800-30 Rev .1	Guide for Conducting Risk Assessments National Institute of Standards and Technology, US Department of Commerce
NIST SP800-82 Rev .2	Guide to Industrial Control Systems (ICS) Security National Institute of Standards and Technology, US Department of Commerce
NSA Defense in Depth	Defense in Depth https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-in-depth.cfm NSA
OWASP ASVS Testing Guide	Open Web Application Security Project The OWASP™ Foundation
US-CERT Defense in Depth	Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-in-Depth Strategies https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf US-CERT
US-CERT ICS Incident Response Control Systems	Recommended Practice: Developing an Industrial Capability Cybersecurity Incident Response Capability

https://www.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf
US-CERT