



# NEII

NATIONAL ELEVATOR INDUSTRY, INC.

---

## Elevator and Escalator Industry Cybersecurity Best Practices

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



This guideline was 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.

April 1, 2019

# Elevator & Escalator Industry Cybersecurity Best Practices

## Table Contents

|     |                                  |         |
|-----|----------------------------------|---------|
| 1.0 | Preface                          | Page 3  |
| 2.0 | Introduction                     | Page 3  |
| 3.0 | Scope                            |         |
| 3.1 | Definitions                      | Page 3  |
| 3.2 | Architectures Considered         | Page 4  |
| 3.3 | Safe/Trusted Zones               | Page 4  |
| 4.0 | Cybersecurity Process Life Cycle | Page 6  |
| 4.1 | Training                         | Page 7  |
| 4.2 | Requirements                     | Page 8  |
| 4.3 | Design                           | Page 14 |
| 4.4 | Implementation                   | Page 15 |
| 4.5 | Verification, a Planned Approach | Page 16 |
| 4.6 | Release                          | Page 17 |
| 4.7 | Operations                       | Page 18 |
| 4.8 | Response Plan                    | Page 19 |
| 5.0 | Levels of Security               | Page 20 |
| 6.0 | Security Measures                | Page 21 |
| 6.1 | Security of Service Tools        | Page 21 |
| 7.0 | Example                          | Page 22 |
| 8.0 | Referenced Documents             | Page 26 |

## 1.0 Preface

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

## 2.0 Introduction

Cybersecurity protection for elevators and escalators has become a necessity. These systems, at one time isolated building conveyances, have become an integrated part of complex modern building systems with multiple controllers and processors, monitoring systems accessing the internet, Wi-Fi capable communications to PC and mobile device based service tools. Elevators and escalators have also become 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.

## 3.0 Scope

This guideline provides a path to aid elevator and escalator manufacturers in designing systems 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 system and the Internet, building area networks and untrusted systems. Maintenance and service tools used by technicians are included and will be treated as an untrusted system. The approach is to use industry best practices as the guidance until such times as a comprehensive cybersecurity standard for elevators and escalators becomes available.

### 3.1 Definitions

|                   |   |
|-------------------|---|
| Asset:            | Anything with a perceived or actual value to the organization   |
| DDS:              | Destination Dispatching System  |
| EMS:              | Elevator/escalator Management System  |
| F&LS:             | Fire and Life Safety System   |
| BMS:              | Building Management System  |
| PSTN:             | Public Switched Telephone Network   |
| Security Control: | These are specific processes and installation and organization controls that need to be implemented to keep up the overall cyber security health of the system. They include, but are not limited to, periodic security audits, continuous security monitoring and incident management processes. |
| 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.                            |
| MRL:              | Machine room-less elevator  |

## 3.2 Architectures Considered

The guideline is targeted primarily at interface points where the elevator or escalator system has communications with untrusted entities. While the guide addresses interface points to other systems, best practices should also consider communications between internal functions. Fig 1, Fig 2 and Fig 3 depict some typical examples of elevator system architectures and the parts of the system at risk; these examples apply equally to escalator control systems. Since they are examples they may be different than actual implementations. The interfaces included in the scope are:

- Connection points that interface to the internet either physically or wireless;
- 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 (e.g. PCs) themselves;
- Trapped passenger alarm system if it can accept downloaded software or elevator interaction; and
- Communication links that connect outside the elevator and escalator system/spaces.

## 3.3 Safe/Trusted Zones

The safe/trusted portions of the systems are not considered in this guideline, they are covered by the semi-transparent green areas in Figs 1, 2, and 3 below. While a cybersecurity architecture should consider a layered approach in the safe/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.

**Figure 1**

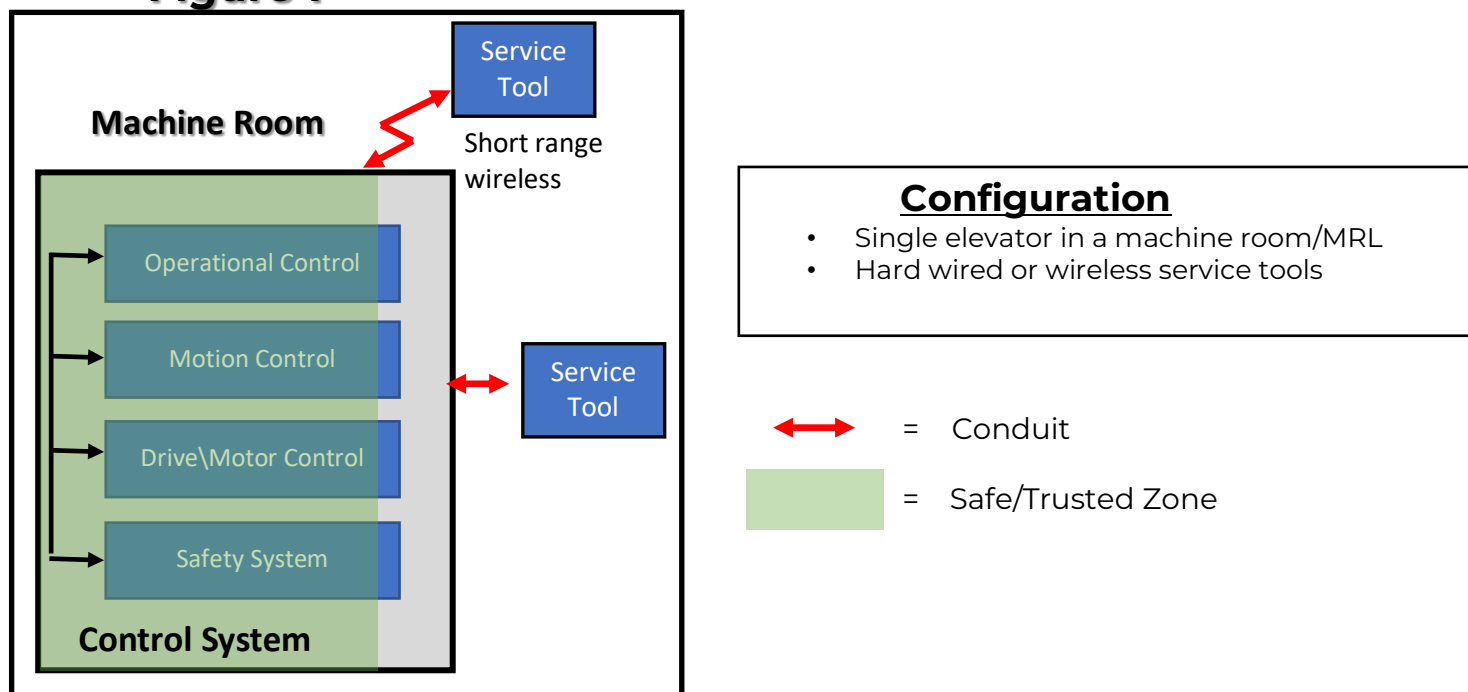


Figure 1 is a single elevator installation, with wireless communications to service tools

**Figure 2**

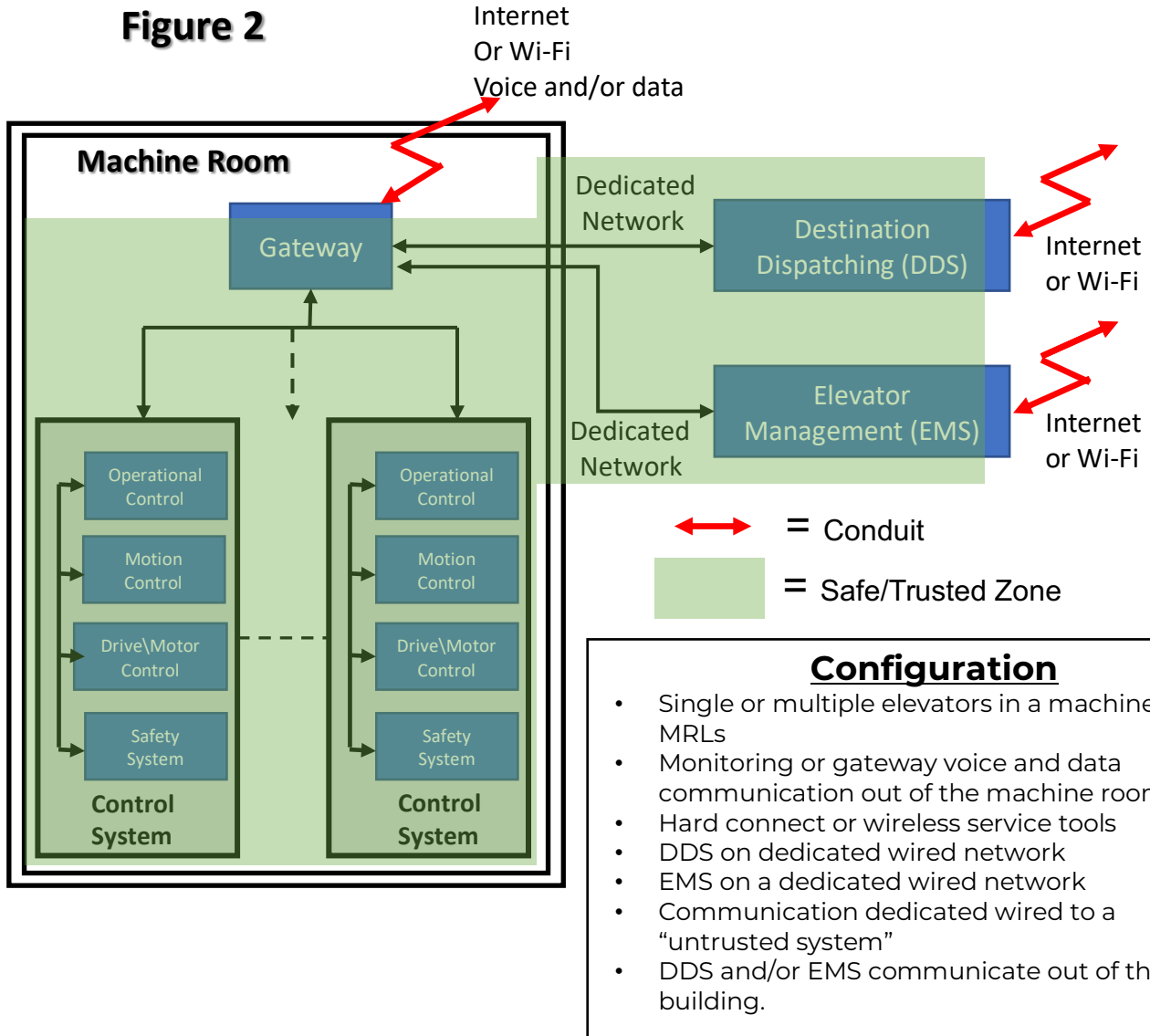
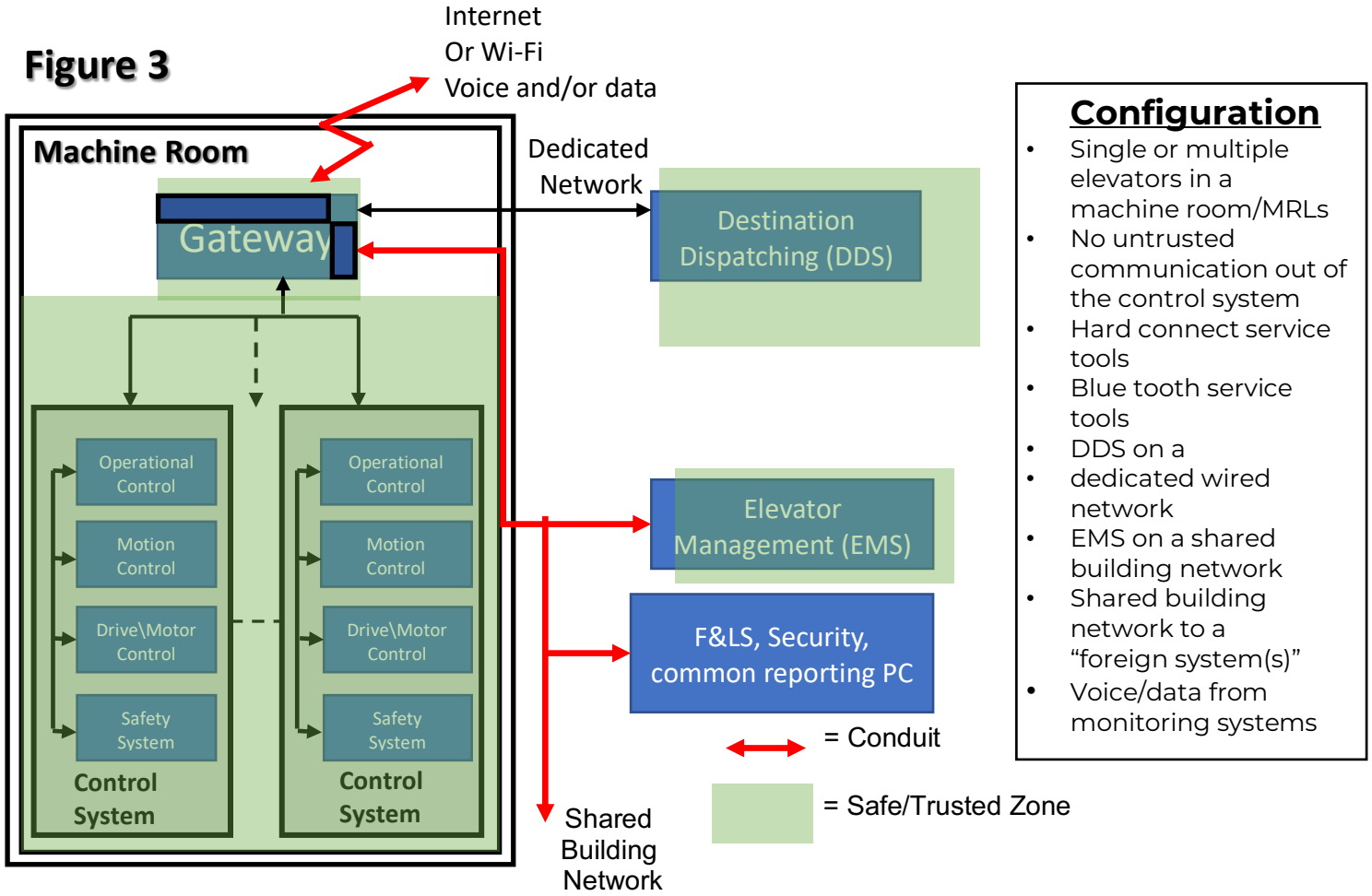


Figure 2 is a more complex installation in which the destination system and the management systems communicate over a network via a gateway which interacts with a cloud.

**Figure 3**



- Configuration**
- Single or multiple elevators in a machine room/MRLs
  - No untrusted communication out of the control system
  - Hard connect service tools
  - Blue tooth service tools
  - DDS on a dedicated wired network
  - EMS on a shared building network
  - Shared building network to a "foreign system(s)"
  - Voice/data from monitoring systems

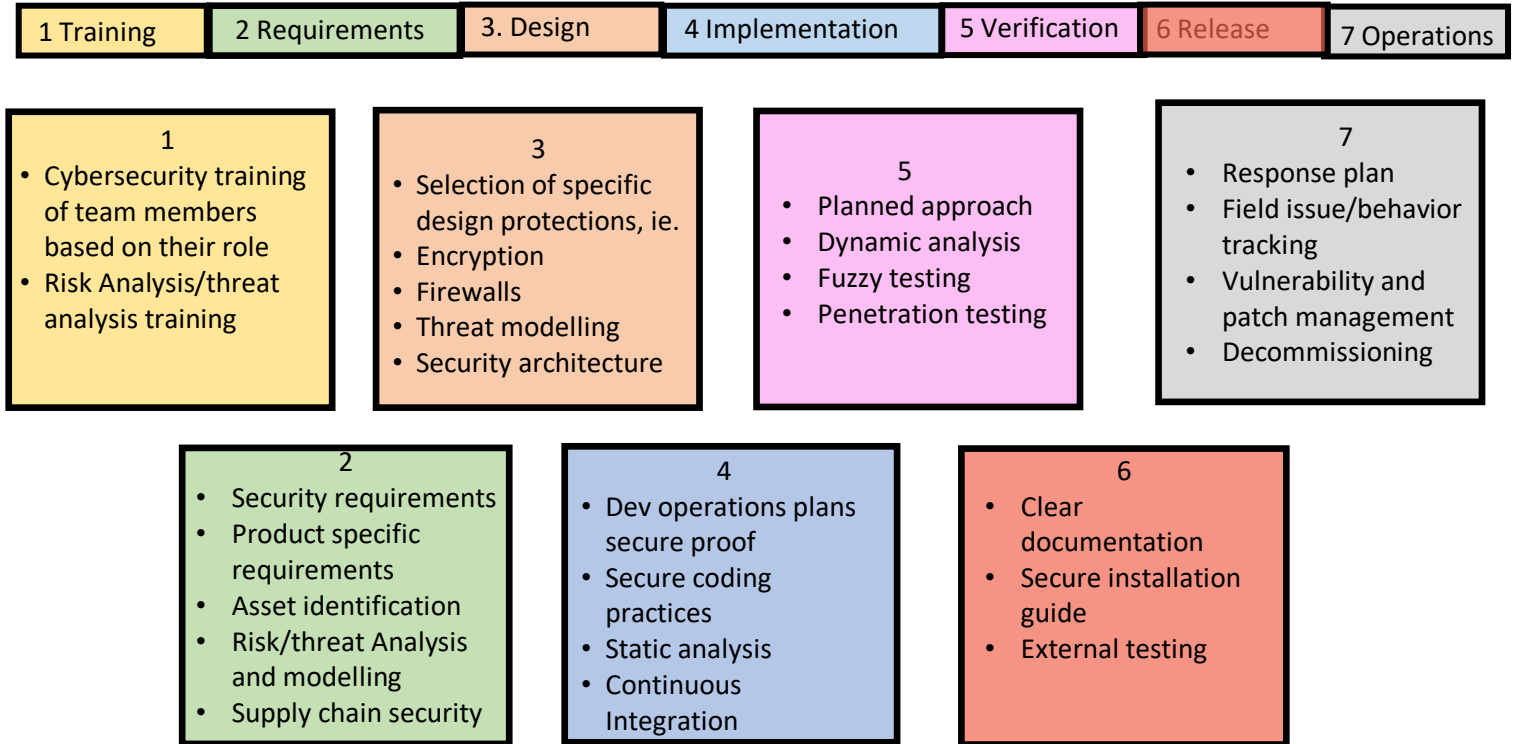
Figure 3 covers the case of an untrusted building network

#### 4.0 Cybersecurity Process Life Cycle

The fundamental recommendation of this guideline is a strong cybersecurity process lifecycle. This lifecycle needs the organization to commit adequate training, tools, resources, and processes to harden and maintain the elevator and escalator system 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. The important point is that the functions described in the following sections are 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 corresponding employees should be tailored to their role and give general information as well as role-specific expertise not necessarily required by other parties. The following are a few examples what this training should consist of:

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 system to be secured as well as the risks induced by cybersecurity threats. It is recommended that the training team includes cybersecurity specialists.

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.

Furthermore, as in normal IT security, upper management needs to understand how important cybersecurity is for elevator and escalator installations. Additionally, management 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 like ISO 14798 and is able to work according to the relevant best practices.

## 4.2 Requirements

### Introduction

The process of managing cybersecurity requirements of an elevator and escalator system 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 system.

Since identifying assets and gathering possible security risks is a creative and cooperative process, seeking professional external support (e.g., for the moderation 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 system 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-directional 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 only rely on implementing a baseline of controls. (Although in some cases, the baseline can be determined to be adequate.)



## Requirements Process

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

- Identify assets and the level of tolerable risk.
- 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 security requirements.
- Further iteration of risk assessment:
  - Evaluate existing countermeasures.
  - Reevaluate likelihood and impact of risk events.
  - Determine residual risk.
- Document cybersecurity requirements, assumptions, and constraints.

The risk assessment should be updated every time when 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 requirement process follow.

## Asset and System under Consideration Identification

- 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 or physical objects. Examples include availability of service, safety of passengers and service personnel, the integrity of the safety system, etc.
- It might be necessary to identify additional assets which are present in the specific System under Consideration (SuC).
- For elevator and escalator systems, safety of passengers and service technicians should be considered as a protected asset, and it takes 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.

## 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 elevator and escalator systems 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
- Sabotage/vandalism
- Additional input for possible threats is given for example in NIST SP800-30, BSI Top 10, OWASP Top 10, CAPEC, 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 adversary capability and intent and the vulnerabilities that exist in the system:
  - 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 systems to exploit?
  - System vulnerabilities and accessibility: For example, is the system exposed over the Internet or is it operated in closed network (e.g. internal elevator and escalator control system network)?
- 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 several. Depending on the specific risk event, the consequences may be:
  - Passenger or service technician injury, e.g. by actuation of the safety gear or uncontrolled motion of the elevator or door drives;
  - Elevator and escalator out of operation 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 systems, the probability and severity may be mapped against ISO 14798:2009 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  |
|---|--|--|
| <b>A — Highly probable</b>  | 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>B — Probable</b>   | 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.  |
| <b>C — Occasional</b>   | 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. |
| <b>D — Remote</b>   | 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.              |
| <b>E — Improbable</b>   | 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. |
| <b>F — Highly improbable</b>  | Probability cannot be distinguished from zero      | No concern, security controls or other measures fully implemented, assessed, and effective.  |
| <ul style="list-style-type: none"> <li>• Lower the probability by one category if the system is operated in closed network.</li> <li>• Lower the probability by two categories if the system is operated in a physically secure location and only accessible in that location.</li> </ul> |  |  |

**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)   |
|--|---|---|---|
| <b>1 - High</b>  | Death, system loss, or severe environmental damage          |   |   |
| <b>2 - Medium</b>  | Severe injury or major system or environmental damage       |   |   |
| <b>3 - Low</b>   | 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) <sup>A, B</sup> | Data integrity compromised (e.g. elevator and escalator management system data tampered with) <sup>A, B</sup> |
| <b>4 - Negligible</b>  | Does not result in injury or system or environmental damage | Minor service disruption (e.g. transport capacity reduced) <sup>A, B</sup>  | Loss of non-critical data (e.g. elevator and escalator management system data) <sup>A, B</sup>                |
| <p>A Raise the severity by one category if the impact is to multiple sites.<br/>                     B Raise the severity by two categories if the impact country-wide/global.</p> |   |   |   |

- 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 are described in Section 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.
- Best practice when creating/choosing countermeasures is the so called “defense in depth” approach. 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.
- Compensating countermeasures, such as physical access control or detective controls, may also be used to satisfy one or more security requirements.
- See Section 6 for a list of countermeasures.

### 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 whether 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 or system, at the end of the risk assessment the required mitigations are identified to minimize the risks identified during the initial assessment.

### 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.
  - Be tracked and at the end of the development verified and validated like all other requirements.

### Externally Developed Component Security

The methods described above should be extended also 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 ideas 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 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. 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.

Best practice is to carry out continuous source code analysis during the development process.

When developers check-in the code, the code is 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 system 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. This analysis should be carried out by a company who is known to be skilled in performing such an analysis.



## 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 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 API (Application Programming Interface) 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.

- Installation Guide for a Secure System

Installation guidelines should list and explain all security configuration options present in the system 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.

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 RACI (responsible, accountable, consulted and informed) matrix with contact details.

## 4.7 Operations

Where service is maintained, operations of the equipment exposed to threats requires 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 Response Plan

Written procedures should be 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. At a minimum the response plan should contain the following:

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

Examples of incidents include:

- Abnormal network traffic
- Unexpected shutdown due to a security breach
- Defacement of an elevator and escalator display

The company 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 system since sensitive information might be stored on some components (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.

## 5.0 Levels of Security

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

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 monetary gain (through ransomware) or 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.

## 6.0 Security Measures

This section recommends the use of security measures for security levels 1 and 2 based on the Systems Requirements (SR) defined in Table 6 a) of the ISA/IEC 62443-3-3 Standard. A detailed description of the requirements can be found in that standard.

### 6.1 Security of Service Tools

Tools that are used for servicing elevators or escalators should employ effective security measures. Service tools can broadly be put into three categories:

- Those that can communicate with the elevator and escalator remotely from anywhere on the Internet;
- 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 in depth strategy that implements multiple security measures based on the level of accessibility to the device and that impact that can be caused if the system was compromised. In this regard, the accessibility in the above three cases would require different types of security controls depending on the extent of system control that is capable through the service tools. For example, if the service tool is capable of writing configuration changes remotely from the Internet, then a multi-factor authentication is recommended. This could include a combination of device authentication using certificates or pre-shared unique keys, passwords and whitelisting. At the least a unique password-based scheme is required even when physical access is required.

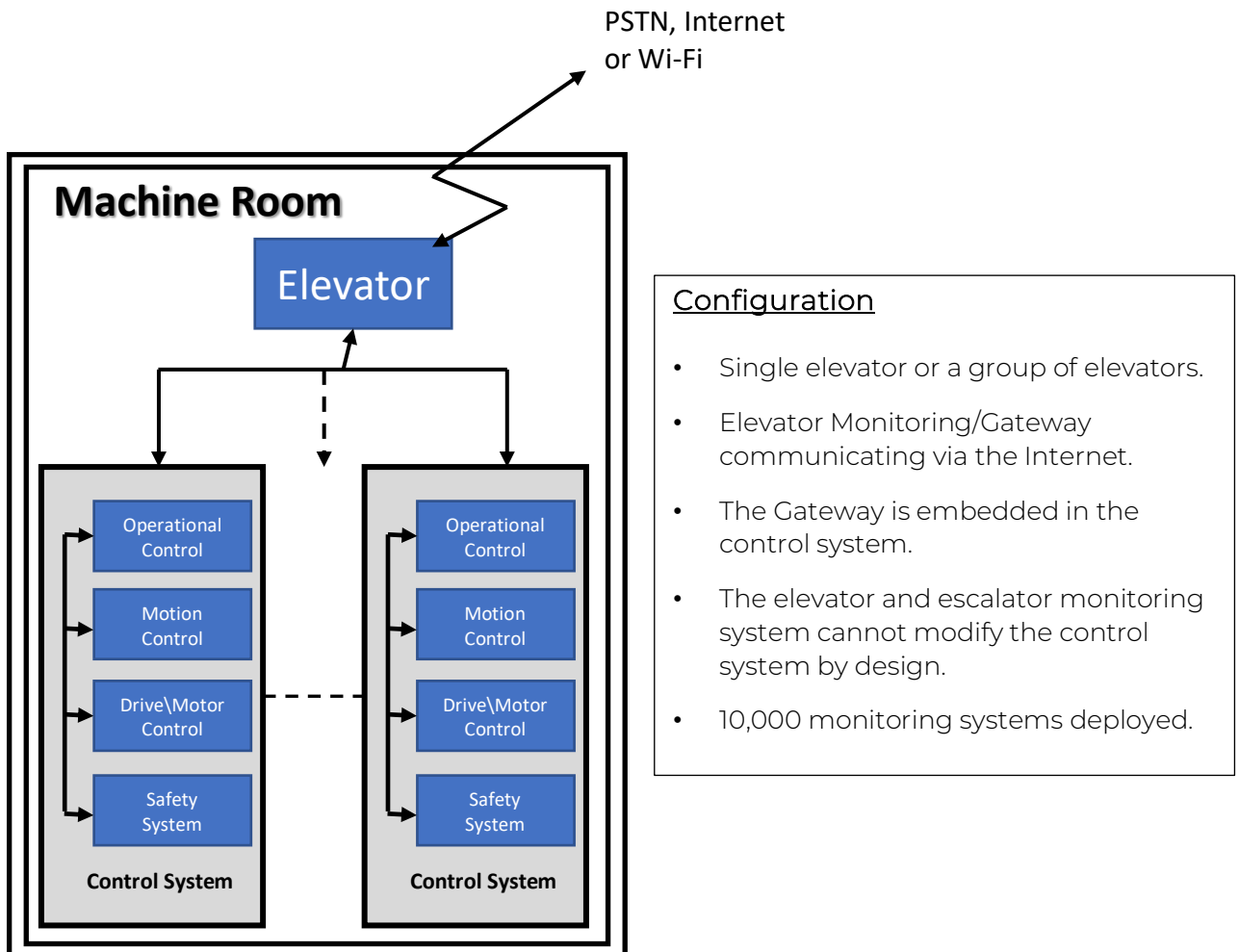
## PC Hardening

In addition to the security controls for authentication and encryption, an important requirement for service tools is to ensure that the machine (PC/mobile device) on which the tool is running is sufficiently hardened and proper access control related to the use of the machine is employed.

Using strong passwords for all user accounts, maintaining good anti-virus and anti-spyware software, applying patches on a timely basis, turning on the software firewalls options, and restricting use of the machine to the function intended are some key elements in a hardening guide. Such hardening guidelines are published by the National Institute of Standards and Technology (NIST) and other organizations and are recommended to be followed by any third party involved in using service tools or servicing the elevator.

## 7.0 Example

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



## Requirement Process

1. Identify assets:
  - Functions of the control system cannot be modified from the monitoring system
  - Integrity of the monitoring system
  - Integrity of the data sent by the monitoring system
  - Availability of the monitoring 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 monitoring system.
    - ii. Tampering with the data sent from the monitoring system.
    - iii. Spoofing the endpoint for data sent from monitoring system.
    - iv. Taking ownership of monitoring system.
    - v. Attacking the control system through the monitoring system.
  - b. Determine likelihood and impact (see Table 7.1 below).

**Table 7.1 Risk Assessment**

| Risk event  | Probability | Impact                      | Note  |
|---|-------------|-----------------------------|---|
| i. Denial of service attack on the monitoring system            | A           | 4 (single),<br>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 monitoring data is not serious. |
| ii. Tampering with the data sent from the monitoring system     | D           | 3 (single),<br>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 monitoring system | B           | 3 (single),<br>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 monitoring system                       | C           | 3 (single),<br>2 (scalable) | If the monitoring system is unprotected, taking ownership will not be hard. However, monitoring is not considered critical function so the impact will be low for single site.  |
| v. Attacking the control system through the monitoring system   | E           | 2 (single),<br>1 (scalable) | Attacking the control system requires extensive skills even after the monitoring system is breached. If attack is successful, impact can be medium on single site.  |

c. Determine unmitigated cybersecurity risk

As the monitoring 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: Unmitigated cybersecurity risk for a scalable attack**

| Probability Level     | Level of Severity |            |         |                |
|-----------------------|-------------------|------------|---------|----------------|
|                       | 1 - High          | 2 - Medium | 3 - Low | 4 - Negligible |
| A – Highly probable   |                   |            | i       |                |
| B – Probable          |                   | iii        |         |                |
| C – Occasional        |                   | 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**

| Risk event  | Probability | Impact                      | Note on mitigation   |
|---|-------------|-----------------------------|--|
| i. Denial of service attack on the monitoring system            | C           | 4 (single),<br>3 (scalable) | Implementing DoS protection (e.g. packet filtering) will make successful attacks harder.   |
| ii. Tampering with the data sent from the monitoring system     | E           | 3 (single),<br>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.   |
| iii. Spoofing the endpoint for data sent from monitoring system | E           | 3 (single),<br>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. |
| iv. Taking ownership of monitoring system                       | E           | 3 (single),<br>2 (scalable) | Implementing authentication and accounting and auditing on the monitoring system will make remote attack to take ownership improbable.   |
| v. Attacking the control system through the monitoring system   | F           | 2 (single),<br>1 (scalable) | Partitioning the monitoring system from the control system will make attacks highly improbable.  |

**Monitoring Table 7.4: Cybersecurity risk for a scalable attack after SL 1 mitigations**

| Probability Level     | Level of Severity |             |         |                |
|-----------------------|-------------------|-------------|---------|----------------|
|                       | 1 - High          | 2 - Medium  | 3 - Low | 4 - Negligible |
| A – Highly probable   |                   |             |         |                |
| B – Probable          |                   |             |         |                |
| C – Occasional        |                   |             | 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.

## 8.0 Referenced Documents

|                                   |   |
|-----------------------------------|---|
| BSI ICS Security Compendium V1.23 | Federal Office for Information Security<br>P.O.B. 20 03 63<br>D-53133 Bonn (Germany)<br>BSI   |
| BSI Top 10                        | BSI Analyses about cyber security<br>BSI  |
| CAPEC V 3.0                       | Common Attack Pattern Enumeration and<br>MITRE Corporation  |
| ISA/IEC 62443-2-4 2017            | Security for industrial automation and control systems – Part<br>2-4: Security program requirements for IACS service providers<br>ISA/IEC   |
| ISA/IEC 62433-3-3: 2013           | Industrial Communication Networks – Network and System<br>Security- Part 3.3: System Security Requirements and Security<br>Levels<br>ISA/IEC  |
| ISA/IEC 62443-4-1:2018            | Security for industrial automation and control systems - Part<br>4-Secure product development lifecycle requirements<br>ISA/IEC   |
| ISO/IEC 27036-3:2013              | Information technology -- Security techniques -- Information<br>security for supplier relationships -- Part 3: Guidelines for<br>information and communication technology supply chain<br>security<br>ISO/IEC |
| ISO 14798:2009                    | Lifts (elevators), escalators and moving walks -- Risk<br>assessment and reduction methodology<br>ISO   |
| ISO 27005:2018                    | Information technology -- Security techniques -- Information<br>security risk management  |
| NIST SP800-30 Rev .1              | Guide for Conducting Risk Assessments<br>National Institute of Standards and Technology, US<br>Department of Commerce   |
| NIST SP800-82 Rev .2              | Guide to Industrial Control Systems (ICS) Security<br>National Institute of Standards and Technology, US<br>Department of Commerce  |
| OWASP ASVS Testing Guide          | Open Web Application Security Project<br>The OWASP™ Foundation  |