Verborgene Risiken:

Die Bedeutung von Bedrohungsanalysen in der OT-Sicherheit

LIMES SECURITY

NIS2

- Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems **appropriate to the risks posed**

- Definition:
  - ‘risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a **combination** of the **magnitude** of such loss or disruption and the **likelihood** of occurrence of the incident

Cyber Resilience Act

- Products shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity **based on the risks**;
- Definition:
  - ‘cybersecurity risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

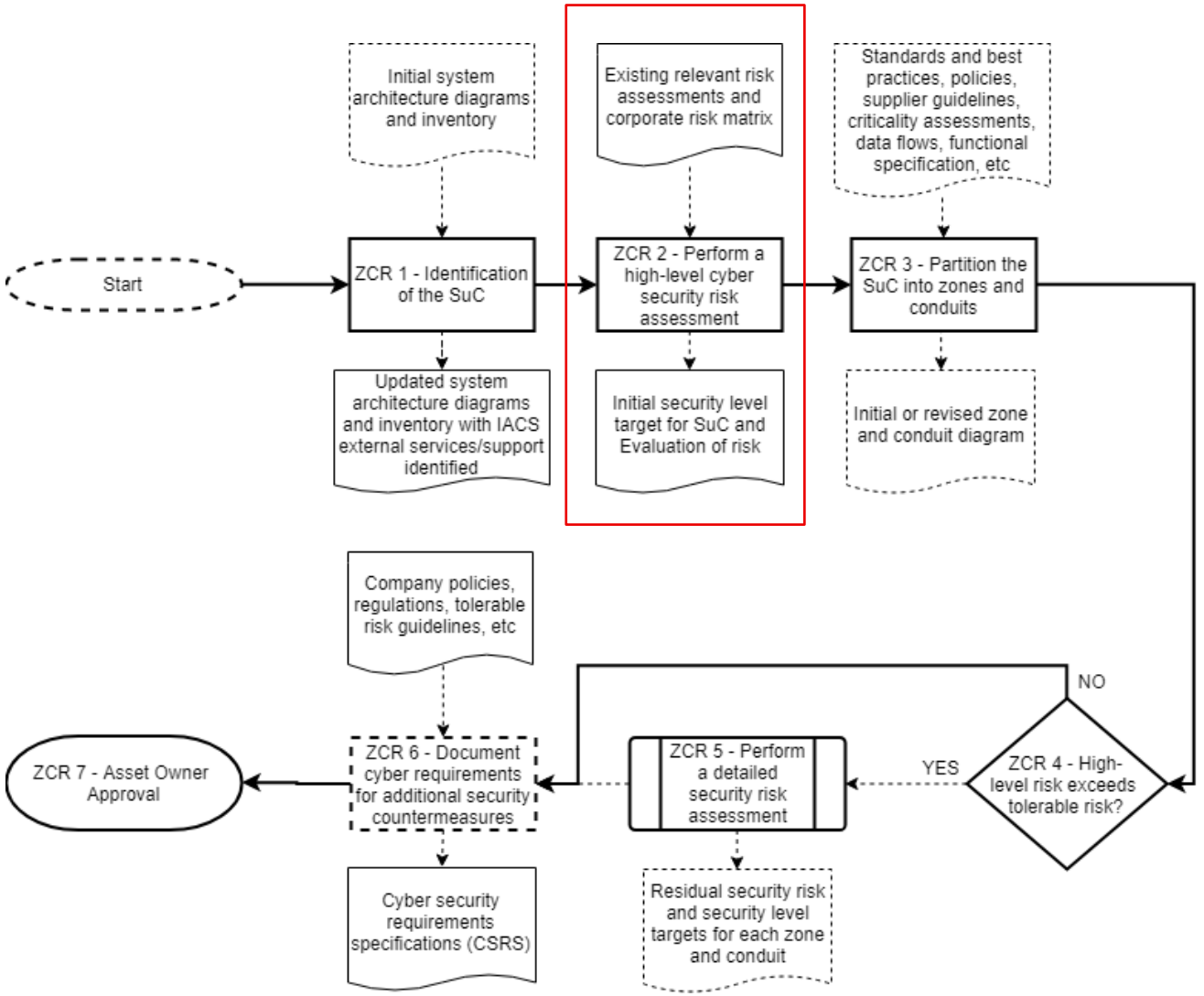
IEC 62443-3-2 Introduction

- There is no simple recipe for how to secure an industrial automation and control system (IACS) and there is good reason for this. It is because **security is a matter of risk management**.

- Definition:
  - **expectation of loss** expressed as the **likelihood** that a particular threat will exploit a particular **vulnerability** with a particular **consequence**

Assessing Risk According To IEC 62443-3-2

ZCR – Zoning and Conduit Requirement



Top 10 Industrial Security Threats 2022

LIMES SECURITY

The Federal Office for Information Security in Germany compiles a list of the current threats with the highest criticality faced by OT.

1. Infiltration of Malware via Removable Media and External Hardware
2. Malware Infection via Internet and Intranet
3. Human Error and Sabotage
4. Compromising of Extranet and Cloud Components
5. Social Engineering and Phishing
6. (D)DoS Attacks
7. Internet-connected control components
8. Intrusion via remote maintenance access
9. Technical failure and Force Majeure
10. Soft- and hardware vulnerabilities in the supply chain

Source: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf?__blob=publicationFile&v=6

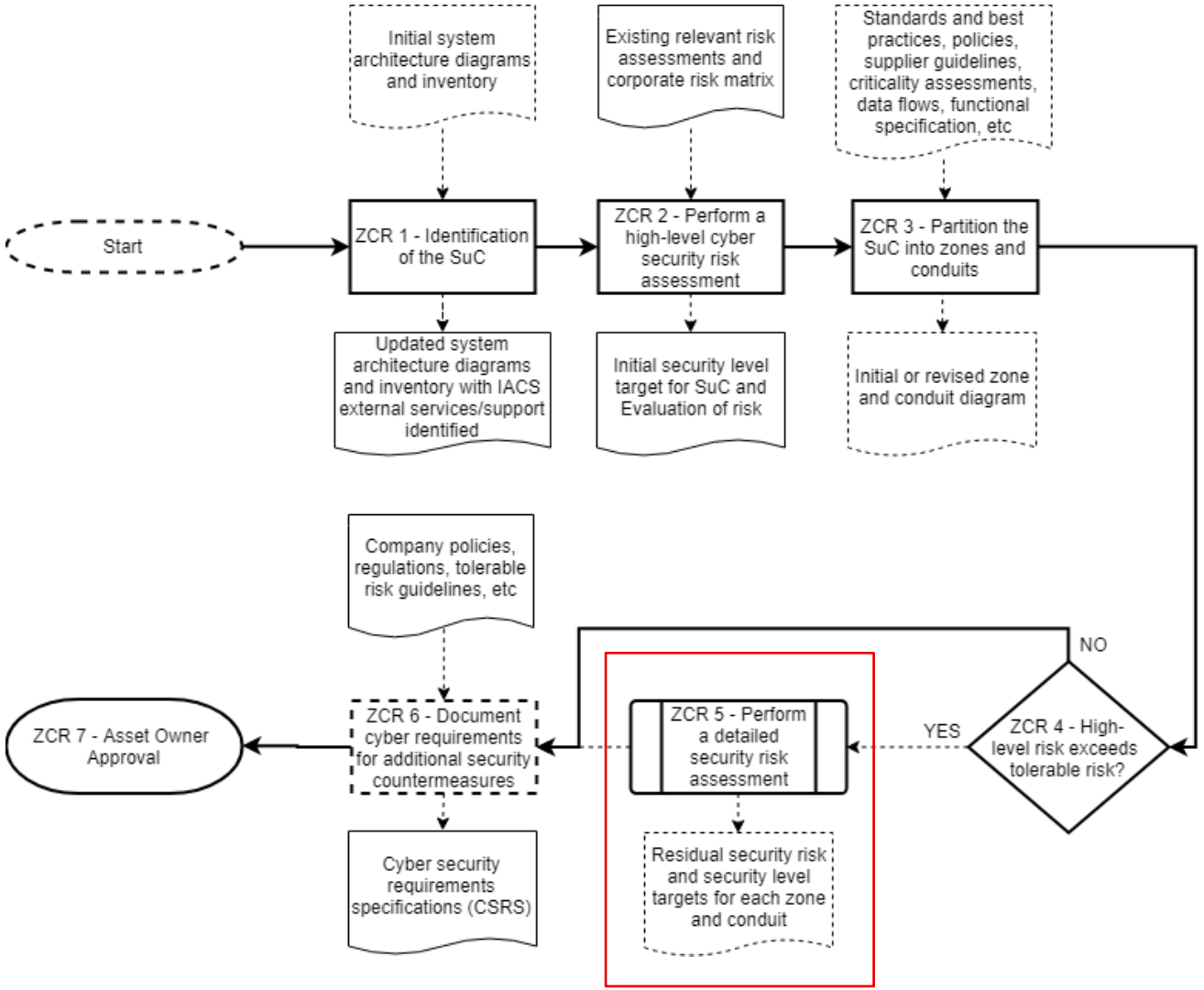
Impacts

- What are the potential implications of asset compromise?
- How are these effects to be classified in terms of their criticality?

		Danger to life and limb	Availability	Confidentiality	Integrity	Physical damage	Violation of regulations and supply contracts
4	Disastrous	Deaths	10,0000 households can't be supplied with electricity for 2 days. (e.g. SCADA system is not switchable for 2 days)			- Damage to a generator	
3	Critical	severely injured			Write access to: - Historian data		- 5% deviation from the specified guideline value over 2h
2	Moderate		1,000 households can only be supplied insufficiently with electricity (e.g. SCADA system cannot be switched for 1h)	Read access to: - Historian data		- Increased wear of the generator blades	
1	Negligible						- 1% deviation from the specified guideline value over 2h

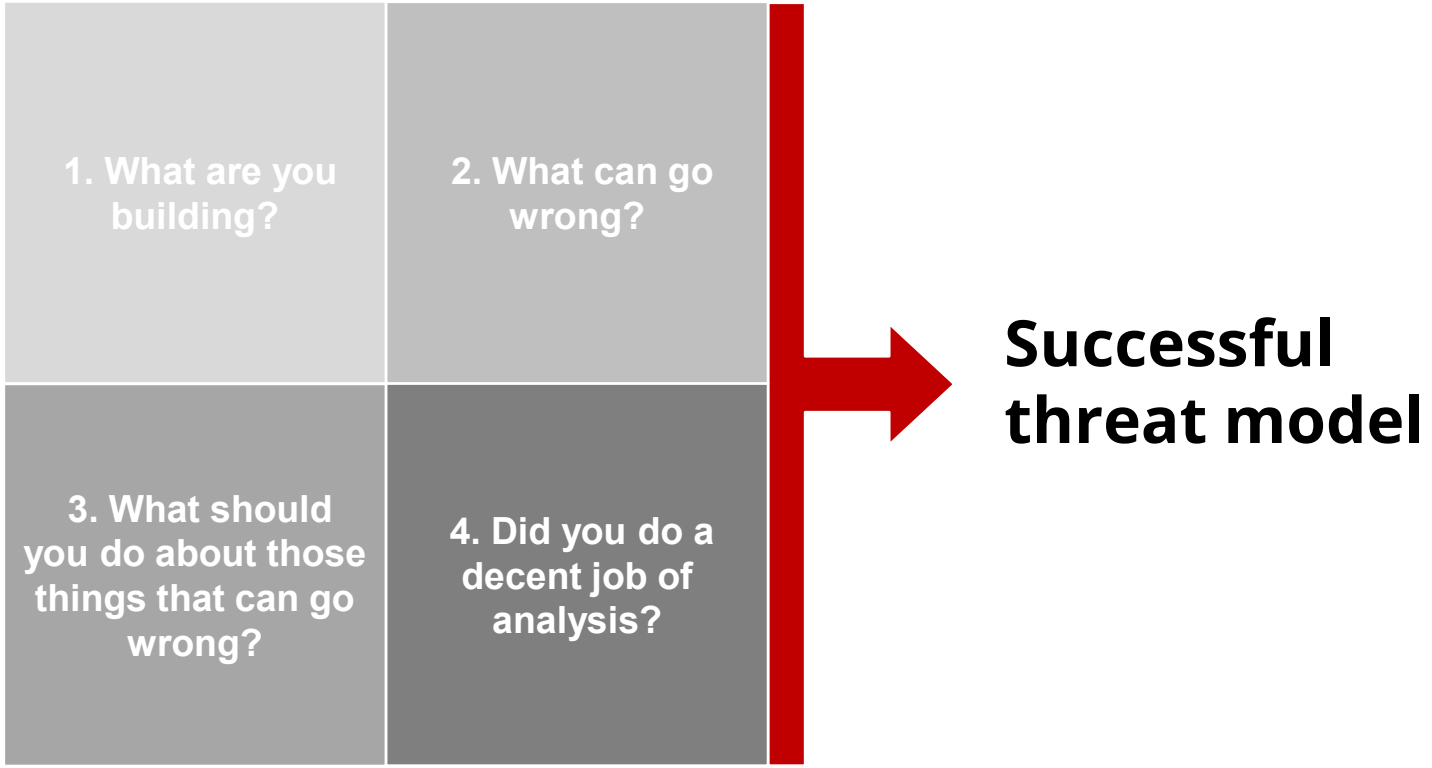
Zoning Process According To IEC 62443-3-2

ZCR – Zoning and Conduit Requirement



Components Of A Threat Modeling Process

- You begin threat modeling by focusing on four key questions:

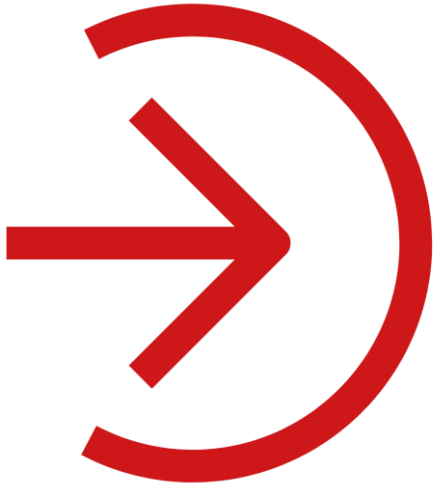


IEC 62443-4-1 Threat Model Requirements

“Ensure that all products shall have a threat model specific to the current development scope of the product with the following characteristics.” – 6.3.1 SR-2 Threat model requirements

- Correct flow of categorized information throughout the system;
- Trust boundaries;
- Processes;
- Data stores;
- Interacting external entities;
- Internal and external communication protocols implemented in the product;
- Externally accessible physical ports including debug ports;
- Circuit board connections such as JTAG connections or debug
- Headers which might be used to attack the hardware;
- Potential attack vectors including attacks on the hardware, if applicable;
- Potential threats and their severity as defined by a vulnerability scoring system
- Mitigations and/or dispositions for each threat;
- Security-related issues identified; and
- External dependencies in the form of drivers or third-party applications that are linked into the application.

The Limes Security Way to do a Threat & Risk Assessment



Assumptions (i.e. Security Context)

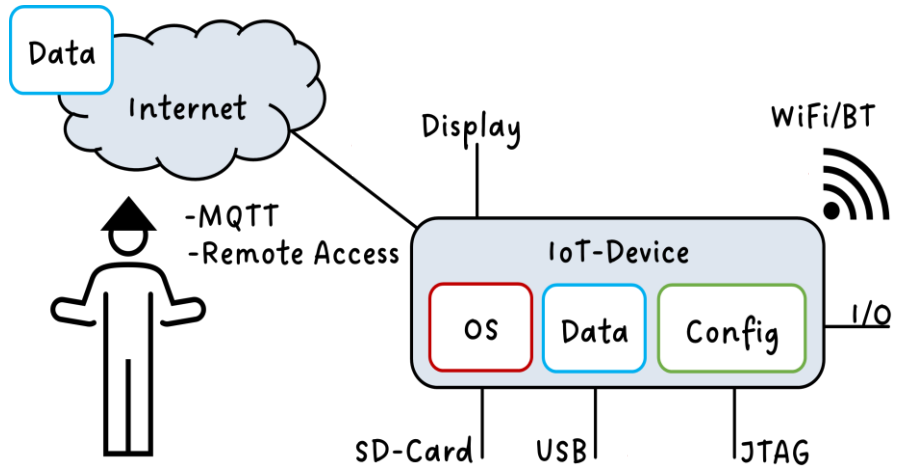
Define the System under Consideration (SUC) and document applicable assumptions

- Finding answers to questions such as:
  - What is the intended use of the product?
  - Who are the users/operators of the product?
  - What does the operational environment look like?
  - What potential mitigating measures already exist?
  - What could be reasonably asked from customers to provide?
  - What is the foreseeable product life expectancy?
  - Can the physical/logical access be restricted?
  - …

Interfaces & Assets

Document all interfaces and assets of the system, to get an idea, where attacks are possible and what the goals could be.

- Interfaces (e.g. TCP ports, USB, JTAG, SWD, I/Os…)
  - What are attacks possible through?
  - What protocols are used?
  - Where is a trust boundary crossed?
  - What data is transferred?
- Assets (e.g. passwords, logic, data,…)
  - What are the possible targets of an attack?
  - What is worth protecting?
  - What is essential for functionality?



Impacts

- What are the potential implications of asset compromise?
- How are these effects to be classified in terms of their criticality?

		Danger to life and limb	Availability	Confidentiality	Integrity	Physical damage	Violation of regulations and supply contracts
4	Disastrous	Deaths	10,0000 households can't be supplied with electricity for 2 days. (e.g. SCADA system is not switchable for 2 days)			- Damage to a generator	
3	Critical	severely injured			Write access to: - Historian data		- 5% deviation from the specified guideline value over 2h
2	Moderate		1,000 households can only be supplied insufficiently with electricity (e.g. SCADA system cannot be switched for 1h)	Read access to: - Historian data		- Increased wear of the generator blades	
1	Negligible						- 1% deviation from the specified guideline value over 2h

Probability

The probability of a threat occurring is made up of:

- the exposure of the affected component
- the exploitability of the misused vulnerability

Exposure		
4	High	**General:** large group of people, Purdue Level: >= 4 **Logical Access:** Internet accessible, large Intranet **Physical Access:** public environment, can be acquired by security researchers
3	Medium-High	**General:** limited, but still large group, Purdue Level: 3, 3.5 **Logical Access:** extranet, medium intranet **Physical Access:** visitor areas with limited surveillance like conference room
2	Medium-Low	**General:** smaller limited group, loosely controlled, Purdue Level: 1 & 2 **Logical Access:** Accessible from fieldbus **Physical Access:** placed in areas with controlled access that is limited to the necessary people and only permanently guarded visitor access
1	Low	**General:** very limited, well controlled group of users, Purdue Level: 0 **Logical Access:** Only accessible by very limited group of people via additional access control, e.g. VPN into DMZ **Physical Access:** secured cabinets with strongly limited access

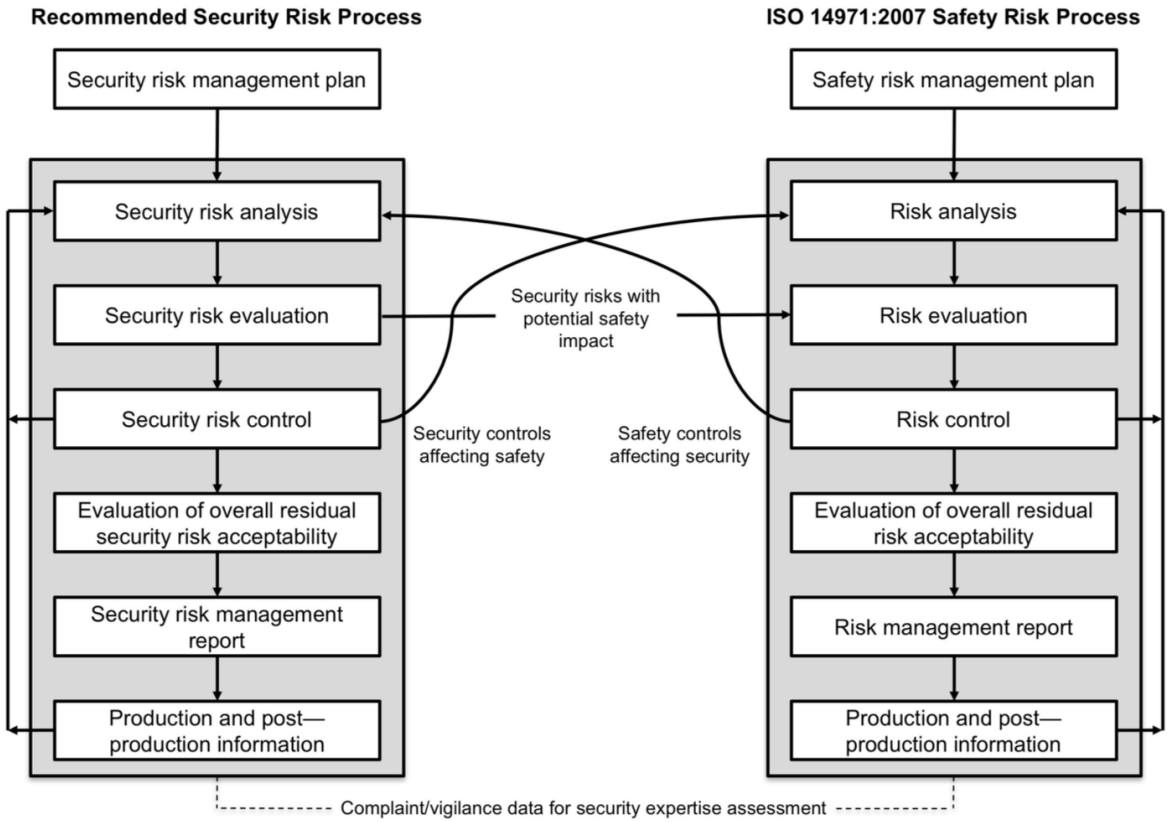
Exploitability		
4	Easy	• basically no knowledge necessary (e.g. usage of default password) • normal usage of the system • IEC 62443 SL1 attacker
3	Mediocre	• can be accomplished with available tools • requires basic IT or domain knowledge (e.g. brute forcing of weak passwords) • exploiting known vulnerabilities of unpatched systems • IEC 62443 SL2 attacker
2	Difficult	• requires development or strong adaption of tools • requires high IT or domain knowledge (e.g. compiling of own tools) • IEC 62443 SL3 attacker
1	Extremely Difficult	• requires exceptional technical expertise • internal knowledge that is only available to a few persons (e.g. requires reverse engineering of a protected binary) • IEC 62443 SL4 attacker

Threats

ID	Who?	Does what?	Affected interface		Impact	Impact Rating	Exposure Description	Exposure Rating	Exploitability Description	Expl. Rating	Likelihood Rating	Risk Rating	Countermeasure-Ideas
1	Attacker	gains access to a user account enabled for SSH	Historian SSH Remote console	that leads to	write access to the historian	3	Accessible from the Intranet	4	Linux commands can be used on the system to change the data. Structure of the data must be understood to make meaningful manipulations.	2	3	3	- MFA - Password Policies - Restriction User Permissions
2	Attacker	is able to install a manipulated firmware image, disabling safety checks	USB-Interface PLC	that leads to	manipulations of configuration data and set-points, resulting in damages to the machine	4	Accessible at machine	2	Knowledge required regarding firmware structure, reverse engineering, internal knowledge on how to manipulate set-points	1	1	2	- Secure Boot (verify authenticity and integrity of firmware image when booting) - Secure Update (install only signed firmware images)

Safety & Security: Risk Management

- There can be positive and negative side effects in both directions!



AAMI TIR57:2016

Training

LIMES SECURITY

SICHERE PRODUKTENTWICKLUNG FÜR OT UND (I)IOT

Produkte konform zu Cyber Resilience Act, Maschinenverordnung, IEC 62443-4-1 und Co. entwickeln

- Überblick zu Security Normen und Regularien gewinnen
- Rahmenbedingungen für sichere Produktentwicklung schaffen
- Security in den Produktentwicklungsprozess integrieren

20. - 22. November 2024

Online

Deutsch

Viel Erfolg bei der Umsetzung!

LIMES SECURITY

Peter Panholzer
+43 664 1631139
ppa@limessecurity.com