Industrial Security – Lessons learned from attacks on industrial control systems

SIEMENS

What is security in context of safety of machinery?

A challenge for the ***machine control system***?

Industrial automation systems can be exposed to security attacks due to the fact that:

- access to the control system is possible, e.g. re-programming of machine functions (including safety)
- "convergence" between standard IT and industrial systems is increasing
- remote access from suppliers has become the standard way of operations / maintenance, with an increased cyber security risk regarding e.g. unauthorized access, availability and integrity

Industrial automation systems represent a *machine control system*

SIEMENS

What is security in context of safety of machinery?

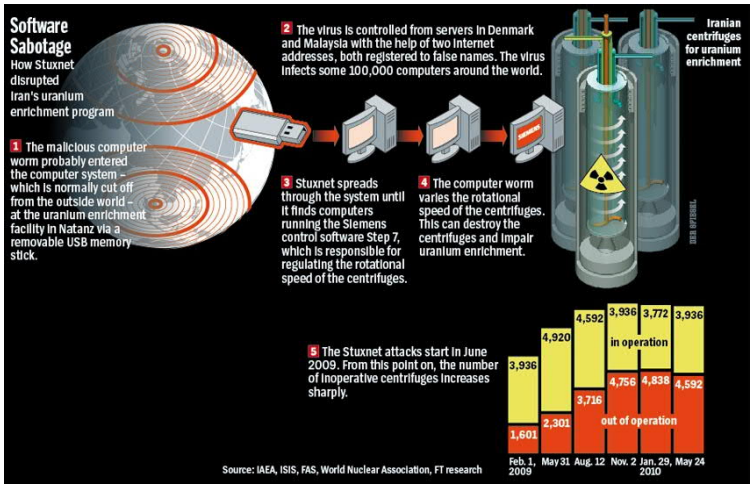
A challenge for the ***machine control system***?

SOURCE: https://cyberhoot.com/cybrary/stuxnet/

Stuxnet is a malicious computer worm first uncovered in 2010 and thought to have been in development since at least 2005.

Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran.

Although neither country has openly admitted responsibility, the worm is widely understood to be a cyberweapon built jointly by the United States and Israel in a collaborative effort known as Operation Olympic Games.



What is security in context of safety of machinery?

A challenge for the ***machine control system***?

SOURCE: https://threatpost.com/florida-water-plant-hack-credentials-breach/163919

The Florida Water Plant Hack
The attack on the Oldsmar water-treatment facility in Florida occurred last Friday, when an attacker used remote access to the system to change the level of sodium hydroxide, more commonly known as lye, in the water from 100 parts per million to 11,100 parts per million.

The change was immediately detected by a plant operator, who changed the levels back before the attack had any impact on the system.

According to a Massachusetts security advisory published Wednesday, the attackers accessed the water treatment plant's SCADA controls via TeamViewer, which is **remote access software**.

SIEMENS

What is security in context of safety of machinery?

A challenge for the ***machine control system***?

Risk assessment | **Risk reduction** | Verification | Marking

As part of an industrial automation system, safety-related control systems of machines can also be subject to security attacks that can result in a loss of the ability to maintain safe operation of a machine

- Functional safety objectives consider the risk by estimating the severity of harm and the probability of occurrence of that harm
- The effects of any risk (hazardous event) determine the requirements for safety integrity
  - Safety Integrity Level (SIL) according to IEC 62061 or IEC 61508
  - Performance Level (PL) according to ISO 13849-1

With respect to the safety function, the security threats (internal or external) might influence the safety integrity and the overall system availability

SIEMENS

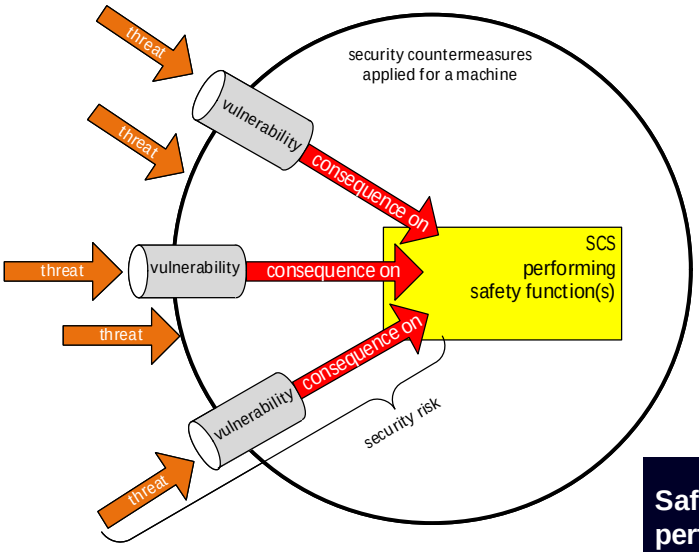
Industrial Security – Basic approach

Risk assessments and interactions

SIEMENS

Basic approach of Industrial Security

Security risk assessment



Risk assessment in machinery

RISK
is the combination of

Severity of harm

Probability of occurrence of harm

- Frequency and duration of exposure
- Possibilities to avoid or limit the harm
- Probability of occurence of a hazardous event

Safety function performed by SCS

SOURCE: IEC TR 63074

SIEMENS

Basic approach of Industrial Security

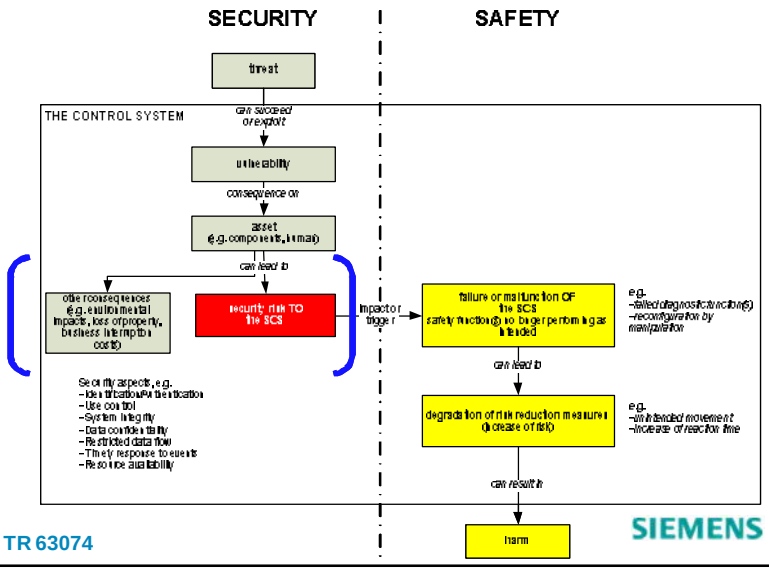
Interactions between security and machine control system

Risk assessment | Risk reduction | Verification | Marking

Security risks and machine functions

Machine control system

- Non safety-related
- Safety-related



SOURCE: IEC TR 63074

SIEMENS

Basic approach of Industrial Security

Interactions between security and machine control system

Risk assessment | Risk reduction | Verification | Marking

Security foundational requirements	Brief description
Identification and authentication control	Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.
Use control	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the control system and monitor the use of these privileges.
System integrity	Ensure the integrity of the control system to prevent unauthorized manipulation.
Data confidentiality	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure
Restricted data flow	Segment the control system via zones and conduits to limit the unnecessary flow of data.
Timely response to events	Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.
Resource availability	Ensure the availability of the control system against the degradation or denial of essential services.

SOURCE: IEC TR 63074

Industrial Security – Cybersecurity

Cybersecurity and functional safety of machinery

SIEMENS

Cybersecurity of Industrial Security

Protection against corruption

Corruption of data or information poses an important vulnerability to network and information systems:

- Connection to safety-related devices
- Hardware for connection (protected against intentional corruption)
- Software and data (protected against intentional corruption)
- Safety-related software to be identified
- Modification of the safety-related software to be recorded

Security countermeasures

Aspects related to protection against corruption of *machine control system*

Cybersecurity of Industrial Security

Potential sources of cybersecurity threats

Industrial automation systems can be exposed to security attacks by access to:

- Network architecture;
- Portable devices;
- Wireless devices and sensors;
- Remote access;
- Interfaces to other systems or human machine interfaces;

Security countermeasures

Functional safety of *machine control system* can also be exposed to attacks

Industrial Security – Cybersecurity

Concrete security countermeasures to be considered

SIEMENS

Concrete security countermeasures in context of safety of machinery?

– Multi-factor authentication –

Where any kind of human interaction with the SCS or parts of it is necessary

- Security factors are stored and used in such a way that a single attack on the user environment does not lead to multiple factors being compromised
- The two security factors use either different transmission paths or different transmission data
- Transmitting the two factors separately in time on the same transmission path, provided that it is ensured that the first factor has been transmitted and received before the second will be transmitted

Basic approach can be used for each online access to machine control system

SIEMENS

Concrete security countermeasures in context of safety of machinery?

– Multi-factor authentication –

SOURCE https://pages.nist.gov/800-63-3/sp800-63b.html

Where any kind of human interaction with the SCS or parts of it is necessary

- NIST Special Publication 800-63B Digital Identity Guidelines

Multi-Factor Cryptographic Devices

Out-of-Band Devices

Basic approach comparable to credit card handling for online payment

Concrete security countermeasures in context of safety of machinery?

– Multi-factor authentication –

SOURCE https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_061E.html

Where any kind of human interaction with the SCS or parts of it is necessary

- BSI (BSI-CS 061E, federal office for Information Security Germany)
  RECOMMENDATION: IT IN PRODUCTION, Industrial Control System Security

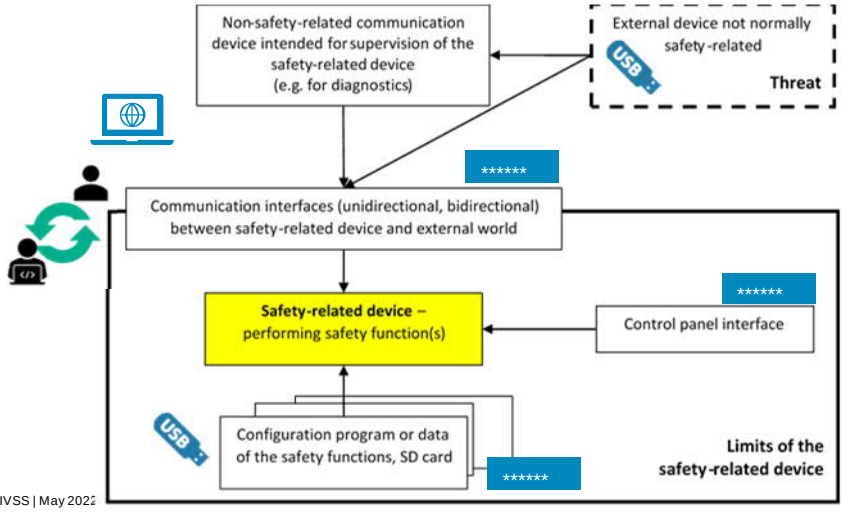
  - ✓ Use of individual accounts with sufficient authentication (e.g. *multi-factor*)
  - ✓ Any operator intervention must be protected by an authentication or according to ***the two-man rule*** (for control systems e.g. programmable logic controllers, PLCs, …)

Basic approach allowing also using the two-man rule

Concrete security countermeasures in context of safety of machinery?

– Attack through direct physical connection –

Direct physical connection to the safety-related control system can have implications on SCS



****** Password protection

SOURCE: IEC TR 63074

SIEMENS

Industrial Security – Cybersecurity

Summary

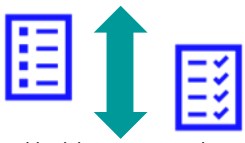
SIEMENS

Summary

Machine manufacturer and user of the machine dialog

Open minded exchange of information

- Overall security risk assessment performed by the user of the machine



- Machine manufacturer supports this risk assessment by providing information on
  - vulnerabilities (phyiscal interfaces)
  - on implemented security countermeasures

User of the machine needs support from machine manufacturer

Summary

Cybersecurity hardware to be considered

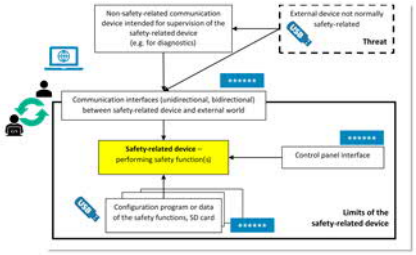
Industrial automation systems can be exposed to security attacks by access to:

- Network architecture;
- Portable devices;
- Wireless devices and sensors;
- Remote access;
- Interfaces to other systems or human machine interfaces;

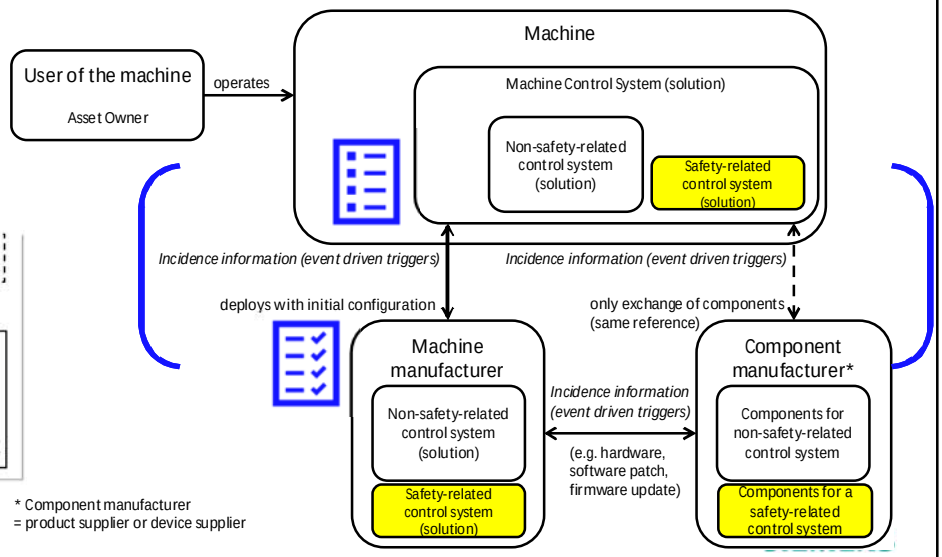
Malicious persons will try to get access via typical vulnerabilities

Summary

Keep informed about new threats



SOURCE: IEC TR 63074



* Component manufacturer
= product supplier or device supplier

Industrial Security – Do not ignore Cybersecurity

SIEMENS