Functional Safety Meets Cybersecurity

Nigel Stanley
Chief Technology Officer
Operational Technology and Industrial Cybersecurity
TÜV Rheinland
Agenda

- Modern industrial cybersecurity risk
- Functional safety and cybersecurity
- Assessing your cybersecurity risk
Agenda

- Modern industrial cybersecurity risk
- Functional safety and cybersecurity
- Assessing your cybersecurity risk
Society is hyper connected, cybersecurity risk permeates modern life

Internet of Things (IoT) = small things!
Industrial Internet of Things (IIoT) = big things!
Information security vs operational technology cybersecurity
Dramatic increase in industrial control system cybersecurity vulnerability disclosures

- Nearly every ICS vendor is affected by vulnerabilities, patches are not available for all discovered issues and even if patches are available they can be difficult to apply to control systems.
- Common vulnerabilities in Industrial Control Systems include buffer overflows, unauthenticated protocols, weak user authentication, poor password policies or management.

Source: Fireeye
Potential impacts of industrial cybersecurity incidents

- Injury or Fatal Accident
- Financial Loss
- Shareholder Confidence
- Destruction of Property
- Public Image
- Intellectual Property Theft
In the news...

BBC NEWS

Hack attack causes 'massive damage' at steel works

By Alfred Ng / May 3, 2017 12:10 PM PDT

Researchers find factory robots can be easily hacked

As the world's factories shift to automation, a series of tests finds some troubling flaws.

Renault stops production at several plants after ransomware cyber attack as Nissan also hacked

Scores of countries have been affected by the so-called ransomware hack, which has infected computers around the world in a number of industries.

Cadbury chocolate factory shut down by Petya cyberattack

The massive ransomware attack reaches Australia, sending things really wonky at the chocolate factory. Ahhhhh, fudge.
...and there's more

Sources:
Information in the open!

Sources:
- https://www.shodan.io/explore/category/industrial-control-systems
- https://scada.hacker.com/library/

Industrial Control Systems

What Are They?

In a nutshell, industrial control systems (ICS) are computers that control the world around you. They’re responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Common Terms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICS</td>
<td>Industrial Control System</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
</tbody>
</table>

Spotlight

XZERES Wind Turbine
XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

PIPS Automated License Plate Reader
The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.
### OT cybersecurity for manufacturers

<table>
<thead>
<tr>
<th>Smart Factory</th>
<th>Attack Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile workers and smartphone controllers</td>
<td>User attitudes inside/outside of the plant</td>
</tr>
<tr>
<td>Cloud systems</td>
<td>No perimeter security for the data</td>
</tr>
<tr>
<td>24/7 smart maintenance</td>
<td>Key data residing where??</td>
</tr>
<tr>
<td>Legacy systems, complex transition to new working</td>
<td>Reduced investment in older systems opens up a door</td>
</tr>
<tr>
<td>New capital equipment</td>
<td>Will want to access the internet (see above!)</td>
</tr>
</tbody>
</table>
The myth about air gaps

**IN THEORY**

Air gap

**IN PRACTICE**

Network diagrams showing potential security vulnerabilities and the concept of air gaps.
Agenda

- Modern industrial cybersecurity risk
- Functional safety and cybersecurity
- Assessing your cybersecurity risk
Functional safety and cybersecurity

**Cybersecurity**
Defence against negligent and wilful actions to protect devices and facilities

**Functional Safety**
Defence against random and systematic technical failure to protect life and environment
Relationship between functional safety & cybersecurity


7.4.2.3 If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out.

NOTE 3 For guidance on security risks analysis, see IEC 62443 series.

7.5.2.2 If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements.

NOTE Guidance is given in IEC 62443 series.
Requirements for Cybersecurity.
Foundational Requirements for Product Development according to IEC 62443.

FR 7 – Resource availability
FR 6 – Timely response to events
FR 5 – Restricted data flow

FR 1 – Identification and authentication control
FR 4 – Data Confidentiality
FR 3 – System integrity

FR 2 – User control
Operator
Administrator

Patch
IEC 62443
PLC
IACS
# Lifecycle for Functional Safety and Cybersecurity

## Functional Safety
**IEC 61508**

### Safety Integrity Level (SIL) 1 – 4

<table>
<thead>
<tr>
<th>Probability of a dangerous failure in:</th>
<th>SIL 1</th>
<th>≈ 10 years</th>
<th>SIL 2</th>
<th>≈ 100 years</th>
<th>SIL 3</th>
<th>≈ 1,000 years</th>
<th>SIL 4</th>
<th>≈ 10,000 years</th>
</tr>
</thead>
</table>

### Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Concept</td>
</tr>
<tr>
<td>2</td>
<td>Overall scope definition</td>
</tr>
<tr>
<td>3</td>
<td>Overall safety &amp; security requirements allocation</td>
</tr>
<tr>
<td>4</td>
<td>Overall safety &amp; security requirements</td>
</tr>
<tr>
<td>5</td>
<td>Specification of E/E/PE System</td>
</tr>
<tr>
<td>6</td>
<td>Realization of E/E/PES Systems</td>
</tr>
<tr>
<td>7</td>
<td>Overall installation and commissioning</td>
</tr>
<tr>
<td>8</td>
<td>Overall validation</td>
</tr>
<tr>
<td>9</td>
<td>Overall operation, maintenance and repair</td>
</tr>
<tr>
<td>10</td>
<td>Decommissioning</td>
</tr>
</tbody>
</table>

## Cyber Security
**IEC 62443**

### Security Level (SL) 1 – 4

<table>
<thead>
<tr>
<th>Security Level (SL) 1 – 4</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SL 1</td>
<td>Protection against casual or coincidental violation</td>
</tr>
<tr>
<td>SL 2</td>
<td>Protection against intentional violation using simple means</td>
</tr>
<tr>
<td>SL 3</td>
<td>Protection against intentional violation using sophisticated means</td>
</tr>
<tr>
<td>SL 4</td>
<td>Protection against intentional violation using sophisticated means with extended resources</td>
</tr>
</tbody>
</table>

### Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Concept</td>
</tr>
<tr>
<td>2</td>
<td>Overall scope definition</td>
</tr>
<tr>
<td>3</td>
<td>Overall safety &amp; security requirements allocation</td>
</tr>
<tr>
<td>4</td>
<td>Overall safety &amp; security requirements</td>
</tr>
<tr>
<td>5</td>
<td>Specification of E/E/PE System</td>
</tr>
<tr>
<td>6</td>
<td>Realization of E/E/PES Systems</td>
</tr>
<tr>
<td>7</td>
<td>Overall installation and commissioning</td>
</tr>
<tr>
<td>8</td>
<td>Overall validation</td>
</tr>
<tr>
<td>9</td>
<td>Overall operation, maintenance and repair</td>
</tr>
<tr>
<td>10</td>
<td>Decommissioning</td>
</tr>
</tbody>
</table>

---

**Hazard and risk analysis**

**Risk and Threat analysis**
Triton – a seminal moment
Reported December 2017

- The attacker gained remote access to a safety instrumented system (SIS) engineering workstation and deployed the TRITON attack framework to reprogram Triconex SIS controllers
- SIS controllers entered a failed safe state
- Target – CNI but otherwise not publicly revealed (likely ME)
- Attribution – not publicly revealed (likely nation state)

Source: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
Agenda

- Modern industrial cybersecurity risk
- Functional safety and cybersecurity
- Assessing your cybersecurity risk
Risk assessments

- **Manufacturers** – risk assess your components (i.e. PLC) or systems
- **Systems integrators** – risk assess your solution to meet an operator’s specifications
- **Systems Operators** – risk assess plant operations, factory operations, or your production facilities
Risk assessment approaches

**NIST**
- Allows you to determine how identified risks are managed
- Will define how your organization stacks up at a high level against existing OT/cybersecurity standards, guidelines, and practices.
- Will help answer the question “How are we doing?”
- Will help you move in a more informed way to strengthen OT/cybersecurity practices

**IEC 62443**
- Provides an assessment against industry standard for OT systems
- Based on 7 foundational requirements
- Can provide a security level (SL)
- Can be used by manufacturers, systems integrators or systems operators
Findings and recommendations

- **Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; the information is used to inform cybersecurity risks, responsibilities, and risk management decisions.

- **Governance (ID.GV):** Policies, procedures, and processes to manage and monitor the organization's regulatory, legal, and compliance requirements.

- **Risk Ratings by Category:**

  - **Identify:**
  - **Detect:**
  - **Respond:**
  - **Recover:**

- **Total Risk Ratings:**

- **Individual Control System Requirements:**

  - SR 1.1: Unique user identification and authentication
  - SR 1.2: Software process and device identification and authentication
  - SR 1.3: Account management
  - SR 1.4: Identifier management
  - SR 1.5: Authentication management
  - SR 1.6: Wireless access management
  - SR 1.7: Strength of password-based authentication
  - SR 1.8: Public key infrastructure certificates
  - SR 1.9: Authentication feedback
  - SR 1.10: Unsuccessful login attempts
  - SR 1.11: Use of untrusted networks
  - SR 1.12: Access via untrusted networks
  - SR 1.13: Explicit access request approval

- **Total Risk Ratings:**

  - High: 15%
  - Medium: 28%
  - Low: 31%
  - NA: 25%
Next steps

- Understand your risk by conducting an assessment on your plants, factories, products or sites

- Regularly monitor new and emerging cyber risks on your OT network

- Understand how new connected systems can enhance productivity and safety if properly implemented

- Review and watch for new and emerging legislation and regulations that may impact cybersecurity in your industry – including data privacy
Thank you

Nigel Stanley
Chief Technology Officer
Operational Technology and Industrial Cybersecurity
TÜV Rheinland
E: nigel.stanley@us.tuv.com