Structured Approach to Functional Safety and Cyber Security
Industrial Applications

Dipl.-Ing. Heinz Gall
Business Line Manager, Certification Body - Functional Safety & Cyber Security
TÜV Rheinland Industrial Service
Agenda.

1. Introductions – who we are and why we care
2. What is Functional Safety and why bother?
3. Functional Safety vs. Cyber Security
4. Overview of IEC 61508 and IEC 62443 standards
5. Where to go from here
Automation has an influence in any technical area and development.

In order to have safe and secure applications the following main topics must be addressed.

- Qualified and reliable products.

- Safety and Security Management throughout all life cycle phases.

- Competent people involved in any activity.
Objectives of Safe & Secure Applications

- Your management has to be aware of these topics and the impact they will have on your business and services.
- They need to consider costs for additional time and investments.
- They should give safety and security top priority and support all required activities regarding safety and security management.

The main service groups and deliverables of the business area Automation, Functional Safety & Cyber Security of TÜV Rheinland are focused on these topics.
Business Area

Automation - Functional Safety & Cyber Security

Products  Systems  Applications  Qualification

Functional Safety & Cyber Security

Test and Certification  Functional Safety Management Certification  Application and System Implementation  Trainings and Workshops  TÜV Rheinland FS Program

Application Areas:
Machinery, Oil & Gas, Process Industry, Automotive, Power Plants etc.

Accreditations

<table>
<thead>
<tr>
<th>Certification Body</th>
<th>DIN EN ISO/IEC 17065:2013</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>▪ Functionally safe products, applications and systems including Functional Safety Management Systems</td>
</tr>
<tr>
<td></td>
<td>▪ Security</td>
</tr>
</tbody>
</table>

Accreditation Number  D-ZE-11052-02-00
Functional Safety.
Why do random faults have to be controlled?

Sensor-signal

TRIP

TRIP

Actual vibration
Functional Safety.
Why do random faults have to be controlled?
Functional Safety.
Why do random faults have to be controlled?

STOP

“0”

Bit fault

1110 0101b

ON!

**Cyber Security**
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
It’s all about risk. Corporate IT / ICS

<table>
<thead>
<tr>
<th>Corporate IT Systems</th>
<th>Industrial Control Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data confidentiality and integrity is number 1</td>
<td>Human safety, closely followed by process protection is number 1</td>
</tr>
<tr>
<td>Availability <strong>may</strong> not be a major business risk</td>
<td>Availability is <strong>normally</strong> a major business risk</td>
</tr>
<tr>
<td>Major risk <strong>may</strong> be a delay or reduction in business processes</td>
<td>Major risk <strong>may</strong> be loss of life or destruction of production plants, environmental damage</td>
</tr>
<tr>
<td>Performance <strong>may</strong> not be an issue (i.e. email can be delayed a few seconds)</td>
<td>Poor performance can impact an industrial process or cause major safety issues</td>
</tr>
<tr>
<td>System lifetime often only 2 – 3 years</td>
<td>System lifetime may be 10 – 30+ years</td>
</tr>
<tr>
<td>System patching and update is a regular occurrence</td>
<td>System may never or very infrequently be updated</td>
</tr>
</tbody>
</table>

❗ Applying corporate IT tools, techniques and procedures to industrial control systems can be disastrous!
It’s not all about power stations ...

Corporate IT Systems

- BMS Workstation (Windows 7)
- BMS Enterprise Server
- BMS/AC Workstation (Windows 7)

- Dedicated ADSL Connection
- BMS Network Switch
- Internet
- GSM/3G remote link

Industrial Control Systems

- Door Controllers
- Physical Access Control System
- CCTV System
- Controllers
- HVAC, Chillers
- Controllers
- HVAC, Chillers
- Controllers
- HVAC, Chillers

HVAC, Boilers, Chillers

Physical Access Control System

CCTV System

05.07.2017

Structured Approach to Functional Safety and Cyber Security

TÜV Rheinland®
Precisely Right.
Requirements for Cyber Security.
Functional 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

To achieve these goals it is required: **Security by Design!**
Requirements for Functional Safety.

To achieve the Safety Integrity with
- Hardware Architecture → HFT
- Good Diagnostic Measures → DC
- Low Dangerous Failure Rates → $\lambda_{DU}$, $PFD_{avg}$, PFH, PL

Guidance how to use
- Safety manual, Installation guide

To achieve the Systematic Safety Integrity with
- Functional Safety Management means avoidance of systematic faults in all life cycle phases to achieve the “Systematic Capability” → SC

To achieve these goals it is required: **Functional Safety by Design!**
Relation between Functional Safety & Cyber Security.

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.
### Lifecycle for Functional Safety and Cyber Security

#### Functional Safety
IEC 61508

- **1** Concept
- **2** Overall scope definition
- **3** Hazard and risk analysis
- **4** Overall safety & security requirements
- **5** Overall safety & security requirements allocation
- **9** Specification of E/E/PE System
- **10** Realization of E/E/PES Systems
- **12** Overall installation and commissioning
- **13** Overall validation
- **14** Overall operation, maintenance and repair
- **16** Decommissioning

#### Cyber Security
IEC 62443

- **1** Concept
- **2** Overall scope definition
- **3** Hazard and risk analysis
- **4** Overall safety & security requirements
- **5** Overall safety & security requirements allocation
- **9** Specification of E/E/PE System
- **10** Realization of E/E/PES Systems
- **12** Overall installation and commissioning
- **13** Overall validation
- **14** Overall operation, maintenance and repair
- **16** Decommissioning

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

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

### Security Level (SL) 1 – 4

<table>
<thead>
<tr>
<th>Level</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>
Software Safety Development Lifecycle (the V-model).

- E/E/PE system safety requirements specification
- Software safety requirements specification
- Validation testing
- HW/SW-integration testing
- E/E/PE system architecture
- Software architecture
- Software system design
- Module design
- Module testing
- Coding
- Integrated Software

Output
Verification
Software Security Dev. lifecycle (simplified V-model).
Created by TÜV Rheinland based on IEC 62443 – Lifecycle phases 9 – 10.
### Functional Safety

<table>
<thead>
<tr>
<th>Product Design and Manufacturing Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Review of Functional Safety Management</td>
</tr>
<tr>
<td>▪ Review of safety concept → FMEA</td>
</tr>
<tr>
<td>▪ Review of SW-verification tests</td>
</tr>
<tr>
<td>▪ Review of HW-verification tests</td>
</tr>
<tr>
<td>▪ Review of calculation of safety related parameters</td>
</tr>
<tr>
<td>▪ Tests of safety related functions</td>
</tr>
<tr>
<td>▪ Fault insertion tests</td>
</tr>
</tbody>
</table>

### Cyber Security

<table>
<thead>
<tr>
<th>Product Support and On-Going Maintenance Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Reviews of modifications</td>
</tr>
<tr>
<td>▪ Review of impact analysis</td>
</tr>
<tr>
<td>▪ Evaluation of all modified functions</td>
</tr>
<tr>
<td>▪ Review of HW/SW-tests</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Review of security design</td>
</tr>
<tr>
<td>▪ Perform penetration and dynamic testing</td>
</tr>
<tr>
<td>▪ Conduct hazard analysis</td>
</tr>
<tr>
<td>▪ Creation of a Traceability Risk Matrix</td>
</tr>
<tr>
<td>▪ Secure code review</td>
</tr>
<tr>
<td>▪ Penetration and dynamic testing to identify vulnerabilities</td>
</tr>
<tr>
<td>▪ Review components for potential Cyber Security weaknesses</td>
</tr>
<tr>
<td>▪ Review and suggest appropriate security controls</td>
</tr>
</tbody>
</table>

### Product Design and Manufacturing Phase

- Reviews of modifications
- Review of impact analysis
- Evaluation of all modified functions
- Review of HW/SW-tests

### Product Support and On-Going Maintenance Phase

- Data breach response planning
- Legal and regulatory assessments
- Software updates and patches
- Determine vulnerable design inter-sections within the device architecture
## Integrated Functional Safety and Cyber Security

IEC 62443 & IEC 61508 requirements for **Systems Integrators**:

### Functional Safety
- Review of Functional Safety Management-Processes
- Review of the application design and safety concept
- Review of Safety risk assessment
- Verification of the safety-loops
- Evaluation of Application software
- Witness test at factory acceptance test

### Cyber Security
- Perform penetration and dynamic testing
- Determine vulnerable design intersections within the device architecture
- Analysis of the device source code
- Creation of a Traceability Risk Matrix
- Secure code review
- Penetration and dynamic testing to identify vulnerabilities

### System Design and Architecture Phase
- System/hardware safety validation
- Software safety review
- Site acceptance testing

### System Installation and Setup Phase
- Review components for potential Cyber Security weaknesses
- Review and suggest appropriate security controls
Integrated Functional Safety and Cyber Security. IEC 62443 & IEC 61508 requirements for Systems Operators:

### Systems Operation and On-Going Maintenance Phase

<table>
<thead>
<tr>
<th>Functional Safety</th>
<th>Cyber Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reviews of Modifications</td>
<td>Data breach response planning</td>
</tr>
<tr>
<td>Review of Impact analysis</td>
<td>Legal and regulatory assessments</td>
</tr>
<tr>
<td>Evaluation of all modified functions and documents</td>
<td>Management of software updates and patches</td>
</tr>
<tr>
<td>Review of HW/SW-tests</td>
<td>Determine vulnerable design intersections within the device architecture</td>
</tr>
</tbody>
</table>

TÜV Rheinland Certification:
Functional Safety & Cyber Security.

Kick-Off (optional)
Verification of documents
Main Assessment (Implementation)
Elimination of NCs (LOP)
Certification

Concept Assessment (GAP analysis)
Elimination of NCs (LOP)
Testing
Certification Decision

IEC 61508
IEC 62443
IEC 62443
IEC 62443
IEC 61508
Risk management is more than a certification …

**Additional value and risk mitigation**
using state of the art tools, techniques and processes to achieve Security Level 3 and 4

IEC 62443 and ISA Secure to Security Levels 1 and 2 Core Certification Requirements

**Evaluation of Security Concept**
- Evaluation of Security Risk Analysis
- Evaluation of Security Development Process
- Review of Functional Security Features
- Vulnerability Test
- Robustness Test
- Penetration Test

**Review of Functional Security Features**
- Review and Evaluation of Security in Depth Strategy
- Network Security Evaluation
- System Vulnerability Scan
- System Penetration Test
We have seen that …

Functional Safety and Cyber Security Standards consider the product lifecycle from specification over design to operation and maintenance:
- This requires risk and threat analysis!
- Need to specify safety and security levels!
- Requires organizational and technical measures!
- Need to consider fault avoidance and fault control!

Operators push requirements of Cyber Security – The regulation by law will follow!

No Safety without security!

The solution is: **Safety & Security by Design!**
Finally … What now…

<table>
<thead>
<tr>
<th>Product Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Consider how Functional Safety and Cyber Security issues are dealt within your</td>
</tr>
<tr>
<td>products, from design to installation and beyond</td>
</tr>
<tr>
<td>▪ Think beyond just being compliant – risk management is more than compliance</td>
</tr>
<tr>
<td>▪ Ensure that you are safe and secure by design</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Integrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Ensure that you manage Functional Safety and Cyber Security risks in your</td>
</tr>
<tr>
<td>system design</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Check that you have safety and security manuals for your systems &amp; products</td>
</tr>
<tr>
<td>▪ Ensure that you maintain a safe and secure operation</td>
</tr>
<tr>
<td>(you need manuals!)</td>
</tr>
<tr>
<td>▪ Track the changing nature of cyber threats</td>
</tr>
</tbody>
</table>

⚠️ Thank you very much for your attention !!!
Contact Details.

**Heinz Gall**

**Business Line Manager**  
**Head of Certification Body**  
**Functional Safety & Cyber Security**

TÜV Rheinland Industrie Service GmbH  
Automation and Functional Safety  
Am Grauen Stein  
51105 Cologne, Germany

gall@de.tuv.com

**Giorgio Puglia**

**Product Manager**  
**Functional Safety**

TÜV Rheinland Italy S.r.l.  
Automation and Functional Safety  
via Mattei, 3  
20010 Pogliano Milanese

Giorgio.Puglia@it.tuv.com