15^{th} International TUV Rheinland Symposium

Functional Safety and Cybersecurity in Industrial Automation

Summary and Highlights

Rodrigo Ferreira | rodrigo.ferreira@cern.ch

TUV

About the Organization

TÜVs (*Technischer Überwachungsverein*, English: Technical Inspection Association) are internationally active, independent service companies from Germany and Austria that test, inspect and certify technical systems, facilities and objects of all kinds in order to minimize hazards and prevent damages.

Wikipedia

TÜVRheinland®

Precisely Right.

- Performs technical testing and certification in systems and products, in the areas of safety, efficiency and quality.
- Trains and certifies people in international standards (e.g. IEC 61511)
- Organizes trainings, seminars and events.

15th International TUV Rheinland Symposium

Functional Safety and Cybersecurity in Industrial Automation

TOPICS

- Functional Safety and Cybersecurity
- Safety for Energy Storage Systems
- Safety of Machinery
- AI Artificial Intelligence
- Management Process and -Systems

https://www.tuv.com/landingpage/en/functional-safety-meets-cybersecurity/meta-navigation/events/

Conference Program

First Day | Cyber Security

Networked Security: New Perspectives of Functional Safety and Cybersecurity in Industry
Dr. Thorsten Gantevoort, Felix Brombach
TÜV Rheinland i-sec GmbH - Germany

Cyber Attacks and Industrial Risks under the new EU Product Liability Directive
Prof. Dr. Thomas Klindt
Noerr - Rechtsanwälte – Germany

New European Security Regulations with Relevance for the Industry
Vanessa Bellinghausen, Björn Flubacher
Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Federal Office for Information Security - Germany

The Machinery Regulation (EU) 2023/1230 and the Introduction of Cyber Security Requirements
David Main-Reade
Rockwell Automation – United Kingdom

Automated Hazard and Risk Assessment for a Flexible Production
Philip Kleen
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB - Germany

Using Digital Device IDs for Industrial IoT under the Cyber Resilience Act
Dr. Michael Jahnich
achelos GmbH – Germany

Vulnerability Management and Prioritization in Industrial Systems: Making the Right Choice
Odei Olalde, Salvador Trujillo
ORBIK - Spain

Cooperation with the German Police in Case of a Cyber Attack
Jan Eckert
Bundeskriminalamt - Nationale Kooperationsstelle Cybercrime (NKC)
German Federal Criminal Police Office - National Cybercrime Cooperation Centre (NKC)

Plant Availability and Cyber Security - Does this work together?
Mirco Kloss
TXOne Networks Europe B.V. - Germany

Leveraging the Human Factor for the Enhancement of SIS Cyber Security
Daryl Wheatley
MWS Risk Pty Ltd. – United Kingdom

Safe Human-Robot Collaboration: An Overview of Key Standards and Recent Changes
Dr. Saeed Abdolshah
KUKA Deutschland GmbH - Germany

PKI ready Battery Powered Field Devices – What did we Learn?
Sushil Siddesh
Endress+Hauser Flowtec AG - Switzerland

Product / Type Certification for Green Hydrogen Electrolysis - New Wine in Old Bottles?
Werner Fellner, Hubertus Rosenow
thyssenkrupp nucera AG & Co. KGaA - Germany

Importance of Cybersecurity in achieving Safety

Functional Safety and Cybersecurity – An Overview

Cyber Security

Defense against negligent and intentional acts to protect devices and systems

Functional Safety

Defense against accidental and systematic technical failures to protect life and the environment

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 3

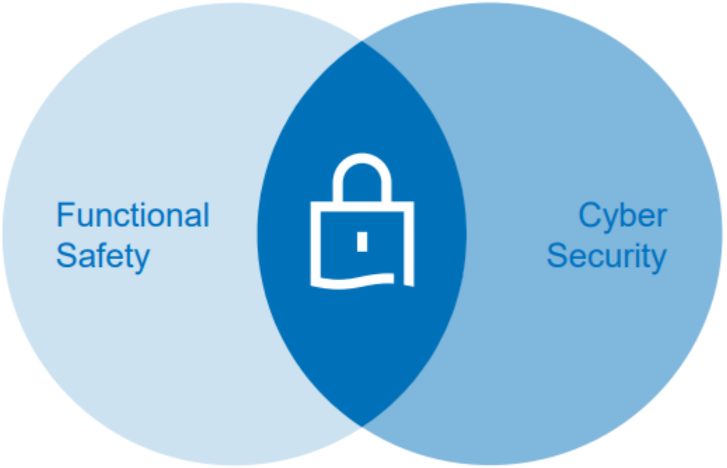
TÜVRheinland®
Precisely Right.

Networked Security: New Perspectives of Functional Safety and Cybersecurity in Industry
Dr. Thorsten Gantevoort, Felix Brombach
TÜV Rheinland i-sec GmbH - Germany

Importance of Cybersecurity in achieving Safety

Functional Safety and Cybersecurity – An Overview

Similarities & Differences



Both provide protection – but in different ways

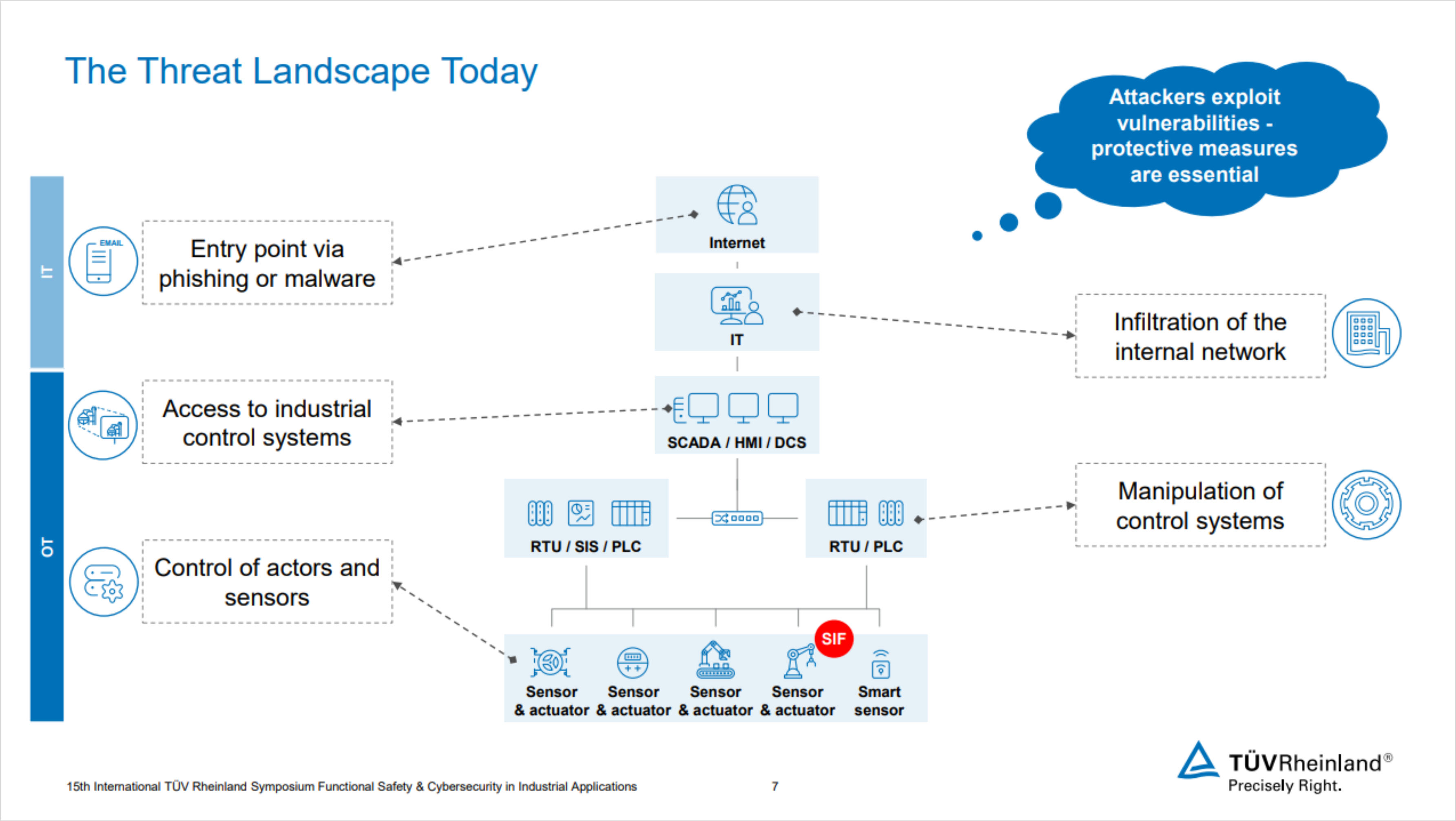
- Protection of Humans and Machines
  Both fields aim to protect humans and machines from potential dangers
- Avoidance of Failures
  The goal is to maintain safe operations
- Proactive Planning
  Both focus on preventive measures to avoid disruptions and security incidents
- Detection and Response
  Both fields employ mechanisms for quick detection and response

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 4

TÜVRheinland®
Precisely Right.

Networked Security: New Perspectives of Functional Safety and Cybersecurity in Industry
Dr. Thorsten Gantevoort, Felix Brombach
TÜV Rheinland i-sec GmbH - Germany

Importance of Cybersecurity in achieving Safety



Networked Security: New Perspectives of Functional Safety and Cybersecurity in Industry
Dr. Thorsten Gantevoort, Felix Brombach
TÜV Rheinland i-sec GmbH - Germany

New Perspectives on Functional Safety

Current Trends

Functional Safety Approach for new Challenges

SOTIF

- Ensures safety when systems work as intended, unlike functional safety's focus on failures
- Addresses unknown risks from rare or unforeseen situations
- Uses scenario-based testing instead of traditional component-level methods
- Designed for autonomous systems, managing complex and unpredictable environments

AI in Safety-Critical Systems

- Bias, ethics, and fairness concerns in AI affecting life-critical decisions
- Traditional methods don't fully apply to AI due to its non-deterministic nature
- Additional activities required like data pre-processing, machine learning, and validation
- Complex risk assessment needed to ensure safe and ethical AI deployment

TÜVRheinland®
Precisely Right.

Networked Security: New Perspectives of Functional Safety and Cybersecurity in Industry
Dr. Thorsten Gantevoort, Felix Brombach
TÜV Rheinland i-sec GmbH - Germany

New Perspectives on Functional Safety

Current Trends

Cybersecurity Approach for new Challenges

Defensive AI

- Automated threat detection and response using machine learning
- Predictive analytics to foresee and prevent potential cyber-attacks
- Utilization of Natural Language Processing (NLP) for threat intelligence analysis
- Self-learning systems for continuous improvement of security measures

Zero Trust

- "Never trust, always verify" – No inherent trust within the network
- Strict authentication and authorization for every access request
- Micro-segmentation to reduce attack surface and limit lateral movement of threats
- Continuous monitoring and evaluation of user activities and access rights

TÜVRheinland®
Precisely Right.

Networked Security: New Perspectives of Functional Safety and Cybersecurity in Industry
Dr. Thorsten Gantevoort, Felix Brombach
TÜV Rheinland i-sec GmbH - Germany

European Directives and Cybersecurity Standards

NIS2, CRA, IEC62443, …

Regulation and Standardization

European examples	National examples	Standardization examples
▪ NIS Directive 2.0 (EU 2016/1148) ▪ Cybersecurity Act (EU 2019/881) ▪ *Cyber Resilience Act* ▪ *Machinery Regulation (EU 2023/1230)* → ENISA	▪ IT-Sicherheitsgesetz (IT-SiG 2.0) ▪ Kritische Infrastruktur (BSI-KritisV) ▪ Kritische Infrastruktur (APCIP) ▪ Informationssicherheitsgesetz (ISG)	▪ ISO/IEC 27001 (Info Sec.) ▪ IEC 62443 (OT Security) ▪ ISO/IEC 27019 (Energy) ▪ ISO/SAE 21434 (Cars) → ISO, IEC

European Union Agency for Cybersecurity

NIS - Network and Information Security
BSI - Bundesamt für Sicherheit in der Informationstechnik
APCIP - Österreichisches Programm zum Schutz kritischer Infrastrukturen

International Organization for Standardization (ISO)

International Electrotechnical Commission (IEC)

Plant Availability and Cyber Security - Does this work together?
Mirco Kloss
TXOne Networks Europe B.V. - Germany

European Directives and Cybersecurity Standards

NIS2

NIS 2 – Risk Management and Reporting Requirement

Bundesamt für Sicherheit in der Informationstechnik

Risk-based uniform security measures for "essential" and "important" entities (Art. 18):

- Risk analyses and ISMS
- Business continuity management/crisis management
- Supply chain security
  - Security measures for the acquisition, development and maintenance of network and information systems, including management and disclosure of vulnerabilities
- Policies for recording the "effectiveness of CS risk management measures"
- Commitment to the use of cryptography and encryption

Harmonizede Reporting Obligations (Art. 20)

- Member States to inform each other and ENISA of incidents with cross-border nature

Responsibility of TOP-Management/CEO level (Art. 17)

5

TÜVRheinland® Precisely Right.

New European Security Regulations with Relevance for the Industry
Vanessa Bellinghausen, Björn Flubacher
Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Federal Office for Information Security - Germany

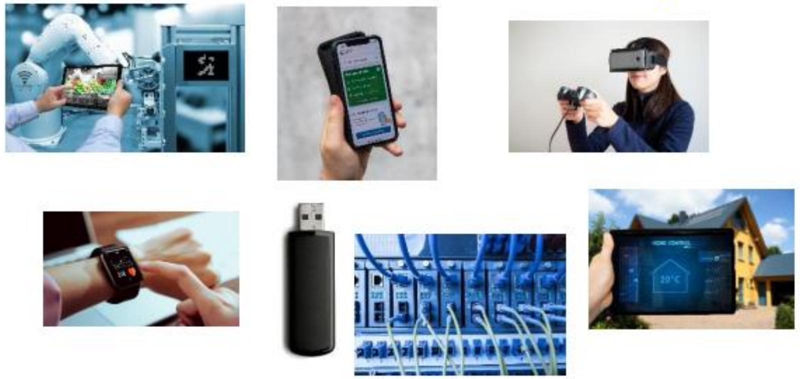
European Directives and Cybersecurity Standards

Cyber Resilience Act

Cyber Resilience Act

Market Access Regulation for Products with Digital Elements

Bundesamt
für Sicherheit in der
Informationstechnik



Newly placed on the market:

- **Hardware**
- **Software**

Not covered:

- **Non-commercial projects,** including ***open source***
- **Services**, in particular cloud/Software-as-a-service – *covered by NIS2*
- **Product categories sufficiently regulated on cybersecurity** (cars, medical devices, in vitro, certified aeronautical equipment etc.)

Machine ordinance ?

14

TÜVRheinland®
Precisely Right.

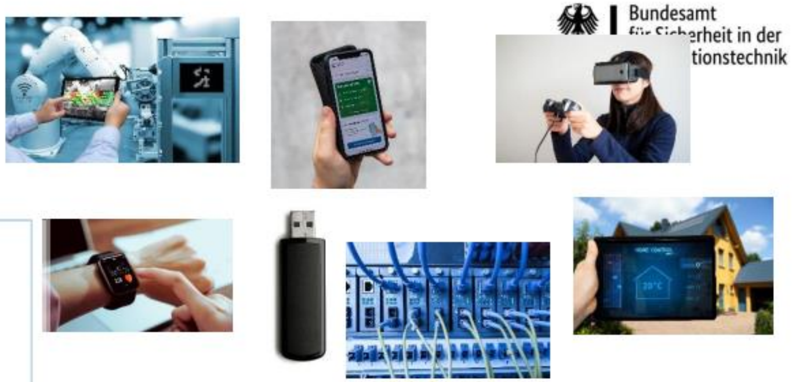
New European Security Regulations with Relevance for the Industry
Vanessa Bellinghausen, Björn Flubacher
Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Federal Office for Information Security - Germany

European Directives and Cybersecurity Standards

Cyber Resilience Act - Requirements

Cyber Resilience Act

Essential Requirements



Security requirements relating to the properties of products with digital elements

- Security-by-design, Security-by-default
- protection from unauthorised access; protection of confidentiality and integrity of data
- designed, developed and produced to limit attack surfaces [...]

Vulnerability management

- SBOM at the very least of the top-level dependencies of the product;
- Address and remediate vulnerabilities without delay, including by providing security updates
- Public disclose of information about fixed vulnerabilities, information allowing users to identify the product [...]

Minimum information for the user

- Contact information where cybersecurity vulnerabilities of the product can be reported and received
- Identification of product
- Possibility to asses conformity information and if made available SBOM [...]

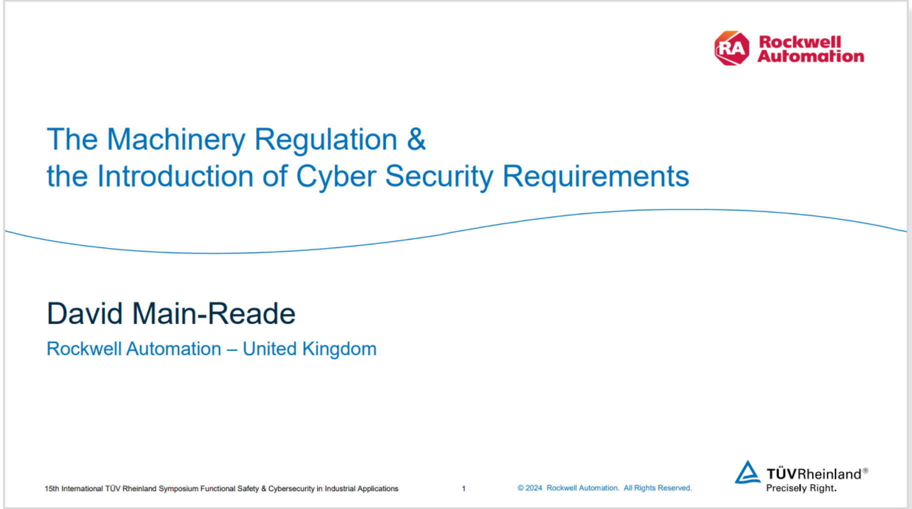
15

TÜVRheinland®
Precisely Right.

New European Security Regulations with Relevance for the Industry
Vanessa Bellinghausen, Björn Flubacher
Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Federal Office for Information Security - Germany

European Directives and Cybersecurity Standards

Cyber Security Requirements



A good summary of the topic of can be found in the following presentation:

The Machinery Regulation (EU) 2023/1230 and the Introduction of Cyber Security Requirements
David Main-Reade
Rockwell Automation – United Kingdom

Software Bill of Materials

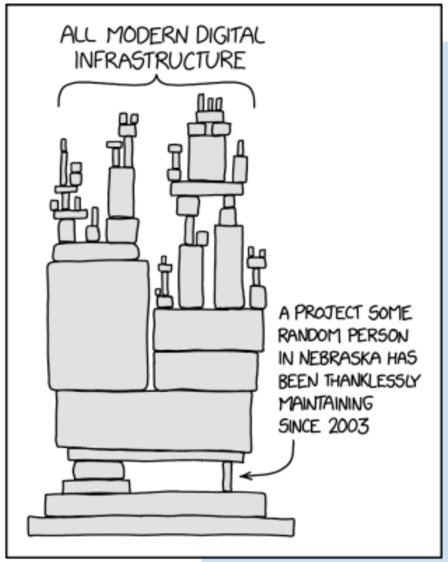
Requirement for CRA

Cyber Resilience Act

Bundesamt
für Sicherheit in der
Informationstechnik

SBOM is part of essential requirements

- SBOM: Information about software components contained in a product
  - to track known newly emerged vulnerabilities and risks
- SBOM should cover at the very least the top-level dependencies of the product
- **The market surveillance authority may request the SBOM**, provided that it is necessary in order for this authority to be able to check compliance with the essential requirements
- **The Commission may specify format and elements of the SBOM**



https://imgs.xkcd.com/comics/dependency_2x.png

16

TÜVRheinland®
Precisely Right.

New European Security Regulations with Relevance for the Industry

Vanessa Bellinghausen, Björn Flubacher

Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Federal Office for Information Security - Germany

Software Bill of Materials

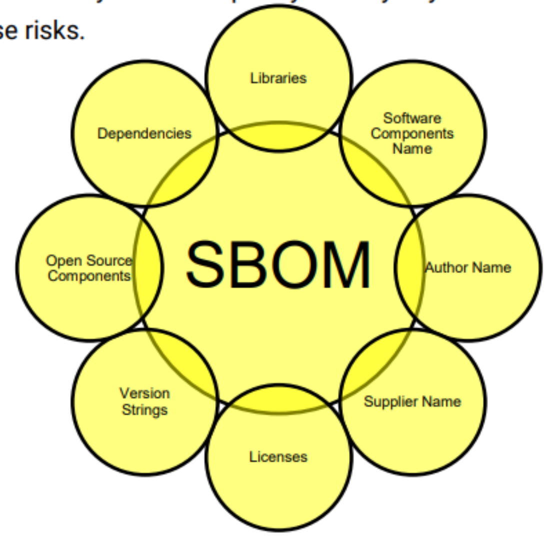
Automated Vulnerability Assessment

SBOM

Orbik

What is it?

A software Bill of Materials (SBOM) is a list of all the open source and third-party components present in a codebase. An SBOM also lists the licenses that govern those components, the versions of the components used in the codebase, and their patch status, which allows security teams to quickly identify any associated security or license risks.




```json
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.4",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "components": [
    {
      "type": "application",
      "name": "Acme Application",
      "version": "9.1.1",
      "cpe": "cpe:/a:acme:application:9.1.1",
      "swid": {
        "tagId": "swidgen-242eb18a-503e-ca37-393b-cf156ef09691_9.1.1",
        "name": "Acme Application",
        "version": "9.1.1",
        "text": {
          "contentType": "text/xml",
          "encoding": "base64",
          "content": "PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiID8+
        }
      }
    },
    {
      "type": "library",
      "group": "org.apache.tomcat",
      "name": "tomcat-catalina",
      "version": "9.0.14",
      "purl": "pkg:maven/org.apache.tomcat/tomcat-catalina@9.0.14"
    }
  ]
}
```


TÜVRheinland®
Precisely Right.

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 8

Vulnerability Management and Prioritization in Industrial Systems: Making the Right Choice
Odei Olalde, Salvador Trujillo
ORBIK - Spain

Software Bill of Materials

Automated Vulnerability Assessment

SBOM

Orbik

Metrics

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 10

TÜVRheinland®
Precisely Right.

Vulnerability Management and Prioritization in Industrial Systems: Making the Right Choice

Odei Olalde, Salvador Trujillo

ORBIK - Spain

Software Bill of Materials

Automated Vulnerability Assessment

Prioritization

Orbik

Ready to go

Vulnerabilities

EXPORT

☐	Identifier	Score	Revised Score	Priority	EPSS	Supre...	KEV	Status	Assessment	Product	Tags	Version	Client	Actions
☐	CVE-2022-1292	9.8 Critical	9.8 Critical	3	0,125	☐	☑	Detected	SCA	Blue		1.0	adm...	
☐	CVE-2022-2068	9.8 Critical	9.8 Critical	3	0,123	☐	☑	Detected	SCA	Blue		1.0	adm...	
☐	CVE-2022-3602	7.5 High	7.5 High	3	0,102	☐	☐	Detected	SCA	Blue		1.0	adm...	
☐	CVE-2023-0215	7.5 High	7.5 High	3	0,006	☐	☐	Detected	SCA	Blue		1.0	adm...	
☐	CVE-2023-0401	7.5 High	7.5 High	3	0,005	☐	☐	Detected	SCA	Blue		1.0	adm...	
☐	CVE-2023-2975	5.3 Medi...	5.3 Medi...	5	0,005	☐	☐	Detected	SCA	Blue		1.0	adm...	
☐	CVE-2022-2097	5.3 Medi...	5.3 Medi...	5	0,004	☐	☐	Detected	SCA	Blue		1.0	adm...	
☐	CVE-2023-0464	7.5 High	7.5 High	3	0,004	☐	☐	Detected	SCA	Blue		1.0	adm...	
☐	CVE-2023-0286	7.4 High	7.4 High	3	0,003	☐	☐	Detected	SCA	Blue		1.0	adm...	
☐	CVE-2023-3817	5.3 Medi...	5.3 Medi...	5	0,003	☐	☐	Detected	SCA	Blue		1.0	adm...	

Rows per page: 10 1–10 of 30

TÜVRheinland®
Precisely Right.

Vulnerability Management and Prioritization in Industrial Systems: Making the Right Choice

Odei Olalde, Salvador Trujillo
ORBIK - Spain

Zero Trust approach in OT Networks

Digital Device IDs and PKI

Using Digital Device IDs for Industrial IoT under the Cyber Resilience Act

achelos

What are Digital Device IDs?

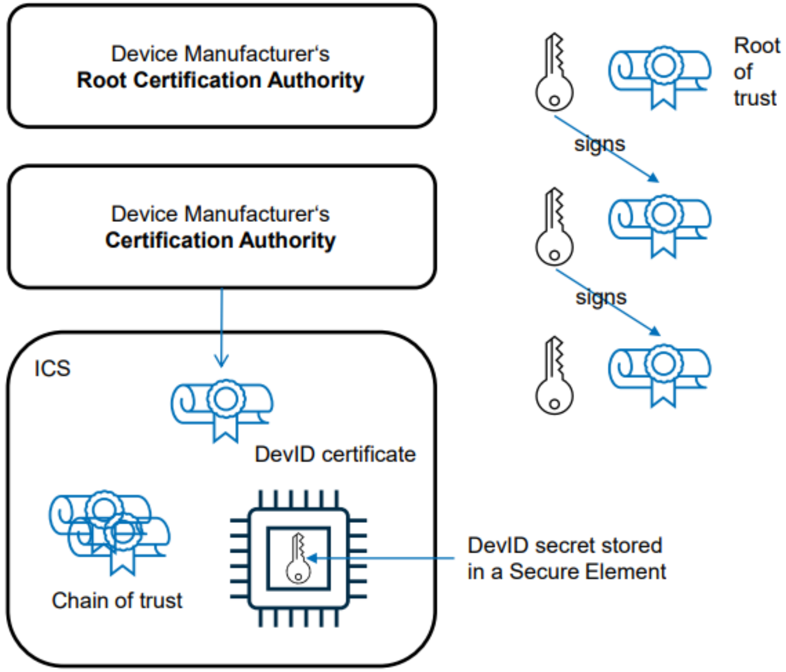
IEEE Std 802.1AR on Secure Device IDs:

"A device identifier that is **cryptographically bound to the device**, and comprises a DevID **secret**, a signed DevID **certificate** that binds possession of that secret to a statement of identity made by the certificate's issuer, and (as required by authenticating systems) a certificate **chain** that links the certificate to a **trust anchor**."

We need public-key cryptography!

A private key connected to a public key certified by a certificate

Technology based on X.509 V3 standard



15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 5

TÜVRheinland®
Precisely Right.

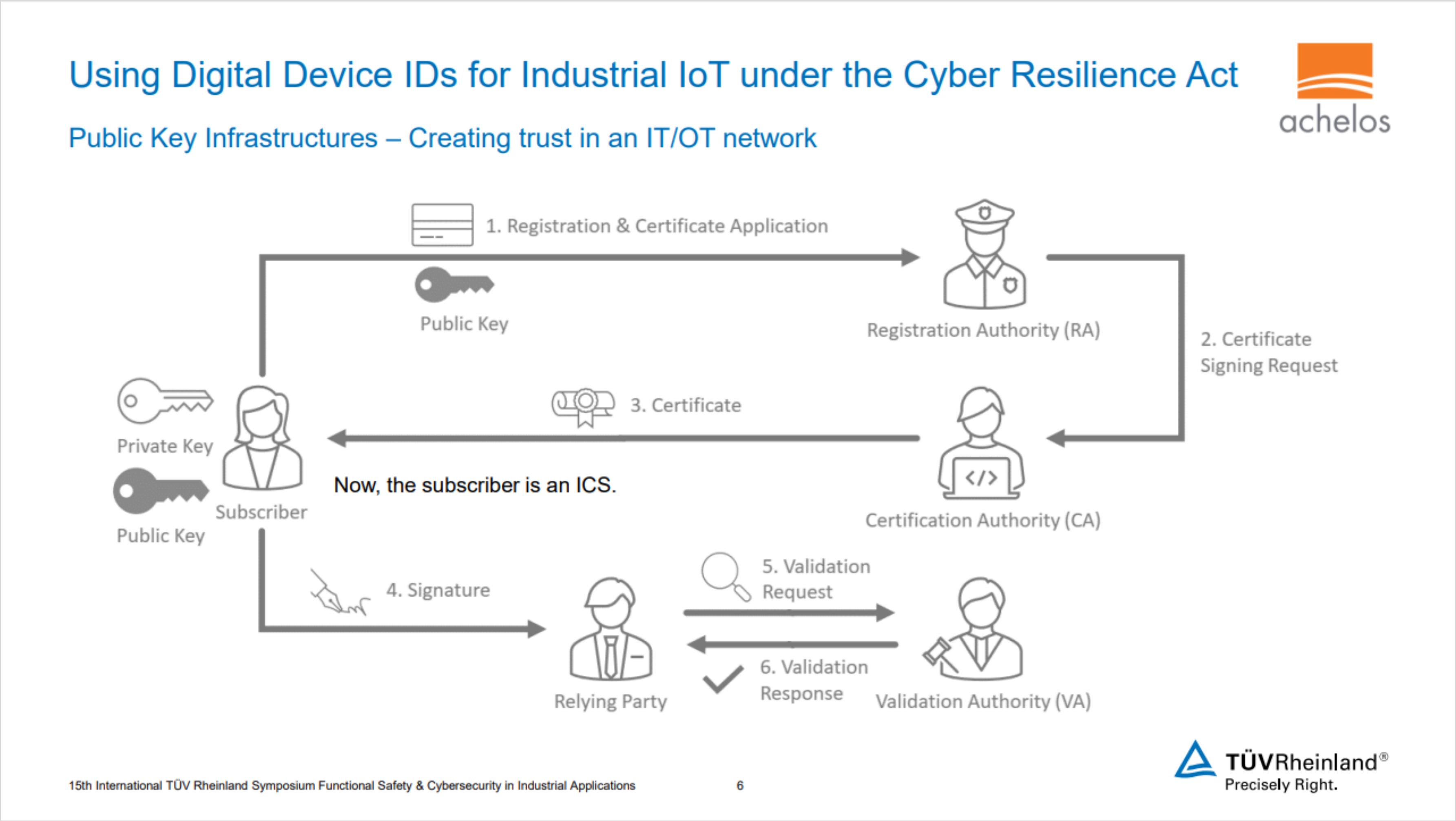
Using Digital Device IDs for Industrial IoT under the Cyber Resilience Act

Dr. Michael Jahnich

achelos GmbH – Germany

Zero Trust approach in OT Networks

Digital Device IDs and PKI



Using Digital Device IDs for Industrial IoT under the Cyber Resilience Act
Dr. Michael Jahnich
achelos GmbH – Germany

Zero Trust approach in OT Networks

Digital Device IDs and PKI

Using Digital Device IDs for Industrial IoT under the Cyber Resilience Act

achelos

Use Cases for Digital Device IDs

1. Establishing trust on the shop floor
2. Client authentication in a TLS based communication, HTTPS, MQTT over HTTPS
3. Webserver authentication
4. Secure network communication (confidential, integer, authentic), OPC-UA
5. Secure firmware and software updates (code signing)
6. Secure boot (code signing)
7. Remote access for maintenance
8. Zero touch onboarding in OT networks, e.g. OPC-UA Part 21 device onboarding

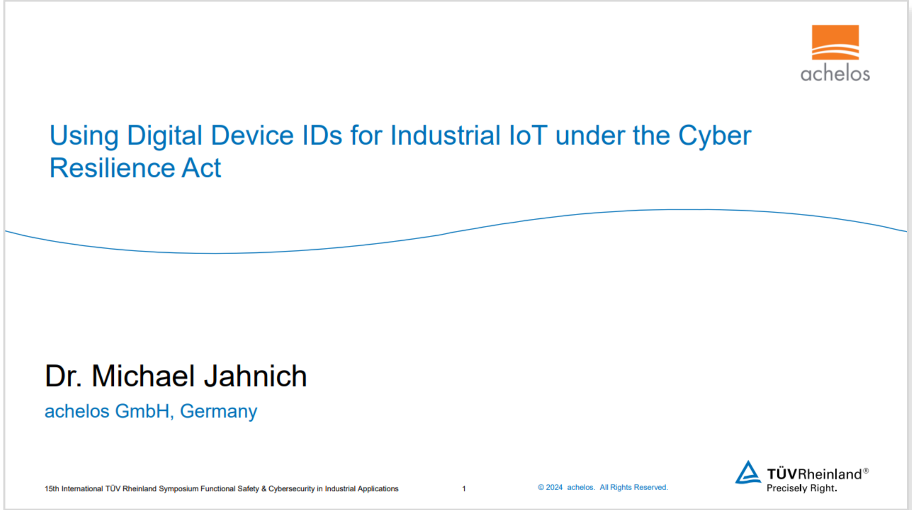
15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 7

TÜVRheinland®
Precisely Right.

Using Digital Device IDs for Industrial IoT under the Cyber Resilience Act
Dr. Michael Jahnich
achelos GmbH – Germany

Zero Trust approach in OT Networks

Digital Device IDs and PKI



Mandatory in some circumstances under the CRA.
A lot of interesting details given in the presentation.
If interested check:

Using Digital Device IDs for Industrial IoT under the Cyber Resilience Act
Dr. Michael Jahnich
achelos GmbH – Germany

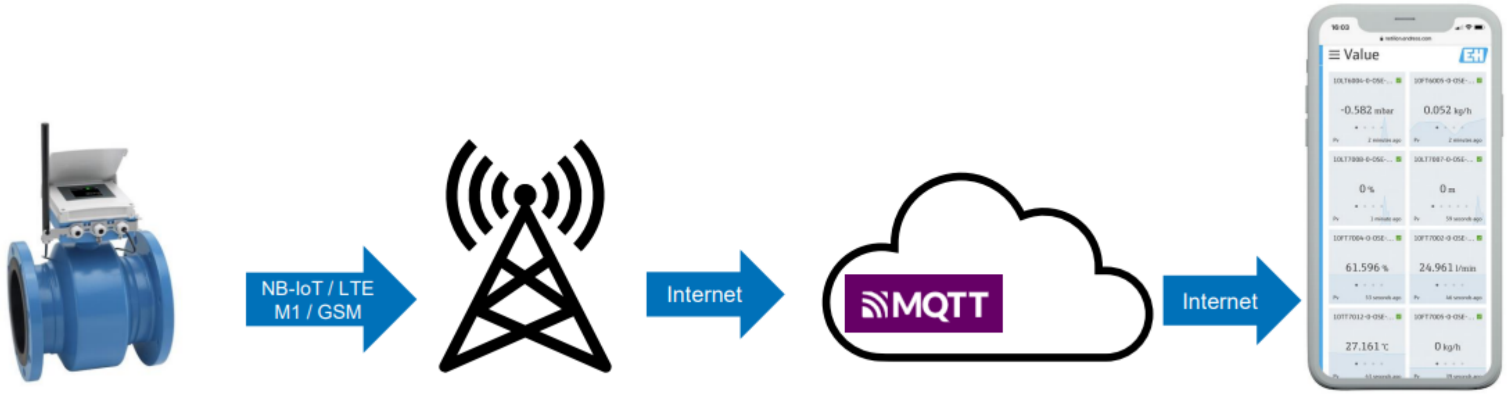
Zero Trust approach in OT Networks

PKI in field devices

Promag 800 C and the cloud

Endress+Hauser

A very high-level introduction



Battery operated Flow meter
Life-time: > 10 Years

connected over the **cellular network**

Exchanging data over **MQTT** with a “server” side application, i.e. The Cloud (MQTT to OPC-UA conversion available as well)

For example, the Endress+Hauser **Netilion** cloud

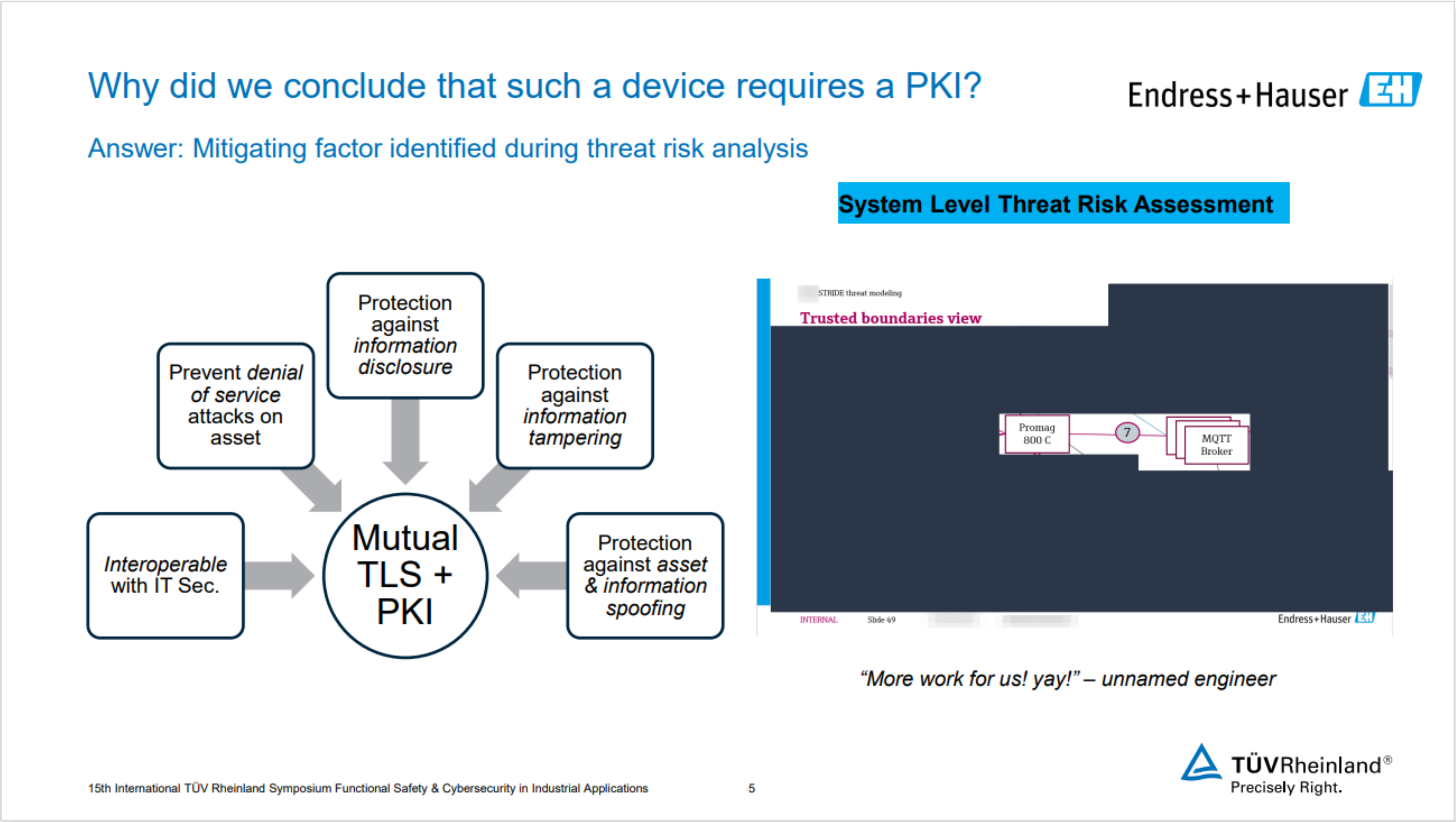
15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 3

TÜVRheinland®
Precisely Right.

PKI ready Battery Powered Field Devices – What did we Learn?
Sushil Siddesh
Endress+Hauser Flowtec AG - Switzerland

Zero Trust approach in OT Networks

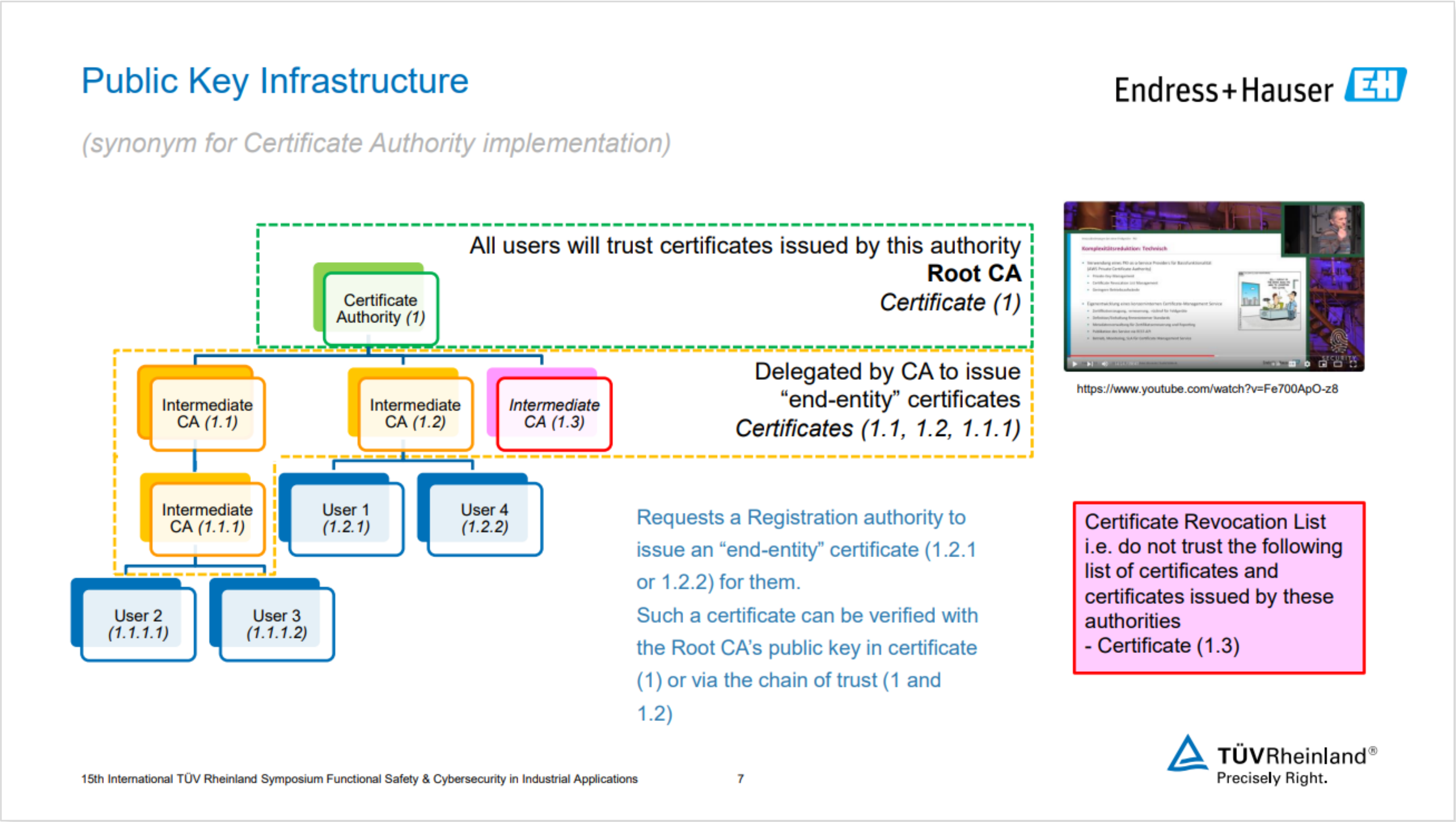
PKI in field devices



PKI ready Battery Powered Field Devices – What did we Learn?
Sushil Siddesh
Endress+Hauser Flowtec AG - Switzerland

Zero Trust approach in OT Networks

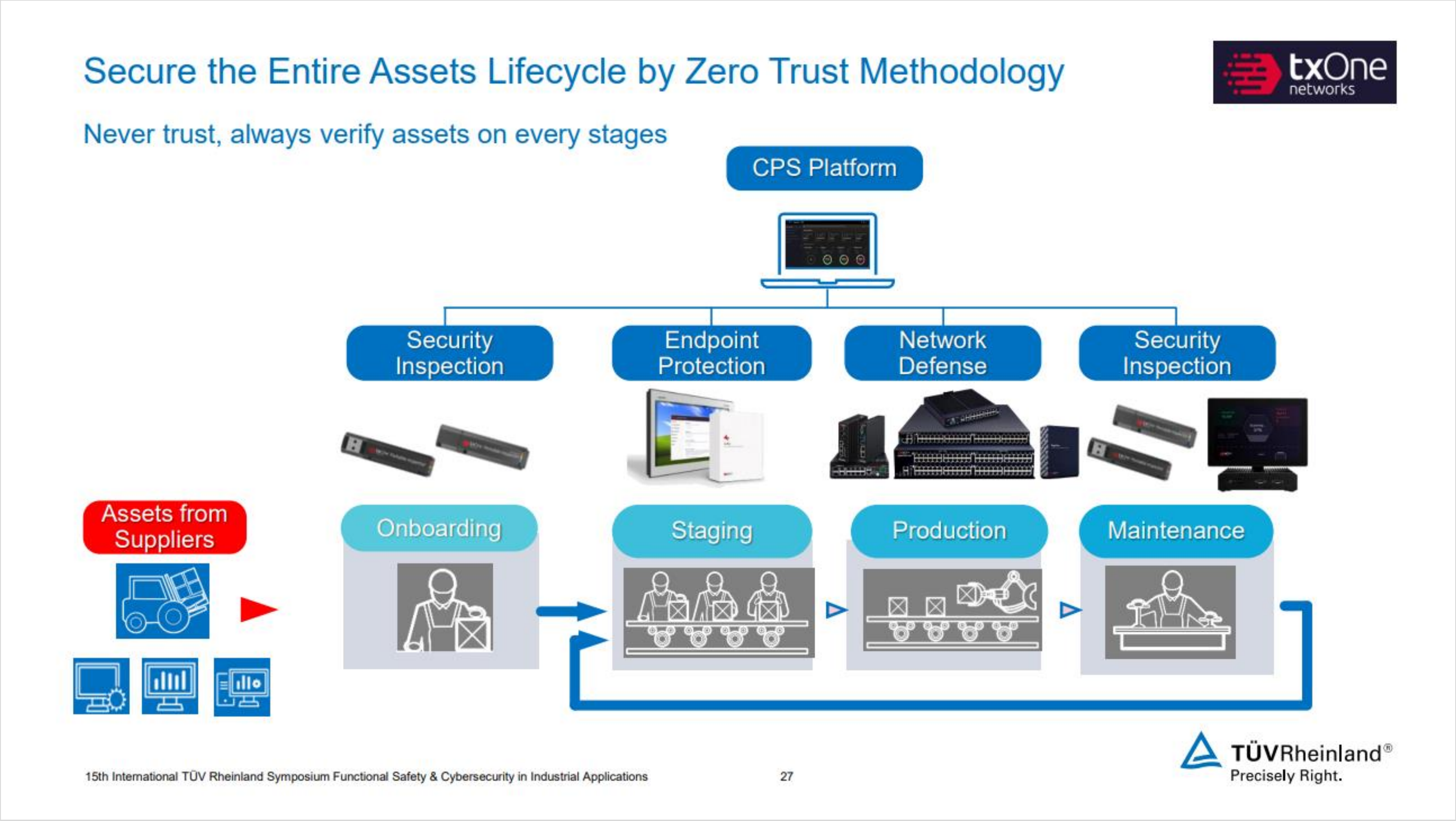
PKI in field devices



PKI ready Battery Powered Field Devices – What did we Learn?
Sushil Siddesh
Endress+Hauser Flowtec AG - Switzerland

Zero Trust approach in Asset Lifecycle

Never trust, always verify



Plant Availability and Cyber Security - Does this work together?
Mirco Kloss
TXOne Networks Europe B.V. - Germany

Human-Centric Security Practices

Cybersecurity as a social-technical problem

Problem and Premise – "Cybersecurity is a socio-technical problem"

- Analysis of 2023 data concludes all cybersecurity attacks still originate from human actors. In 2023 it was noted that there was an increase in Artificial Intelligence supporting the efficiency and effectiveness of social engineering and information campaigns.
- While there is little documented evidence of cybersecurity breaches that have been thwarted by human intervention, there is an abundance of data on human factors being exploited by cybersecurity threat vectors. Human error remains a leading cause of most malicious attacks in cybersecurity. {References vary estimating between 35% to 45% of data breaches are attributed to human error.}
- Conversely it is also accepted wisdom that human decision-making, situational awareness and flexibility is fundamental to enhanced cybersecurity resilience. Though defences may be automated, their response will be human mediated. Healthcare, aviation, and defence have utilised human factors research to reduce and treat risks. In comparison, the cybersecurity sector, as a whole, lags in leveraging human factors.

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 2

TÜVRheinland® Precisely Right.

Leveraging the Human Factor for the Enhancement of SIS Cyber Security

Daryl Wheatley
MWS Risk Pty Ltd. – United Kingdom

Human-Centric Security Practices

Cybersecurity as a social-technical problem

Humans – What are we good at? What are we bad at?

MWS RISK

Information process stage	Humans are better at:	Automation is better at:
Data Acquisition	Detecting small amounts of signals or detecting abnormal signal ranges	Monitoring large numbers of signals
Data Analysis	Pattern perception Making generalisations **Making innovative associations**	Ignoring noise in the data Making quantitative assessments Applying precise criteria Storing and recalling a huge amount of data
Action selection	Improvisation, making flexible solutions **Reasoning inductively and correcting error**	Repeating procedures consistently Reasoning deductively
Action implementation	Flexibility when switching between actions **Adjusting dynamically**	Performing many complex operations in parallel Responding quickly and precisely

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 5

TÜVRheinland® Precisely Right.

Leveraging the Human Factor for the Enhancement of SIS Cyber Security

Daryl Wheatley
MWS Risk Pty Ltd. – United Kingdom

Human-Centric Security Practices

Cybersecurity as a social-technical problem

MWS RISK

Human sensory acuity that we use when physically attendant on the plant

- Vision
- Aural – noise
- Feel – vibration

The human operators already have these sensors. How do you better leverage human sensory acuity to detect information critical to the safe operation of the plant?

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 9

TÜVRheinland® Precisely Right.

Leveraging the Human Factor for the Enhancement of SIS Cyber Security

Daryl Wheatley
MWS Risk Pty Ltd. – United Kingdom

Human-Centric Security Practices

Cybersecurity as a social-technical problem

Conclusion and Take-aways

- The way we design safety systems will have to evolve one-way or another to counter the escalation in the cybersecurity threat environment.
- Making safety system design human centred should not be discarded. Elements of the safety system design that may be leveraged to better enable human interaction should be a focus.
- Design features can be simple and low cost – you don't have to install expensive and elaborate systems over the top of your design rather build them in at the ground level as part of the realisation phase of the safety lifecycle.

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 13

TÜVRheinland® Precisely Right.

Leveraging the Human Factor for the Enhancement of SIS Cyber Security

Daryl Wheatley
MWS Risk Pty Ltd. – United Kingdom

Conference Program

Second Day | Functional Safety

Rethinking Priorities in Functional Safety: A Management and Assessment-Centric Approach
Tino Vande Capelle
T V C Functional Safety Services – U A E

Functional Safety Digitalization - Unleash the Opportunities
Marco Turdo
HIMA Paul Hildebrandt GmbH – Germany

Current Status of IEC 61508 Edition 3
Dr. Fan Ye
Environmental Resources Management ERM – United Kingdom

Model Based Safety Instrumented System (SIS) Programming using Artificial Neural Networks
Ajay Mishra, Murugananth Muthuramalingam, Erna Banchik
Schneider Electric – USA

Expediting execution of Failure Modes and Effects Analysis through automation by available Machine Learning Techniques
Jonathan Holm, Adam Lehmann
Amazon Robotics - USA

Contribution of AI Quality Measures to Functional Safety Properties
Michael Kieviet
LAPWING GmbH - Germany

Storage Tank Overfill Protection in Compliance with Functional Safety Standard: IEC 61511
Hassan D. Alsada
SABTANK, A SABIC Affiliate – Saudi Arabia

Proper SIS Design: Logic Solver Subsystem HFT is all I need to worry about….or is it?
John Walkington, Rafal Selega
ABB Energy Industries Division – United Kingdom

Mission Time of Machines and Systems in Functional Safety
Peter Arnold, Jürgen Steinhäuser
ELESTA GmbH - Germany

Maintaining SIL with Proof Test - Practical Experiences
Ton Beems, Arjen de Koning
Yokogawa Europe B.V. - Netherlands

Rethinking Priorities in FS

Management and Assessment – Centric Approach

Traditional Approaches to Functional Safety

TVC FUNCTIONAL SAFETY SERVICES

- **Phase 01: Hazard and Risk Assessments**

During this phase, engineers conduct a HAZOP, a widely recognized and utilized technique globally. While the assessment of hazards often yields realistic consequences, estimating the frequencies of these hazards can pose a challenge. How do you approach this in your assessments?

- **Phase 02: Allocation of Safety Functions to Protection Layers (LOPA)**

LOPA is favored for its quantitative approach, appealing to engineers who value precise data. However, it's important to consider the origins of these numbers. Are they derived transparently and objectively, or are there influences from budget constraints or managerial expectations?

- **Phase 03: Safety Requirement Specification (SRS)**

This phase requires engineers to define additional risk reduction measures, including hardware redundancies, diverse technology deployments, and mechanical barriers. Despite over two decades since the introduction of the IEC61511 standard, it remains a challenge to encounter fully complete and correctly documented SRS.

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 5

TÜVRheinland® Precisely Right.

Rethinking Priorities in Functional Safety: A Management and Assessment-Centric Approach

Tino Vande Capelle
T V C Functional Safety Services – U A E

Rethinking Priorities in FS

Management and Assessment – Centric Approach

Safety Integrity Level and PFD

TVC FUNCTIONAL SAFETY SERVICES

- **However**

It should be noted that SIL & PFD, whether certified or not, are still too frequently the only aspects that engineers document comprehensively. This approach can overlook the importance of a holistic documentation process that covers all critical aspects of safety system integrity and functionality.

- **Pitfalls'… Far Too Many!**

Prooftest intervals – Prooftest coverage – production downtime – Process engineer/management support – shutdown valve mission vs useful lifetime – firmware-based instrument/devices – Assessment conditions and assumptions vs plant conditions and environment – Etc.

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 7

TÜVRheinland® Precisely Right.

Rethinking Priorities in Functional Safety: A Management and Assessment-Centric Approach
Tino Vande Capelle
T V C Functional Safety Services – U A E

Rethinking Priorities in FS

Management and Assessment – Centric Approach

Key Takeaways from This Presentation

TVC FUNCTIONAL SAFETY SERVICES

- **The lack of Functional Safety Management (FSM) and Functional Safety Assessments (FSA)** critically undermines the safety integrity of operations across all Safety Integrity Level (SIL) categories in the process industries. This gap significantly heightens the risk of severe incidents, such as leaks, fires, and explosions, which could lead to catastrophic health, environmental, and financial consequences.
- **Adhering to the robust engineering principles and standards outlined in IEC 61511 goes beyond mere regulatory compliance**; it is crucial for ensuring the highest levels of safety and protection for the plant, its personnel, and the environment.
- **Properly implemented FSM and FSAs enhance the quality of all life-cycle activities** and are pivotal in preventing systematic failures. Since systematic failures cannot be controlled or precisely predicted, their prevention through rigorous implementation of FSM and FSAs is essential.
- **Moreover, we must design our systems to manage failures effectively** by incorporating reliable redundancy and diversity. This approach is fundamental to controlling potential failures and ensuring robust safety design.

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 13

TÜVRheinland® Precisely Right.

Rethinking Priorities in Functional Safety: A Management and Assessment-Centric Approach
Tino Vande Capelle
T V C Functional Safety Services – U A E

Rethinking Priorities in FS

Management and Assessment – Centric Approach

Key Takeaways from This Presentation (continued)

- **Cease using complex calculation tools** if you cannot employ your own failure data or realistic equivalent data.
- **Reject the notion that process availability** takes precedence over safety performance testing.
- **Avoid using shutdown valves** until failure; ensure compliance with mission times within their useful lifespan.
- **Question information sourced from generic internet searches** and rely on dependable, competent resources instead.

TVC FUNCTIONAL SAFETY SERVICES

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 14

TÜVRheinland® Precisely Right.

Rethinking Priorities in Functional Safety: A Management and Assessment-Centric Approach

Tino Vande Capelle
T V C Functional Safety Services – U A E

Maintaining SIL with Proof Test

Large-Scale proof testing practical example

1. IEC 61511-1:2016; Clause 16 SIS operation and maintenance

YOKOGAWA
Co-innovating tomorrow™

16.3.1 Proof testing

16.3.1.1 Periodic proof tests shall be conducted using a written procedure to **reveal undetected faults** that prevent the SIS from operating in accordance with the SRS.

NOTE 1 Particular attention can be made to identify failure causes that may lead to common cause failures.

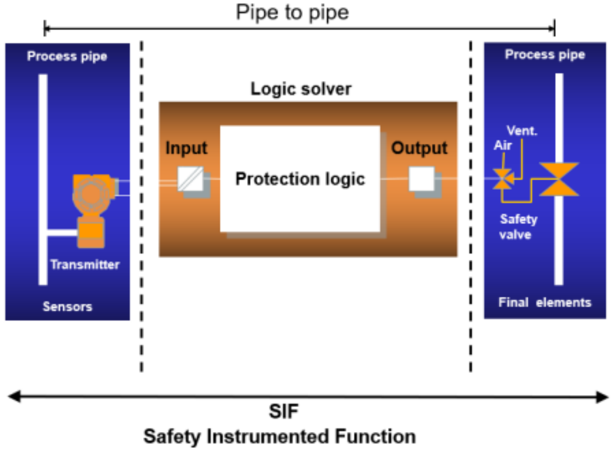
NOTE 2 Functional test procedures can also emphasize the need to avoid introducing common cause failures.

16.3.1.2 The entire SIS shall be tested including the sensor(s), the logic solver and the final element(s) (e.g., shutdown valves and motors).

NOTE Testing of the SIS can be performed either end-to-end or in segments (see 11.8.1).

16.3.1.3 The schedule for the proof tests shall be according to the SRS. The frequency of proof tests for a SIF shall be determined through PFDavg or PFH calculation in accordance with 11.9 for the SIS as installed in the operating environment.

NOTE Different parts of the SIS can require different test intervals, for example, the logic solver can require a different test interval than the sensors or final elements



15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 3

TÜVRheinland®
Precisely Right.

Maintaining SIL with Proof Test - Practical Experiences
Ton Beems, Arjen de Koning
Yokogawa Europe B.V. - Netherlands

Maintaining SIL with Proof Test

Large-Scale proof testing practical example

1. Proof Test

YOKOGAWA
Co-innovating tomorrow

A proof test means a complete test of the SIF.

The purpose of the proof test is to reveal all undetected failures that are present in the SIF →

- SIF must be tested completely
- Also allowed to split it in sensor, LS and final elements and test separately
- Also allowed to use (false) trip as a proof test, if recorded that actions were successful.

After the proof test the elements in the SIF should be in their initial state

Proof test does not mean only a functionality check to confirm the (expected) function of the loop

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 4

TÜVRheinland®
Precisely Right.

Maintaining SIL with Proof Test - Practical Experiences
Ton Beems, Arjen de Koning
Yokogawa Europe B.V. - Netherlands

Maintaining SIL with Proof Test

Large-Scale proof testing practical example

1. Let's do Proof test!

Easier said then done

Client:
Original HAZOP report is not available.
SIL classification was done for this existing site based on the crosses on the C&E.

After SIL Classification; proof testing is a KPI for Functional Safety compliance

But nothing available.
Start from Scratch

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications

TÜVRheinland®
Precisely Right.

Maintaining SIL with Proof Test - Practical Experiences
Ton Beems, Arjen de Koning
Yokogawa Europe B.V. - Netherlands

Maintaining SIL with Proof Test

Large-Scale proof testing practical example

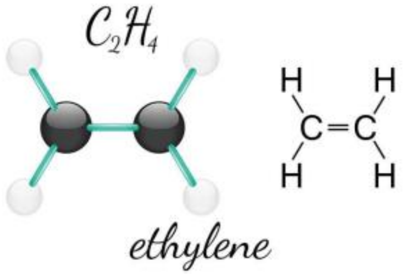
2. Proof Test Preparation: Project Scope

YOKOGAWA
Co-innovating tomorrow

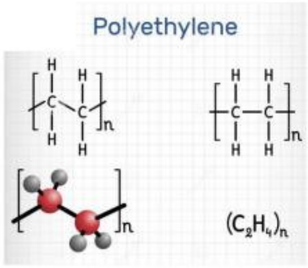
Site: Ethylene / Polyethylene Plant

Built in mid 90's

Ethylene C_2H_4 Plant –
157 SIF's **96 +16 Selected during Site** SIL 0 - 3



Polyethylene $(C_2H_4)_n$ Plant –
52 SIF's **48 selected** SIL 1 - 3



15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 6

TÜVRheinland®
Precisely Right.

Maintaining SIL with Proof Test - Practical Experiences
Ton Beems, Arjen de Koning
Yokogawa Europe B.V. - Netherlands

Maintaining SIL with Proof Test

Large-Scale proof testing practical example

2. Proof Test Preparation: Project Team

Project team: 1 Lead with 5 safety engineers

4 months preparing the 144 SIF proof test dossier.

4 weeks at site – The actual proof test Execution

What is needed to Create this Proof test procedure & Dossier?

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications

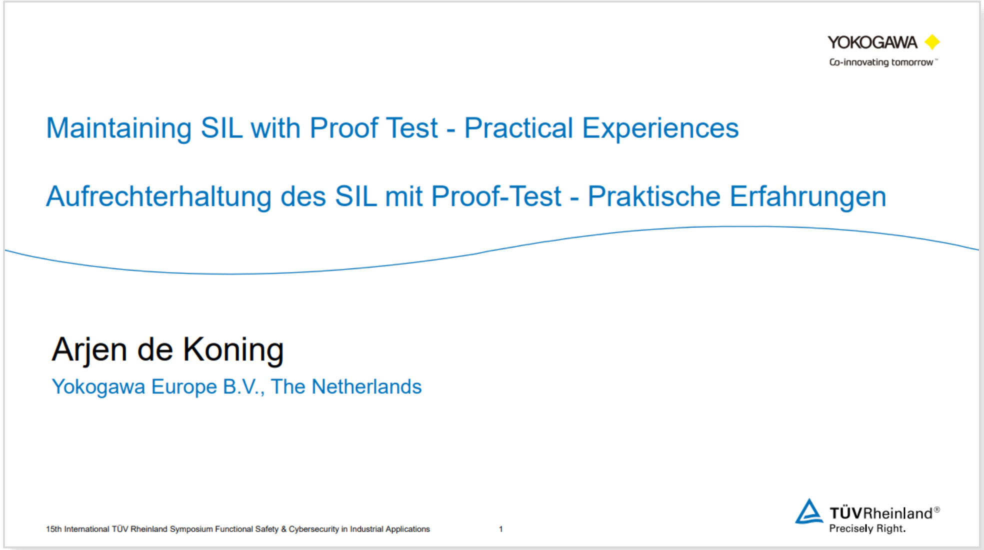
TÜVRheinland®
Precisely Right.

Maintaining SIL with Proof Test - Practical Experiences

Ton Beems, Arjen de Koning
Yokogawa Europe B.V. - Netherlands

Maintaining SIL with Proof Test

Large-Scale proof testing practical example



Consult the presentation for a very detailed description of all the steps taken in the preparation, execution and documentation of the process.

Maintaining SIL with Proof Test - Practical Experiences
Ton Beems, Arjen de Koning
Yokogawa Europe B.V. - Netherlands

Maintaining SIL with Proof Test

Large-Scale proof testing practical example

3. Key Take Aways

YOKOGAWA
Co-innovating tomorrow

- Proof test “Buzz word” - Easier said then done.
- Proof test is more then just a function test of a trip point
- Good proof testing require a detailed planning, manpower, time and budget.
- Proof test during TA schedule is too tight/impractical with many parallel activities
- Systematic Safety Integrity (Inspection) is not expected and appreciated.
- Proof Test Coverage can be a serious limitation – can result in additional Proof testing to meet the SIF SIL requirement.
- FSM in the Operational Phase is almost non-existing.
- Analyzing the Proof test results – limited follow up (budget/operational constrain)
- Digital systems can provide actual (operational) data – but verification is still Human (Manual) exercise.

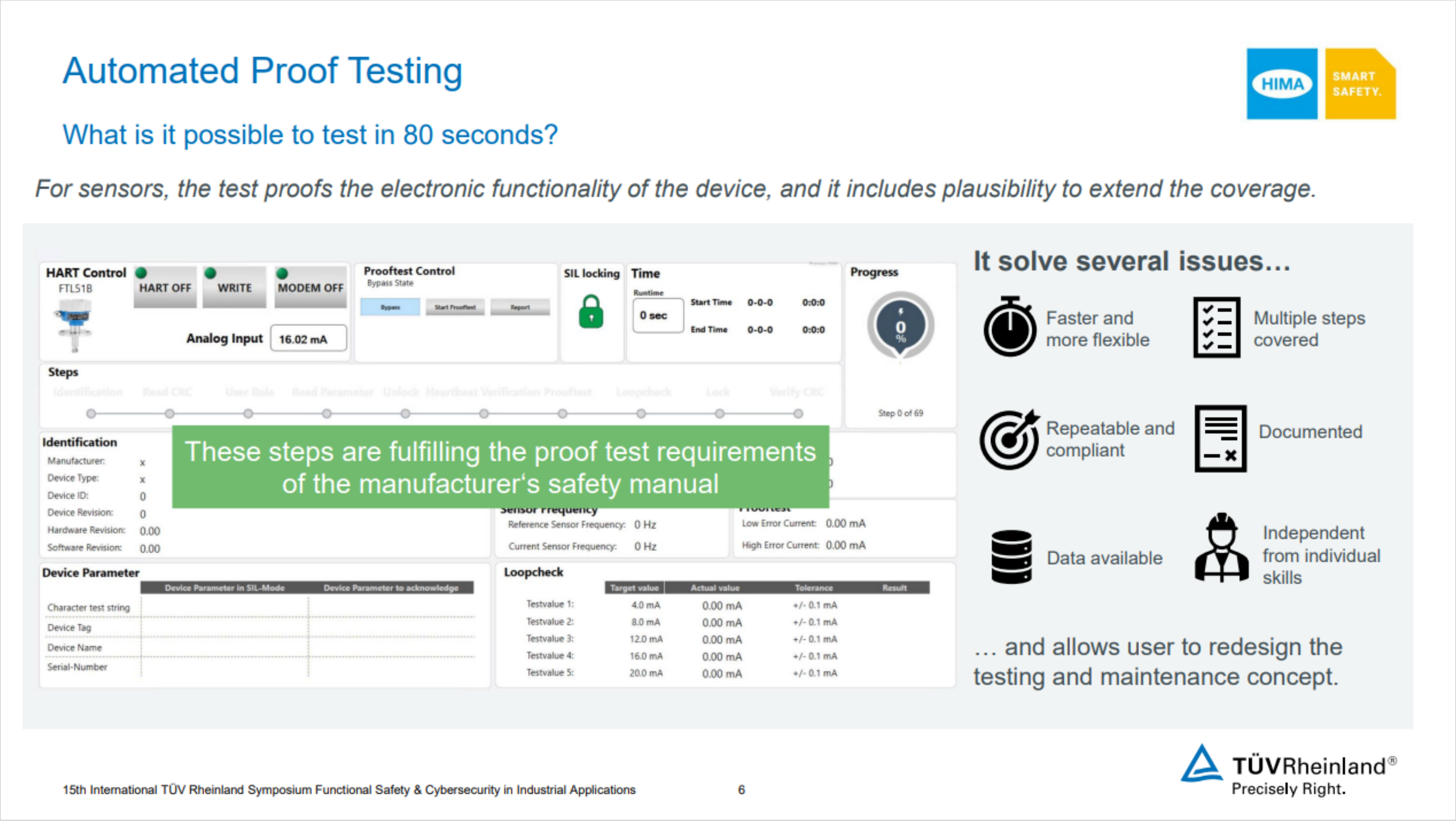
15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 28

TÜVRheinland®
Precisely Right.

Maintaining SIL with Proof Test - Practical Experiences
Ton Beems, Arjen de Koning
Yokogawa Europe B.V. - Netherlands

Digitization of Functional Safety

Automated Proof Testing



Functional Safety Digitalization - Unleash the Opportunities
Marco Turdo
HIMA Paul Hildebrandt GmbH – Germany

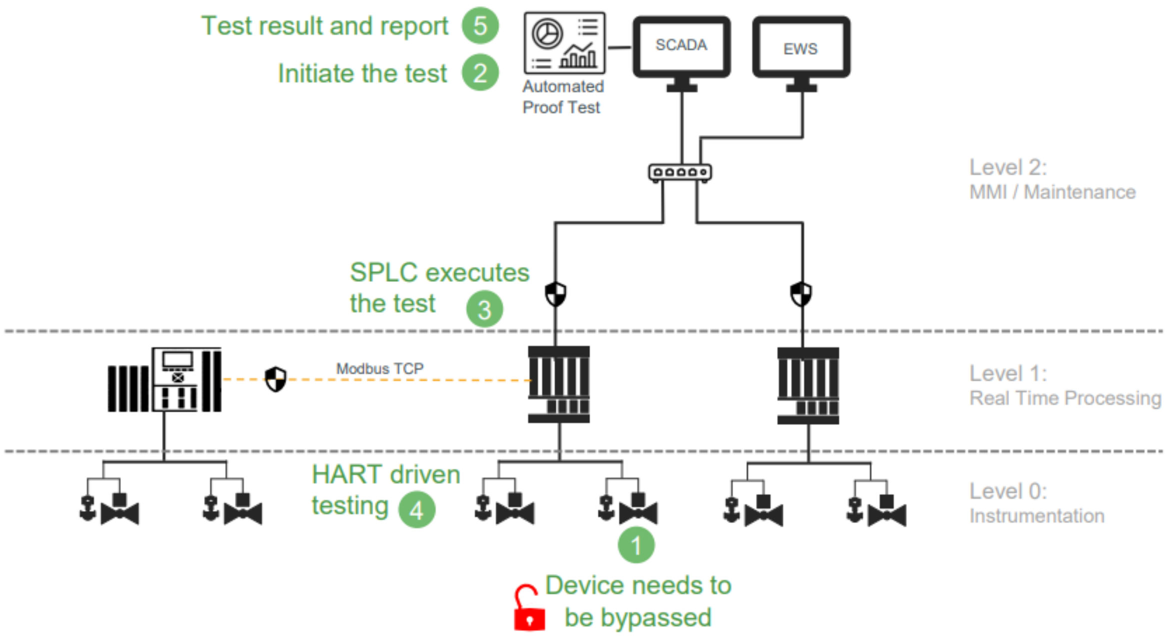
Digitization of Functional Safety

Automated Proof Testing

Automated Proof Testing

HIMA SMART SAFETY.

How does it work in a typical installation?



Key features

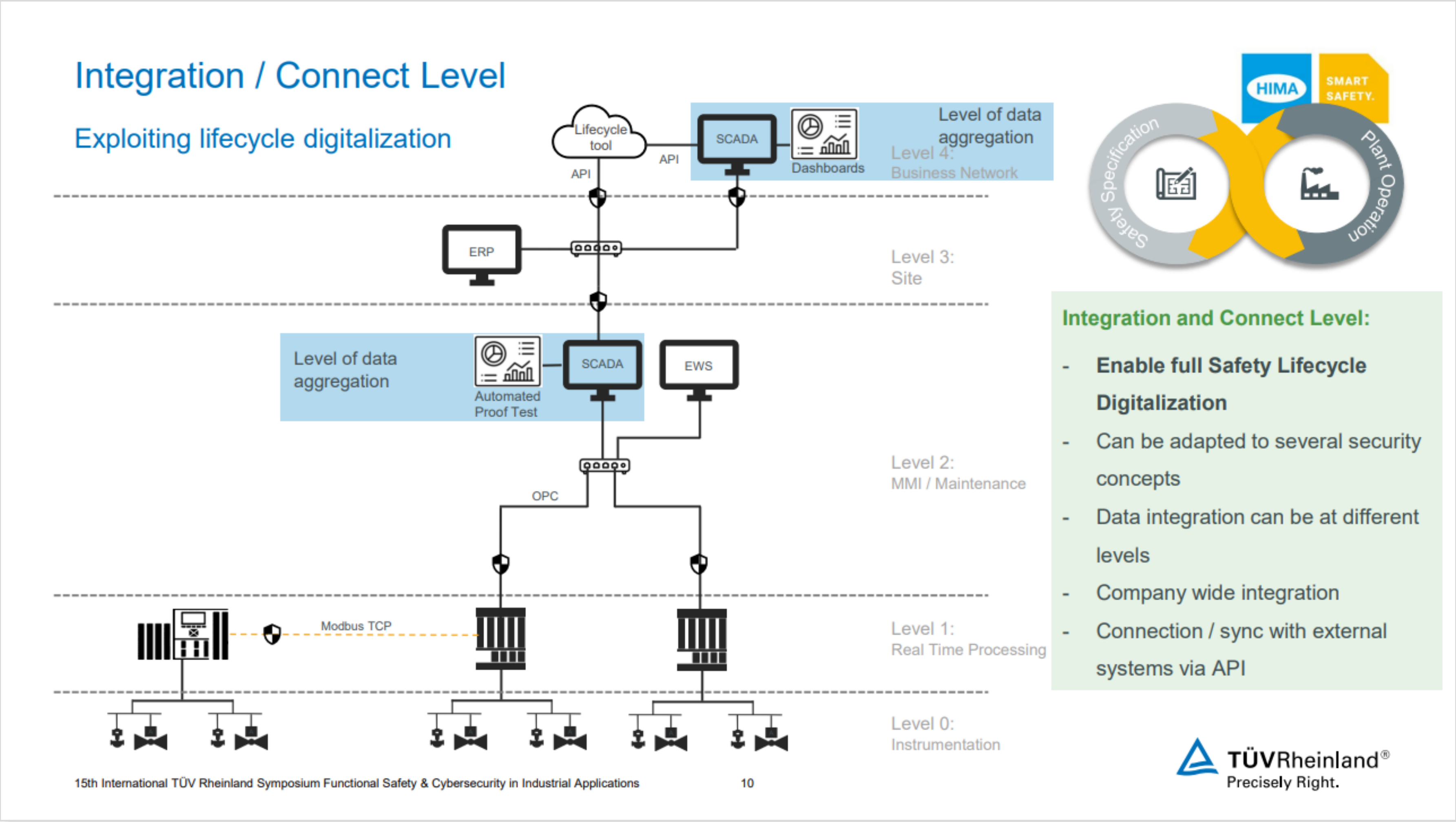
- Proof tests managed by single HMI
- Only devices that are bypassed can be tested
- Test are performed by SIL3 logic solver through standard logic blocks
- HART communication is used to drive the test
- Results are stored and can be printed in reports

TÜVRheinland® Precisely Right.

Functional Safety Digitalization - Unleash the Opportunities
Marco Turdo
HIMA Paul Hildebrandt GmbH – Germany

Digitization of Functional Safety

Vertical Integration of FS Data and Documentation



Functional Safety Digitalization - Unleash the Opportunities
Marco Turdo
HIMA Paul Hildebrandt GmbH – Germany

Proper SIL Design

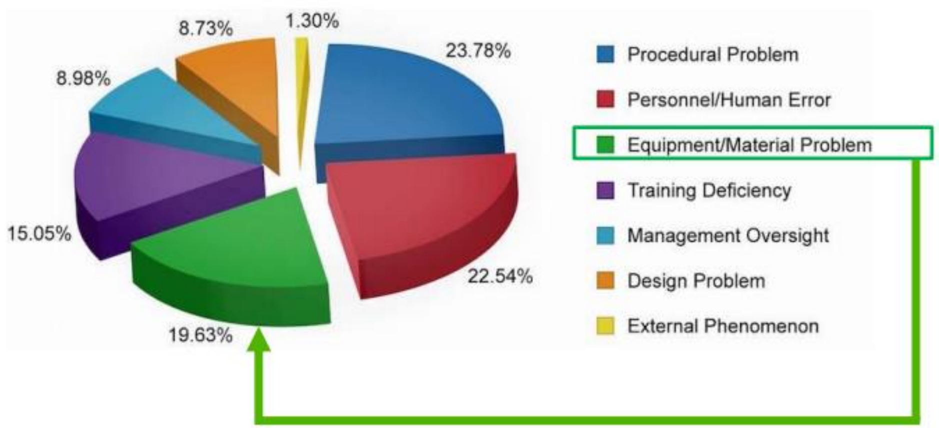
Beyond Logic Solver HFT

Typical Causes of Process Incidents

Random hardware failures should be our only focus for the Logic Solver…Right?

Not Really:

- Based on statistical evidence, around 80%* of process plant incidents can be contributed to human factors; and most of them are 'systematic failures'…



*Example Source: Based on the survey conducted by 'The RAM Review' https://theramreview.com/the-human-side-of-failure

TÜVRheinland® Precisely Right.

Proper SIS Design: Logic Solver Subsystem HFT is all I need to worry about….or is it?

John Walkington, Rafal Selega
ABB Energy Industries Division – United Kingdom

Proper SIL Design

Beyond Logic Solver HFT

Summary

So, it's not just about Logic Solver HFT in design…?

- Frequently SIS engineers only make their technology selection based on the evaluation of the reliability/availability of the SIS logic solver by comparison of PFD_{avg}, PFH or STR values of the specific logic solver architecture e.g. 1oo2, 2oo3, 2oo4. **All architectures can achieve high reliability figures, but we now recognise that this alone is not sufficient!**
- The PFD_{avg}/PFH calculations provide the probability of SIS failure due to random failures only (systematic faults are not quantified). As the probability of SIS failure is related to both random and systematic failures, PFD_{avg} alone is not enough in evaluating the probability of SIS failure. These calculations are therefore only one SIL target requirement.
- The effect of common cause failures related to HFT architectures **shall be assessed qualitatively** as per IEC 61508-2. This needs to be applied across both the manufacturing and end user safety lifecycle requirements.
- After the analysis has detected all the likely common cause initiators and coupling mechanisms, **appropriate measures shall be implemented** to control and avoid common cause failures.
- In addition, **the SIS software** shall be developed based on the requirements as found in IEC 61508-3.

SIS engineers need to seek documented evidence of CCF analysis across the safety lifecycle i.e. products, design, operation & maintenance, to form a sufficient judgement that the intended safety integrity of the SIS can be achieved…

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 14

TÜVRheinland® Precisely Right.

Proper SIS Design: Logic Solver Subsystem HFT is all I need to worry about….or is it?
John Walkington, Rafal Selega
ABB Energy Industries Division – United Kingdom

SIL Beyond the Numbers

The High Integrity E-Stop fallacy

The High Integrity Estop fallacy!

SHAKTI CORP

IEC AS 61508-4 – Functional Safety of E/E/PE safety related systems

3.4.1
safety-related system

NOTE 5 A person can be part of a safety-related system. For example, a person could receive information from a programmable electronic device and perform a safety action based on this information, or perform a safety action through a programmable electronic device.

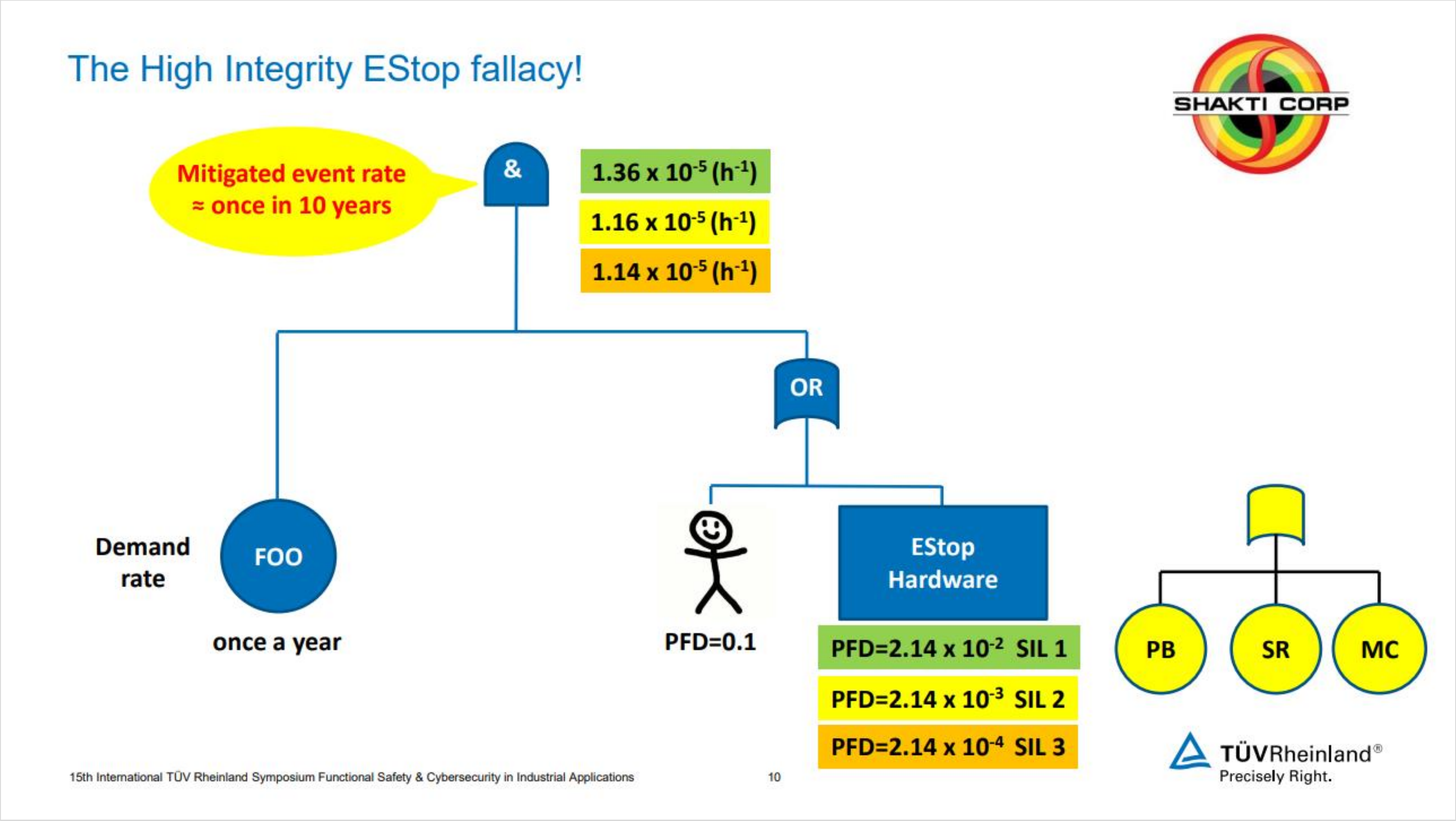
15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 9

TÜVRheinland®
Precisely Right.

SIL Beyond the Numbers
Keerthy Mysore, David MacDonald
Shakti Corp Pty Ltd - Australia

SIL Beyond the Numbers

The High Integrity E-Stop fallacy



SIL Beyond the Numbers
Keerthy Mysore, David MacDonald
Shakti Corp Pty Ltd - Australia

SIL Beyond the Numbers

General Advice

Finally,

SHAKTI CORP

- Target is Risk Reduction, not SIL
- Fitness for purpose, certification is one way
- Be a skeptic, but don't cry wolf!
- Beware of "Normalisation of Deviance"
  blow the whistle if you need to!
- Due diligence is required of every stakeholder,
  not just the Safety Engineer
- Not just about "going through the motions"
  let's make the world a safer place

15th International TÜV Rheinland Symposium Functional Safety & Cybersecurity in Industrial Applications 25

TÜVRheinland®
Precisely Right.

SIL Beyond the Numbers

Keerthy Mysore, David MacDonald
Shakti Corp Pty Ltd - Australia


TÜV


Z(1, 3)
Z(2, 2)
Z(4)
Z(1, 1, 2)