Sicherheit von vernetzten, modularen Industrieanlagen erfordert eine dynamische Sicherheitsarchitektur 4.0 (Safety & Security)

Automatica 2018 – IT2Industry Forums - 22.06.2018

Dr. Detlev Richter
TÜV SÜD Product Service GmbH
Global Head of Industrial and Energy Products
## Agenda: dynamische Sicherheitsarchitektur 4.0 - Safety & Security

1. **Industrie 4.0 = IT + OT** ➔ *connectivity, real time and safety*

2. **I4.0 Life Cycles, Value Chain** ➔ *risk assessment as a “continuum”*

3. **Smart Factory\(^{KL}\) based on OPC-UA**  
   *Modular and adaptive safety case*

4. **AGV’s, Robots and production cells** ➔ *event driven risk assessment I4.0*

   | Safety & Security over lifetime ➔ *enabler for I4.0 business* |
Industrie 4.0 – Industrial production processes are based on Cyber-Physical Systems - Interconnectedness

- From a world of not connected things …
- … to the Industrial Internet of Things

Mechanization Industrie 1.0 [1784]

Electrification Industrie 2.0 [1870]

Digitalization Industrie 3.0 [1969]

Connectivity Industrie 4.0 [2010]

Components, tools and machines are becoming \[ \Rightarrow \] I4.0 Components (Cyber-Physical Systems)

\[ \Rightarrow \] Definition of CPS: A system of collaborating computational elements including mechanical and electrical elements connected in a smart cloud able to communicate in real time
How a machine/component (asset) becomes an **Cyber-Physical Systems (I4.0 Component)**?

⇒ Adding a digital copy (**Digital Twin**) to the machine/component by creating an „**Administration Shell**“ including the required content specified in the **Reference Architecture Model Industrie 4.0**.

⇒ Deployment of the **Administration Shell** – **connectivity** – **security, safety & interoperability**
Three dimensional model represents the I4.0 space - connectivity

Reference Architecture Model - RAMI 4.0 - contains fundamental aspects of Industrie 4.0

Merge IT (Information Technology) & OT (Operation Technology) in a reference model - DIN SPEC 91345:2016-04, but most documents target the IT integration of vertical, horizontal and product life cycle processes.

⇒ Are autonomous and safe operations of I4.0 components adequately addressed => not in depth
⇒ How do we support risk assessment as the starting point for adaptive plug & produce concepts?
Agenda: dynamische Sicherheitsarchitektur 4.0 - Safety & Security

1. Industrie 4.0 = IT + OT ➔ connectivity, real time and safety

2. I4.0 Life Cycles, Value Chain ➔ risk assessment as a “continuum”

3. Smart Factory\(^{KL}\) based on OPC-UA
   Modular and adaptive safety case

4. AGV’s, Robots and production cells ➔ event driven risk assessment I4.0

Safety & Security over lifetime ➔ enabler for I4.0 business
Production plant goes Industrie 4.0 - “Connectivity of all life cycles”

- Digitalization is based on seamless data availability between all life cycles ➔ Industrie 4.0

Robots (cobots), AGV’s and I4.0 connectivity in real time ➔ Plug & Produce on plant level
Production: Plant Management ➔ Technical Risk Management

- From theory to practical solutions – technical risk management approach within Industrie 3.0

**RISK MANAGEMENT**

- Financial risks …
- Market risks …
- Operational risks

---

**Technical Risk Management**

- Manufacturer
- Operator
- Plant & machinery

---

- Machinery Directive
- Local Safety & Health regulations

---

**Safety - Compliance - Efficiency**
Industrie 4.0 – Industrial production processes are based on Cyber-Physical Systems - Interconnectedness

- From a world of not connected things …
- … to the Industrial Internet of Things

Safety & Compliance
- Human
- Environmental
- Legal

Efficiency
- Availability
- Operating performance
- Energy efficiency

---

- **Machinery Directive** has consequences on machine modules, machines and production lines
  - *Risk evaluation starts with determination of limits of machines and identification of hazard*
- **Safety architecture**: Observe and consider always the complete safety chain
Industrie 3.0 → **4.0**: Technical Risk Management in real time

Industrie 4.0 – Industrial production processes are based on Cyber-Physical Systems - Interconnectedness

- From a world of not connected things …
- … to the Industrial Internet of Things

Safety & Compliance
- Human
- Environmental
- Legal

Efficiency
- Availability
- Operating performance
- Energy efficiency

Connectivity & Security

Communication & Interoperability

- Machinery Directive has consequences on smart machines, m2m communication and smart components
  - Risk evaluation starts with determination of limits of machines and identification of hazard
- Safety architecture: Observe and consider always the complete safety chain
  - What is a complete safety chain in the world of IIoT?
Production plant goes Industrie 4.0: Security can impact safety

- Data have to be secured all the way around and analytics results impact safety critical decision.
- What is a complete safety chain in this world?

**Connect**

**Analyze**

**Integrate**

Platform Layer

- Stream data
- Process data
- Correlate data

Zero Effort integration based on Business Apps

Sensor networks

Asset

TÜV SÜD Product Service GmbH

Folie 11
**Industrie 4.0 – Risk assessment process extends over time**

*Machinery Safety Risk Assessment – Intelligent and connected components impacts Safety & Security processes*

### Machinery Limits

<table>
<thead>
<tr>
<th>Limits</th>
<th>$T_{1_{\text{Construktion}}}$</th>
<th>$T_{2_{\text{Commissioning}}}$</th>
<th>$T_{X \text{ Configuration } y}$</th>
<th>$T_{X+1 \text{ Config. } y+1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Areal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energetic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>..</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Concatenation</td>
<td>Concatenation</td>
<td>Concatenation</td>
<td></td>
</tr>
<tr>
<td>Connectivity</td>
<td>Cloud</td>
<td>Cloud/Software</td>
<td>Cloud/Software</td>
<td></td>
</tr>
</tbody>
</table>

### Safety

**Safety:**
Absence of catastrophic consequences on the user(s) and the environment.”

*(Laprie)*

### Security

**Confidentiality**

**Integrity**

**Availability**

### Connectivity / Interoperability
Agenda: dynamische Sicherheitsarchitektur 4.0 - Safety & Security

1. Industrie 4.0 = IT + OT ➔
   connectivity, real time and safety

2. I4.0 Life Cycles, Value Chain ➔
   risk assessment as a “continuum”

3. Smart Factory$^{KL}$ based on OPC-UA
   Modular and adaptive safety case

4. AGV’s, Robots and production cells ➔
   event driven risk assessment I4.0

Safety & Security over lifetime ➔
enabler for I4.0 business
SmartFactory$^{	ext{KL}}$ – Learning in a pilot production line

- Technologie Initiative SmartFactory$^{	ext{KL}}$ e.V. (Trippstadter Str. 122, 67663 Kaiserslautern)

Smart fabrication line

Smart machines

Smart objects
Configurations of machines and machine modules are validated during the change of the production line.

- Validation of changes in a I4.0 production line on request (dynamically)
  - Safety is based on the correct (trusted) data of a I4.0 component
    - Content of RAMI 4.0 Administration Shell

- Assessment of changes in real time
  - Based on digital models (digital twin)
  - and the real behavior (real time analyze)

- Digital certificates are part if I4.0

**I4.0 plug & produce:** $CE_{I4.0} + CE_{I4.0} = CE_{I4.0}$
Validation of configurations of machines and machine modules during the change (plug) of production line

- **Module interface description:**
  - define safety profiles
    - modular approach

- **Safety profiles**
  - part of RAMI 4.0 Administration Shell
    - an unique semantic for safety relevant data
    - an I4.0 classification of data integrity

- **Risk properties** are still missing
  - part of I4.0 Safety profile to enable autonomous planning for plug & produce

*Reference to* SmartFactory^KL^ Whitepaper SF-3.1: 04/2018 “Safety an modularen Maschinen”

Smart Factory^KL^ Production line – ensures a predefined risk assessment for process technologies
Requirements for Plug & Produce - Modular Certification:

- **Security** is achieved by security by design combined with communication based on messages (*context sensibility*).
- **Interoperability** is ensured by pre-tested and certified components (*based on an OPC-UA platform approach*).
- I4.0 machines are **intrinsically safe** designed.
Smart Manufacturing: Safety 4.0 requires Pragmatic Interoperability

All basic concepts and interoperability platforms (OPC-UA information models) for adaptive safety are available.

- **Discovery Phase** (OPC-UA functions)
- **Validation Phase** (OPC-UA + I4.0)
- **Plausibility Phase** (Safety properties)
- **I4.0 Connectivity** (dig CE Conformity)

**Administration Shell (RAMI 4.0)**
(DIN SPEC 91345)

**OPC-UA** (IEC 62541)
Information models for machines based on VDMA companion spec.

**Automation/ML** (IEC 62714)
*Automation Markup Language*
Physical and logical devices

**eCl@ss** (IEC 61360)
Create the language of the things

- Information models and syntax for SOA
- data format for engineering
- Properties from eCl@ss define the Semantic

**Level of Interoperability**
- Pragmatic
- Semantic
- Syntactic
- Technical

**Product Safety** and **CE-Conformity** require an **Interoperability Solution – I4.0 safety semantic** - to **ensure** communication between products, tools and machines and to the cloud (edge, fog, private, ..)
Deployment of I4.0 Administration Shell has to consider security and safety aspects for plug & produce.

**Safety Engineering 4.0** is part of the platform selection ➔ deployment of administration shell (DIN SPEC 91345) impacts the usage of safety properties ➔ risk and safety properties impacts the communication channel ➔ **DIN SPEC 92222**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Asset-based AS</th>
<th>Fog-based AS</th>
<th>Cloud-based AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td>()</td>
<td>(+)</td>
<td>(+++)</td>
</tr>
<tr>
<td>Safety validation (real time)</td>
<td>(+)</td>
<td>(++)</td>
<td>(-)</td>
</tr>
<tr>
<td>Safety Profile integrity</td>
<td>(++)</td>
<td>(++)</td>
<td>( )</td>
</tr>
</tbody>
</table>
**Agenda: dynamische Sicherheitsarchitektur 4.0 - Safety & Security**

| 1 | Industrie 4.0 = IT + OT ➔  
connectivity, real time and safety |
|---|---|
| 2 | I4.0 Life Cycles, Value Chain ➔  
risk assessment as a “continuum” |
| 3 | Smart Factory\textsuperscript{KL} based on OPC-UA  
Modular and adaptive safety case |
| 4 | AGV’s, Robots and production cells ➔  
event driven risk assessment I4.0 |

Safety & Security over lifetime ➔  
enabler for I4.0 business
Highly automated production line includes interactions between machines, automated guided vehicles, industrial robots, and manual workers.

- Moving systems and humans equipped with multiple reliable sensors for safe man-machine interaction
- Obvious need for dynamically reconfigurable I4.0 sensor & I4.0 component networks

**real time critical & real time data** (AS) based calculations to ensure motion planning, object recognition, .. safe operations
I4.0 Safety for Smart Production: Industrial Robotic and AGV Case

Autonomous robots & guided vehicles – risk assessment in advance of motion planning

Requirements defined by collaborative robots

- Servo drive, motion control and motion planning
  - require the same I4.0 safety semantic

- Safety engineering: partitioning for cost effective and optimized solution
  - Drive control (asset based AS),
  - Robot and AGV (Fog/Edge based AS) and
  - Fabrication cloud (cloud based AS)

- Risk assessment in advance of motion planning becomes the key challenge to ensure compliance

What is a complete safety chain for this specific I4.0 Industrial Collaborative Robot and AGV Case?
I4.0 Safety for Smart Production: Industrial Robotic and AGV Case

Autonomous robots & guided vehicles – risk assessment in advance of production planning

Technical Risk Management
- Availability
- Operating performance
- Energy efficiency
I4.0 Safety for Smart Production: Industrial Robotic and AGV Case

Autonomous robots & guided vehicles – risk assessment in advance of production planning

Technical Risk Management
- Availability
- Operating performance
- Energy efficiency

Products, Robots, Tools, Load (size and dimension) of AGVs, Process parameter change over time

risk evaluation on request
Agenda: dynamische Sicherheitsarchitektur 4.0 - Safety & Security

1. Industrie 4.0 = IT + OT \(\rightarrow\) connectivity, real time and safety

2. I4.0 Life Cycles, Value Chain \(\rightarrow\) risk assessment as a “continuum”

3. Smart Factory\textsuperscript{KL} based on OPC-UA
   Modular and adaptive safety case

4. AGV’s, Robots and production cells \(\rightarrow\) event driven risk assessment I4.0

Safety & Security over lifetime \(\rightarrow\) enabler for I4.0 business
Smart Manufacturing: Safety Engineering – Safety Architecture 4.0

- Steps from Digitalization to Connectivity ⇒ Safety as an intrinsic property of I4.0 components

From a world of not connected things … … to the Industrial Internet of Things

The availability of all relevant information in real time by networking of all instances involved in adding values.

- The ability to use those data to establish the optimum value stream at any particular time in business processes, and facilitating new digital business models.
- I we translate this we end up with: on request; event driven; context based; ..
From a world of not connected things …

… to the Industrial Internet of Things

Risk Assessment for connected Industrie 4.0 products:
• Limits of risk analysis for machines end in a cloud → algorithm in real-time @edge
• Automatic proof of validity of last risk assessment → concept called “on-request”

Standardization (de-facto) of I4.0 components, machine modules and systems
• I4.0 machine modules are intrinsically safe and talk the same I4.0 safety semantic
• I4.0 SOA: OPC-UA becomes step by step the “interoperability & security platform”

Establish digital and real time processes for conformity assessment
• Test and validation of interconnectedness and concatenation in real time
• Reduction of Complexity by autonomous decisions to support people

Software defined networking and 5G Industrial Communication enables:
• Autonomous guided vehicles & robots ensured by fail operational safety solutions
I4.0 products based on CPS require a comprehensive risk assessment covering security & interoperability.
We are looking forward to a successful cooperation!
• Member of SmartFactoryKL initiative at the DFKI in Kaiserslautern
• Member of Industrial Internet Consortium - IIC
• Member of IEC TC44 IEC 62998 Machinery Safety standardization
  • Safety-related sensors used for protection of person
• Member of the Industrie 4.0 Interoperability WG at Bitkom
Tobias Pfeiffer
Leiter Maschinen und Anlagensicherheit
TÜV SÜD Product Service GmbH
Gottlieb-Daimler-Str. 7
70794 Filderstadt
Tobias.Pfeiffer@tuev-sued.de
T: +49 (0) 711 7005-575
M: +49 (0) 151 584 312 86