Evolution for the Technical Lifecycle – Experiences and Insights - Smart Manufacturing

Dr.-Ing. Detlev Richter
Global Head of Industrial and Energy Products
TÜV SÜD Product Service

Seoul, July 23rd 2019

Mehr Wert. Mehr Vertrauen.
Add value. Inspire trust.
Content

1. Smart Manufacturing ➔ Digital Twin Safety Engineering
2. Smart Manufacturing ➔ extended IIoT Risk Assessment
3. Plug & Produce ➔ IIoT Risk Assessment as a “…continuum”
4. Pilot learning ➔ Practical consideration for safety & security
5. Evolution for the Technical Lifecycle of adaptive IIoT products
Smart Manufacturing – Connectivity in real time combined with Cyber-Physical Systems

From a world of not connected things …

Mechanization Industrie 1.0 [1784]

Electrification Industrie 2.0 [1870]

Digitalization Industrie 3.0 [1969]

Connectivity Industrie 4.0 [2010]

… to the Industrial Internet of Things

Components, tools and machines are becoming I4.0 Components (Cyber-Physical Systems) .. partially correct called Digital Twins

\( \rightarrow \) Combination of technologies (cloud, 5G) enable new capabilities (software defined networking, machines, products, ..)

\( \rightarrow \) Certification & Inspection focused on product level – based on regulation with a static non-adaptable product/asset

\( \rightarrow \) Risk Assessment is defined based on well defined & static limits of an asset within an application
Smart Manufacturing – What is needed for safe operation? What is required by law?

What has to be ensured?
- The subject is driven by law and directives
  - Requirements for different roles (operator, ..)
  - Product liability
    - Machinery Directive (2006/42/EG)
    - Low Voltage Directive (2006/95/EG)

How it has to be ensured?
- Standards are hierarchical organized
  - A-Standards – EN ISO 12100 Risk Assessment
  - B-Standards – e.g. IEC 62062 functional safety
  - C-Standards – for specific assets (EN ISO 23125 CNC)
    - Application specific risk assessment

Smart Manufacturing for a global network
- Country specific interpretation of rules
- Regional specific acceptable risk level

Are connectivity, distributed products and adaptability covered? Requirement level => YES
Smart Manufacturing – IIoT – Safety and Security are based on three pillars:

I) Organization (.. and Company Culture)
- Process Certification (management process)
- Certification of people

II) Process
- Specification, Development, Validation and Test processes combined with tools and methods
- Process Certification (proof of capabilities)

III) Technology
- Product behavior and production monitoring
  - OPC-UA based machine information models
  - Product features optimized by AI @runtime
- Product Certification (incl. production audits)

Are connectivity, distributed products & adaptability over lifetime covered? IV) adaptability ➔ NO
Digital Manufacturing and Digital Engineering – Technical Life Cycle requirements

Integrate

Analyze

Connect

Stream/processing correlation

Zero effort integration
Based on business apps

Platform layer

App

Sensor networks

Assets

Machines

Security

Safety
Digital Manufacturing – from static safety rules .. to Digital Twin Safety Engineering

- Adding a digital copy (Digital Twin) to the machine by creating an "Administration shell" including the required content .. IIC ..
- Deployment of a distributed administration shell requires safety & security guidelines ➔ Digital (Twin) Safety Engineering

How do we generate trust into the correct behaviour of the digital and the analog part of an IIoT component?
Digital Manufacturing – Physical Twin and Digital Twin

**Physical Twin**

**Digital Twin**

**Layers**
- Business
- Functional
- Information
- Communication
- Integration
- Asset

**Value Stream**
- Development
- Production
- Maintenance
- Usage

**Hierarchies**
- IEC 62264
- IEC 62541

**Integration & Test**

**Operation**

**Digital Manufacturing – from Physical Twin to Digital Twin**

**Safety Engineering**

**Physical Twin**
- Plan
- Design
- Build & Qualify
- Integrate & Test
- Operation

**Digital Twin**

**Administration shell**
- Representation of information
- Technical functionality

**Asset**

**14.0 component**
- Manifest
- Component manager
Content

- Smart Manufacturing ➔ Digital Twin Safety Engineering
- Smart Manufacturing ➔ extended IIoT Risk Assessment
- Pilot learning ➔ Practical consideration for safety & security
- Evolution for the Technical Lifecycle of adaptive IIoT products
Production plant goes Industrie 4.0 - Connectivity of all life cycles

IIoT establishes a connectivity goes beyond the shop floor along the value chain extending to suppliers and customers, addressing the entire product life cycle. Safety is becoming an intrinsic part of product life cycle. ➔ Plug and Produce on plant level.

What is a complete safety chain within an IIoT production landscape? / How to ensure an appropriate secure environment?
Manufacturing – Risk Management ➔ What is required for safe operations?

RISK MANAGEMENT
Financial risks …
Market risks …
Operational risks

Technical Risk Management

plant & machinery

Machinery Directive

Local Safety & Health regulations

Safety - Compliance - Efficiency

List of directives (EU)
- Machinery Directive
- EMC Directive
- Low Voltage Directive
- Equipment Directive
- Energy-related Products
- Gas Appliance Directive
- RED Directive
- Cyber Security Act
Smart Manufacturing – Risk Management ➔ What is required for safe operations?

From a world of not connected things …

- Safety & Compliance
  - Human
  - Environmental
  - Legal

Efficiency

- Availability
- Operating performance
- Energy efficiency

… to the Industrial Internet of Things

- Horizontal and Vertical Integration

- **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**
Smart Manufacturing – Risk Management ➔ extended IIoT Risk Assessment

From a world of not connected things …

- Security
- Resilience

Efficiency

- Human
- Environmental
- Legal

- Availability
- Operating performance
- Energy efficiency

… to the Industrial Internet of Things

- Authentication
- Unique Identification
- Availability
- Data Integrity
- Privacy

• 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 / embedded in a secure environment
Production plant goes Industrie 4.0 - … „Data Economy“ and „Digital Twin“

Connectivity requires Interoperability
Interoperability between machines, robots, software apps
- OPC-UA information models base for SOA
- eCL@ss properties define the semantic

Observe and consider always the complete safety chain
Technological Risk Management
- Availability
- Operating performance
- Energy efficiency

TÜV SÜD stepwise methodology for the certification of connected and adaptive products:

1. Modified risk assessment for connected smart machines, robots and sensor networks and evaluation of the application covering the safety and the security asset assessment.

2. Creation of functionality and reliability models of the system including sensors, additional control logic and actors and the latency and the probability part of wireless communication (into edge & fog cloud).

3. Estimation of failure rates and reliability data including real time data analytics.
Content

Smart Manufacturing ➔ Digital *Twin* Safety Engineering

Smart Manufacturing ➔ extended IIoT Risk Assessment

Plug & Produce ➔ *IIoT* Risk Assessment as a … “continuum”

Pilot learning ➔ Practical consideration for safety & security

Evolution for the Technical Lifecycle of adaptive IIoT products
Manufacturing - Machinery Services during technical life cycle

Machinery Directive

2006/42/EC

MANUFACTURING
- design
- assembly
- CE Consultancy
- Risk Assessment according EN 12100
- ...

Use Of Work Equipment Directive
2009/104/EC

COMMISSIONING
- CE - declaration
- CE Approval Test
- Acceptance Test prior use of Work Equipment
- ...

OPERATION
- use
- production
- Periodic Inspection
- Safety Audit / Risk Assessment
- ...

TÜV SÜD Product Service | Risk Management in the Age of IIoT / Digital Manufacturing
Manufacturing – **Machinery Safety** Services during technical life cycle

- **Risk Assessment** starts with the definition of the limits of the machine

<table>
<thead>
<tr>
<th>Limits</th>
<th>T1_{Konstruktion}</th>
<th>T2_{Commissioning}</th>
<th>T_X Configuration</th>
<th>y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spatial extend</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></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Machinery Directive
2006/42/EC

Use Of Work Equipment Directive
2009/104/EC
Smart Manufacturing – requires a Security Life Cycle (Threat analysis)

- Risk Assessment starts with the definition of the limits of the machine

<table>
<thead>
<tr>
<th>Limits</th>
<th>T1_Construktion</th>
<th>T2_Commissioning</th>
<th>T_X_Configuration_y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spatial extend</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energetic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>..</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td>Concatenation</td>
</tr>
</tbody>
</table>

Security Life Cycle is running always as a *continuum*.

<table>
<thead>
<tr>
<th>Information Gathering</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Collect and understand requirements</td>
</tr>
<tr>
<td>• Assessment Framework Design</td>
</tr>
<tr>
<td>• Customer specific Profiles</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Analytics &amp; Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Automated analysis of gathered information</td>
</tr>
<tr>
<td>• Correlation and synch up check with other data (e.g. CVSS)</td>
</tr>
<tr>
<td>• Enrichment with relevant Add-On Information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enhanced Info-based Assessment (ACV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Execution of defined Assessment based on valuable and relevant information</td>
</tr>
<tr>
<td>• Assessments under realistic conditions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Advisory</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Definition of actionable insights</td>
</tr>
<tr>
<td>• Support for implementation of countermeasures</td>
</tr>
<tr>
<td>• 3rd party solution evaluation</td>
</tr>
<tr>
<td>• Certification Governance (e.g. ISO 2700x, IEC-62443)</td>
</tr>
</tbody>
</table>
Smart Manufacturing – requires a Safety Life Cycle (Risk assessment as a continuum)

- **Risk Assessment** starts with the definition of the limits of the machine

<table>
<thead>
<tr>
<th>Limits</th>
<th>T1\textsubscript{Construktion}</th>
<th>T2\textsubscript{Commissioning}</th>
<th>T\textsubscript{X} Configuration \textsubscript{y}</th>
<th>T\textsubscript{X+1 \textsubscript{Konfig}; \textsubscript{y+1}}</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spatial extend</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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td></td>
<td></td>
<td>Cloud/Software</td>
<td></td>
</tr>
</tbody>
</table>

Are connectivity, distributed products and adaptability **over lifetime** adequately covered?
Smart Manufacturing (IIoT) – Security Lifecycle - Role definition acc. to IEC 62443

Asset Owner
- operates
- IACS environment / project specific

System Integrator
- integration capabilities (design and deployment)
- independent of IACS environment

Product Supplier
- develops
- -4-1

Includes a configured instance of the Control System Product

Industrial Automation and Control System (IACS)
- Operational and maintenance capabilities (policies and procedures)
- -2-1
- -2-4

Automation Solution
- -3-3

Control System Product as a combination of
- Supporting Applications
- Embedded devices
- Network components
- Host devices

Generic Business Process Control System (BPCS)
- Safety Instrumented System (SIS)
- Complementary hardware and software

Asset Owner operates System Integrator

Integration capabilities (design and deployment)

Product Supplier develops

Independent of IACS environment

IACS environment / project specific

-2-4
Content

- Smart Manufacturing ➔ Digital Twin Safety Engineering
- Smart Manufacturing ➔ extended IIoT Risk Assessment
- Plug & Produce ➔ IIoT Risk Assessment as a “continuum”
- Pilot learning ➔ Practical consideration for safety & security
- Evolution for the Technical Lifecycle of adaptive IIoT products
Certification and Inspection – practical considerations for IIoT

- Demand is coming from (or mostly driven by):
  - Operator (OEM, ..)
  - Insurance companies
  - Regulators

Platform

- Demand generation driven by adaptability and platform complexity
- System Integrator
- Product Supplier
- Asset Owner / Operator

Driven by fast development cycles

virtual type approval
Production scenario ➔ AGV and Cobot move between production cells

Technical Risk Management
- Availability
- Operating performance
- Energy efficiency

➔ Certification & Inspection focused on product level – based on regulation with a static non-adaptable product/asset
➔ Risk Assessment is defined based on well defined & static limits of an asset within an application

AGV (automated Guided Vehicle)
Worker
Robot / Cobot
Production scenario ➔ AGV and Cobot move between production cells

Technical Risk Management
- Availability
- Operating performance
- Energy efficiency

[Tomorrow (t₁ = t₀ + x)]

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

1) Are all changes correctly reflected within the digital twin representation?

2) Is a risk evaluation on request necessary?
Production scenario ➔ AGV and Cobot move between production cells

Smart Factory KL White Paper (HMI 2019) addresses specifically the hazard decision tree for modular production processes.

Safety decision at runtime: Which safety properties are fulfilled?
Safety and Security Life Cycle – practical considerations

*IIoT products require a consistent handling of hazards and risk*

Moving from not connected to Smart Manufacturing / IIoT

…entering the Cyber Security Life Cycle
Safety and Security Life Cycle – *let’s look on the IEC TR 63069 draft*

IEC TR 63069 – Framework for functional safety and security based on IEC 61508 and IEC 62443

**Safety**

- Modified Safety Risk Assessment
  - Identification of Hazard
  - Control measure (Safety functions, ..)
  - Remaining Risk acceptable

- Safety Design

- Safety and Security implementation

**Security**

- Security Threat-Risk Assessment
  - Security countermeasure (security by design requirem.)

- Security environment
Safety and Security Life Cycle – we do need a continuous combined cycle

IEC TR 63069 – Framework for functional safety and security based on IEC 61508 and IEC 62443

- Modified Safety Risk Assessment
- Security Threat-Risk Assessment
- Safety Design
- Security environment
- Changes to safety
  - Continuously inspection
- Safety and Security implementation
- Operation
  - Plug & Produce
- Requirement

IEC TR 63069 – Framework for functional safety and security based on IEC 61508 and IEC 62443
Safety and Security Life Cycle – we do need a continuous combined cycle

Only **quantitative** measures for safety and security will result into Engineering Guidance and a complete lifecycle model.
Safety and Security Life Cycle – we do need ONE technical life cycle for safety & security

Stream data
Process data
Correlate data

Zero Effort integration based on Business Apps

Plattform Layer

Connect

Integrate

Sensor networks

App

Analyse

How different lifecycles are handled in reality?

Changes to safety Continuously inspection

Safety – Security

Asset
Content

- Smart Manufacturing ➔ Digital Twin Safety Engineering
- Smart Manufacturing ➔ extended IIoT Risk Assessment
- Plug & Produce ➔ IIoT Risk Assessment as a… “continuum”
- Pilot learning ➔ Practical consideration for safety & security
- Evolution for the Technical Lifecycle of adaptive IIoT products
Digital evolution for the technical lifecycle of adaptive products

Technical Risk Management
- Availability
- Operating performance
- Energy efficiency

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

- Risk assessment at run time on request
- Based on safety properties => safety semantic

@ \( t_1 = t_0 + x \)
Digital evolution for the technical lifecycle of adaptive products and systems
Combining core know how and new technologies with safety domain expertise

Digital evolution for the technical lifecycle of adaptive products and systems
Combining core know how and new technologies with safety domain expertise

Risk assessment 4.0 (IIoT)
Integrate Smart (IIoT) requirements (safety and security) for connected machinery/robots into assessments

Digitize risk assessment with mCom ONE
Digitize hazard and risk assessment and inspection results over lifetime within ONE safety compliance solution

Integrate Hazards & Threats in Model based simulation
Use model based simulation of hazards and threats to upgrade customers' digital twins for robustness over the lifecycle

Runtime Certification
Safety life cycle services
Provide run-time safety assessment based on digital twin properties for connected production environments

The digital twin integrates lifecycle phases and allows for hazard analysis at early stages

Lifecycle
Design
Construct
InTeGrate & Test
Operation
Digital Twin
mCOM ONE

Advisory services based on holistic process know how

mCOM ONE

Integrate Smart (IIoT) requirements (safety and security) for connected machinery/robots into assessments

Digitize risk assessment with mCom ONE
Digitize hazard and risk assessment and inspection results over lifetime within ONE safety compliance solution

Integrate Hazards & Threats in Model based simulation
Use model based simulation of hazards and threats to upgrade customers' digital twins for robustness over the lifecycle

Runtime Certification
Safety life cycle services
Provide run-time safety assessment based on digital twin properties for connected production environments

The digital twin integrates lifecycle phases and allows for hazard analysis at early stages

Lifecycle
Design
Construct
InTeGrate & Test
Operation
Digital Twin
mCOM ONE

Advisory services based on holistic process know how
Lifecycle calls for new technologies – Example Smart Manufacturing (plug & produce)

- **mCom ONE** is a risk & safety (compliance) management cloud solution
- which empowers our customer to seamlessly integrate a “digital safety twin” for assets (machines & infrastructure)
- into the **end to end business processes** of our customer.
Digital Solution for the technical lifecycle of adaptive products

mCom ONE is a risk & safety compliance management cloud solution which empowers you to seamlessly integrate a “digital safety twin” for assets (machines & infrastructure) into your end to end business processes.

Global standards, risks and hazards → Cloud based assessment and asset management → Targeted solutions and services

mCom+ covers the safety dimension of your digital twin
Digital evolution for the technical lifecycle of adaptive products and systems

Self-Declaration versus IIoT Certification and Inspection

Constraints for **IIoT certification** are different than for **analog products** and strongly application specific

- Same IIoT product has to work properly in different environments
  
  **Against which criteria we certify at time t₀?**

- An IIoT product will change its behaviour over time
  
  - *How do we integrate these changes into the certification/inspection requirements over lifetime?*

- How do we setup validation and test to proof that the certificate guarantees **99% (100%)** achievement?
  
  - Safety it’s clear
  
  - Adaptive safety it’s published
    

  - Security is well described based on IEC 62443 and in other aspects still under discussion

  - Interoperability – the framework is created
Thank you for your attention!