Industrial IoT
Risk Assessment of Smart Factories

IT2Industry – 10.11.2016
Ulrich Ermel | Maximilian Hülsebusch
“Ten years from now, the global manufacturing sector will look nothing like it does today.

Advanced manufacturing technology is rapidly transforming the global competitive landscape. The companies – and nations – that act now to seize its promise will thrive in the 21st century.

Those who are devoted to incremental change and fail to engage in smart manufacturing will rapidly fall behind.”

Sujeet Chand, Chief Technology Officer, Rockwell Automation
Risk Management Standard Factory - Basics

Operational Risks

- Sales
- Sourcing
- Production
- Human Resources
- IT / ERP
Risk Management Standard Factory - Basics

Production Risks

- Resources
  - Machine breakdown
  - Staff shortfall
  - Transport disruption
  - ...

- Materials
  - Materials Shortage
  - Supplies Shortage
  - ...

- Quality
  - Defective products after manufacturing process
  - ...

- Process
  - Technology’s weaknesses
  - ...

Business interruption due to missing and/or defective products
Keeping this assessment in mind, how will smart factories look like?
Smart Factories – VDMA Perspective

![Diagram showing Smart Factories and related concepts]

- **Smart services**
  - Condition Monitoring
  - Predictive Maintenance
- **Online services**
  - Remote maintenance
- **Virtual machines**
  - Traceability
- **Smart production**
  - Circular economy
  - Smart factory
  - 4.0
  - Smart machine
- **Remote control**
  - Central computer
  - MES
- **Data exchange**
  - Self-optimising
- **Intelligent user interfaces**
  - Individualisation
Risk Management Smart Factory - Basics

- Operational Risks
- Sales
- Sourcing
- Production
- Human Resources
- IT / ERP
Risk Management Smart Factory - Basics

Source: Steve Gandy - www.exida.com
Risk Management Smart Factory - Assessment

- Most of **business interruption risks in traditional factories** are covered with business continuance plans (by factory itself) and with business continuance insurances.

- The connection between IT / ERP and production adds risks (USB – „Bring your own device“ – trap with Stuxnet)

- Connecting ERP / IT and production to world wide internet will add new major risks to business continuance (IoT)

- M2M and M2M to IoT will add new major risks to business continuance (data exchange and self-optimization)
Risk Management Smart Factory - Assessment

Who will have to take care of this growing risk?

**Factories**

Who will pay for it?

**Insurance companies**

And who will pay for it in the end?

**Factories**
Let’s be smart and one step ahead.

How risky do insurance companies see smart factories?
Smart Factory – Risk Management Perspective

Who or what is CRO? *
Group of Chief Risk Officers from large multi-national insurance companies

*CRO members as of 14.10.2016, according to www.thecroforum.org
Smart Factory – Risk Management Perspective

What does CRO? *

- Focus on developing and promoting industry best practices in risk management
- Represents the members' views on key risk management topics, including emerging risks.

* according to www.thecroforum.org
Smart Factory – Risk Management Perspective

Landscape of the Smart Factory – complex and cross-linked
Smart Factory – Risk Management Perspective

What are the biggest risks of Smart Factories?

1. Difficulties in determining liability for losses
2. Using and securing data flows
3. Increased vulnerability to cyber-attack
4. The potential for much greater disruption from business interruption
5. Changing labour requirements
Smart Factory – Risk Management Perspective

How will insurance coverage develop with Smart Manufacturing:

Existing
1. Product liability and recall
2. General liability
3. Workers Compensation
4. Contingent Business Interruption and Standard Business Interruption
5. Sudden and accidental losses

Emerging
6. Professional liability
7. High value concentration losses
8. Cyber coverage
Smart Factory – Risk Management Perspective

Cyber related losses caused by:

- **Cyber Attack** (e.g. DDoS)
- **Cyber Espionage** (e.g. data theft)
- **Cyber Sabotage** (e.g. break down of factory)
- **Malware** (e.g. Stuxnet)
The Smart Factory – Risk Management

Hardware and Software in combination will form smart factories.

- We know about **software risks** now and we are able to prepare (see white papers)!

- Do we know about **hardware risks** in smart factories?
The Smart Factory – Risk Management

“IT Equipment will evolve from office environment to be built into industrial and rugged areas.”

Industrial requirements:

- Long-term supply / support
- Spare Parts
- Obsolescence Management
- Risk Management
- Harsh environments
- Medium/low order volumes
The Smart Factory – Risk Management

Standard availability: Industrial

10A power supplies available at 2016

Standard availability: IT
The Smart Factory – Risk Management

There is a lot of work and problems to be solved around hard-and-software topics for future smart factories!

Let’s start to work on it today.
Thank you very much!

Ulrich Ermel  
Director New Business Development  
Arabellastr. 15  
81925 München  
ulrich.ermel@pulspower.com

Maximilian Hülsebusch  
Marketing Communications Specialist  
Arabellastr. 15  
81925 München  
maximilian.huelsebusch@pulspower.com
References

- **Slide 7:** VDMA – „Industrie 4.0 – Begriffe und Nutzen“ on http://plastics40.tv/ October 2016

- **Slides 11-15:** „The Smart Factory – Risk Management Perspectives“ by CRO Forum, December 2015

- **Slide 13:** Vizexplorer, 6 Critical Ideas Behind the Smart Factory and the Internet of Things (IOT)

- **Slide 16:** „White Paper: Managing security, safety and privacy in Smart Factories“ by Smart Factory Innovation Forum, September 2014

- **Slide 16:** „White Paper: Sicherheit in der Industrie 4.0“ by Bundesdruckerei GmbH, October 2016