THE GENEVA ASSOCIATION

The 12th Geneva Association Annual Liability Regimes Conference

Session 1: Industry 4.0 – Industrial Applications of the Internet-of-Things

Munich, 17-18 November 2016

SPEAKERS – Session 1

Christian Fuhrmann (Session Chair)
Chief Executive Global Clients/North America, Munich Re

Hans-Jörg Bullinger
Fraunhofer-Institutszentrum Stuttgart

Thomas Hemker
Security Strategist Symantec

Sebastian Lach
Partner Hogan Lovells LLP

Industry 4.0

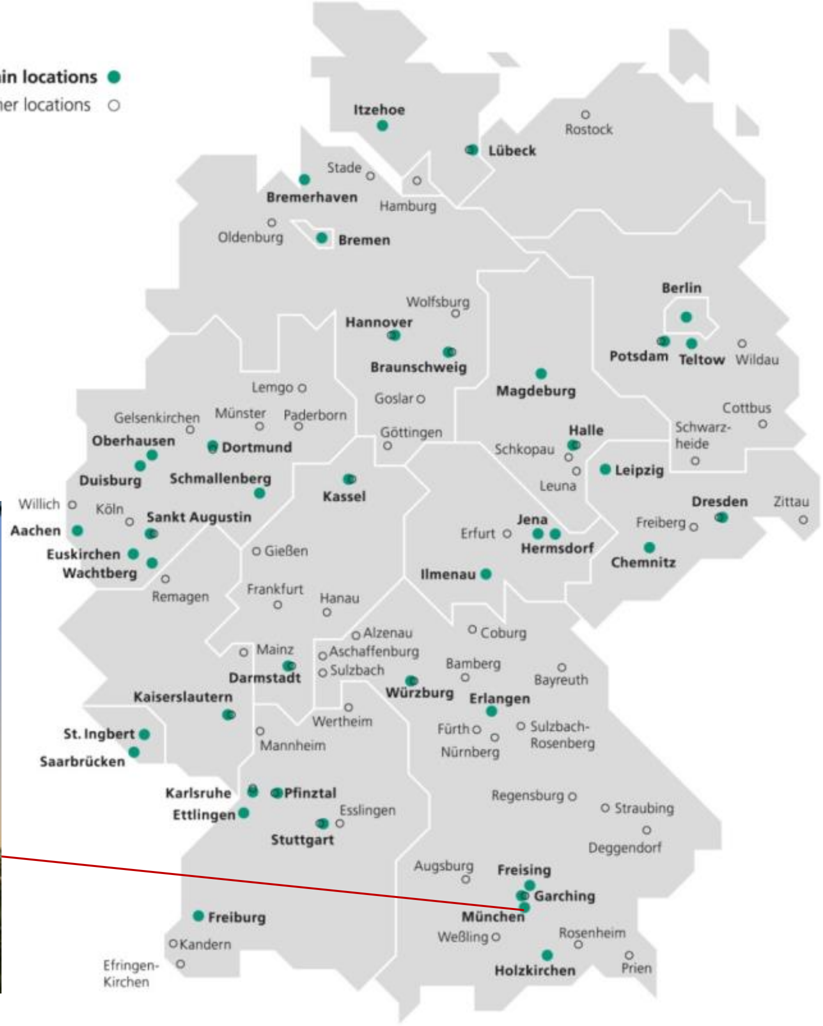
Definition, Impacts, Challenges & Opportunities

Hans-Jörg Bullinger
Fraunhofer-Gesellschaft
www.fraunhofer.de

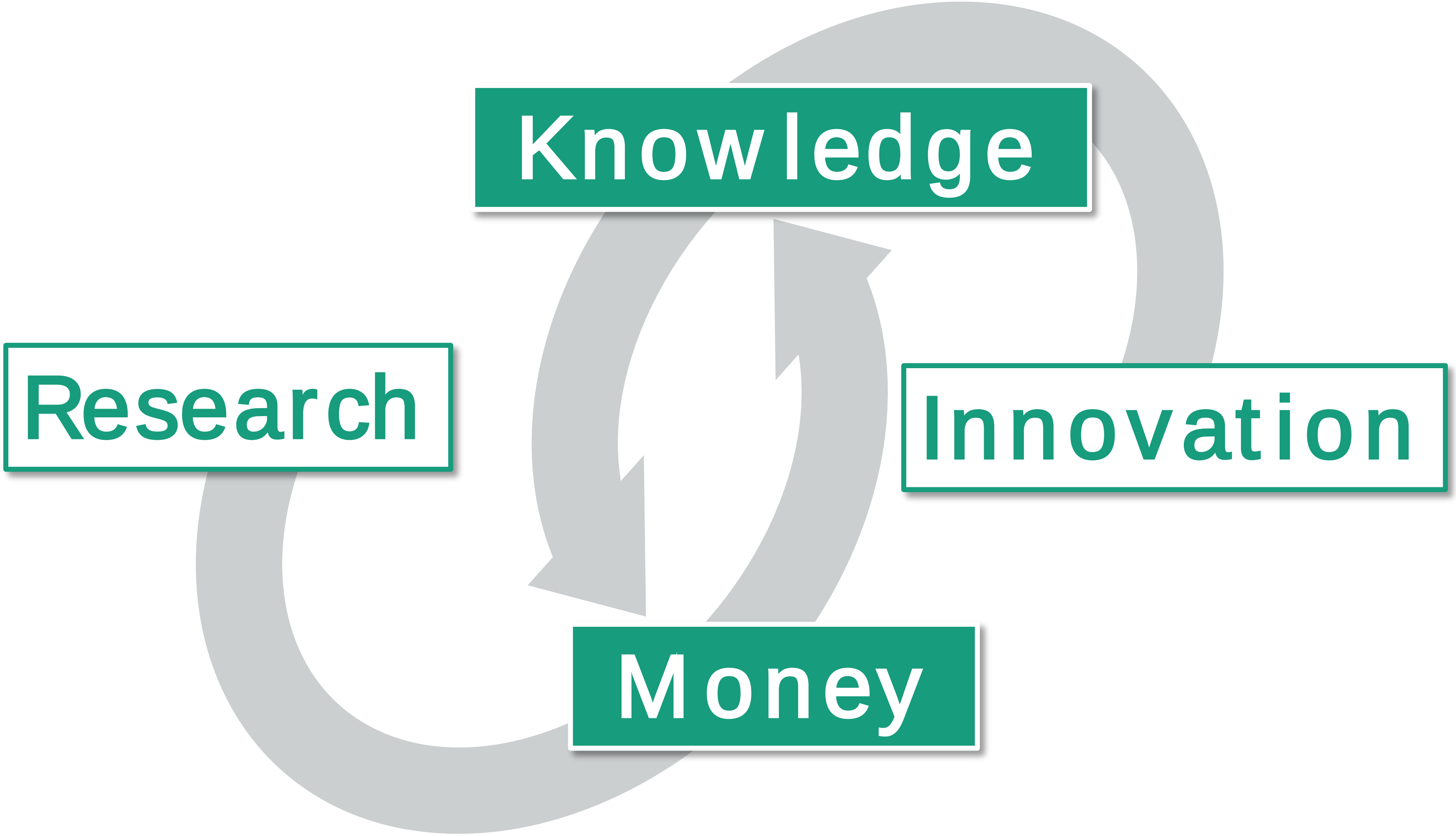
The Fraunhofer-Gesellschaft : Europe‘s largest organization for applied research

- More than 80 research institutions, including 67 Fraunhofer institutes
- International collaboration through representative offices in Europe, the US, Asia and the Middle East
- Approx. 24,000 staff
- Budget: 2.01 Bill. Euro
- Institutes work as profit centers
- One-third of the budget consists of income from industrial projects
- Spinoffs by Fraunhofer researchers are encouraged

Central administration in Munich



Research transfers money into knowledge – Innovation transfers knowledge into money



Knowledge

Research

Innovation

Money

Success stories – Made by Fraunhofer

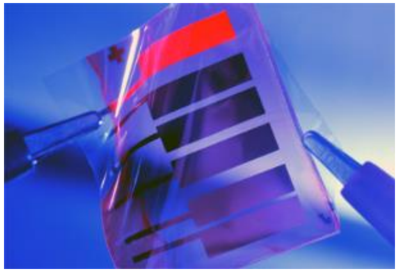
Some of the most popular inventions…

- **MP3** – from a trendsetting technology to a global standard

- **H.265/HEVC** is the next-generation video compression standard

- **Highly efficient solar cells** and concentrator modules with a record-efficiency of 44.7 %

- **White LEDs** and **OLEDs**



Industry 4.0

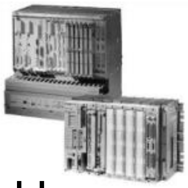
Fraunhofer

Towards an Industry 4.0

Cooperation within social networks

»Smart Factory«

4. Industrial Revolution
Basis: Cyber-Physical Systems

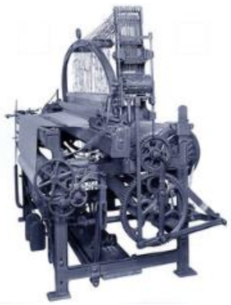


First **programmable controller** »Modicon 084« 1969

3. Industrial Revolution
Electronics and IT for automation of production

Ford **assembly line**
Beginning 20th century

2. Industrial Revolution
Work-sharing mass production with electrical power



First **weaving loom** 1784

1. Industrial Revolution
Mechanical production with water and steam power

Complexity

	End of 18th century / Beginning 20th century	Beginning 1970	today
Work	instruction	workers' participation	cooperation
Processes	rigid	flexible	adaptive in real-time
Resources	based on prediction	consumption	order related

Fraunhofer

Vision #1:
Cyber-Physical Systems and IoT

Cyber-Physical Systems

- via IP addresses connected objects with embedded hardware and software that interact with their environment.
- Objects that consist of their real and virtual representation and keep them up-to-date in real-time over their entire lifetime.

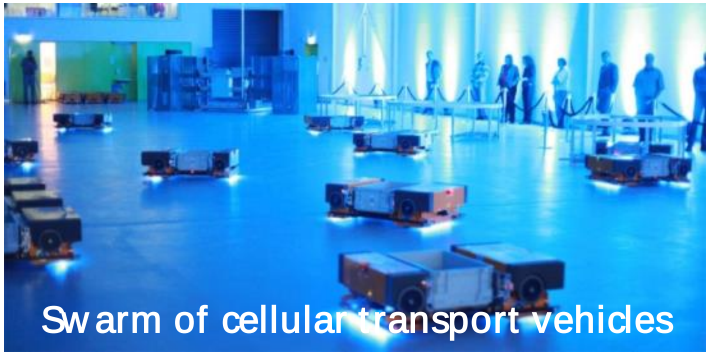
Internet of Things (IoT)

- The Internet of Things is the technical vision, to integrate objects of any kind into a universal digital network. The objects have a unique identity (smart objects) and are / move in a 'smart' environment.”

[Federal Ministry of Economics and Technology 2007]

Intelligent carrier

Source: Fraunhofer IML



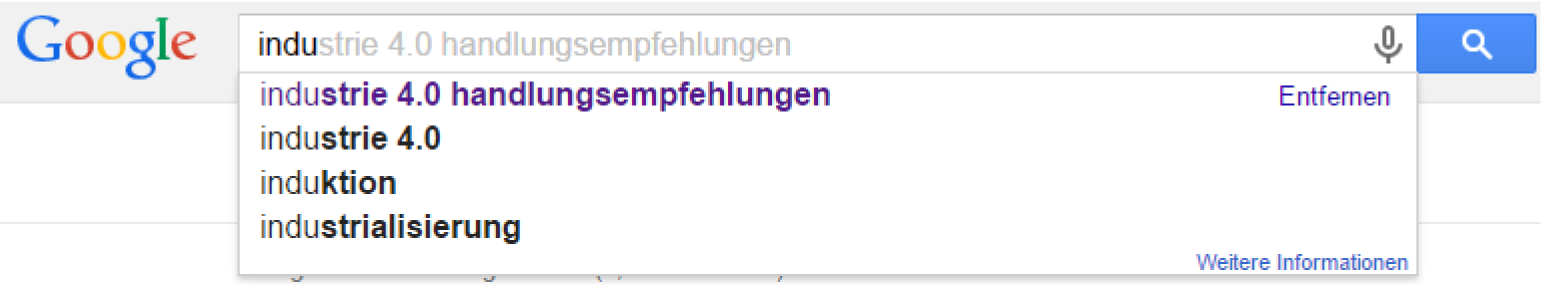
Swarm of cellular transport vehicles

Expectations: significant decrease in planning processes over the life cycle, data acquisition and data processing.

Vision #2:
Big and Smart Data

Big Data

- Real-time processing of **large unstructured data** offers new interrelations for process and product improvement
- Real-Time data processing and process transparency can be used to make **better decisions** than today



industrie 4.0 handlungsempfehlungen

industrie 4.0 handlungsempfehlungen — Entfernen

industrie 4.0

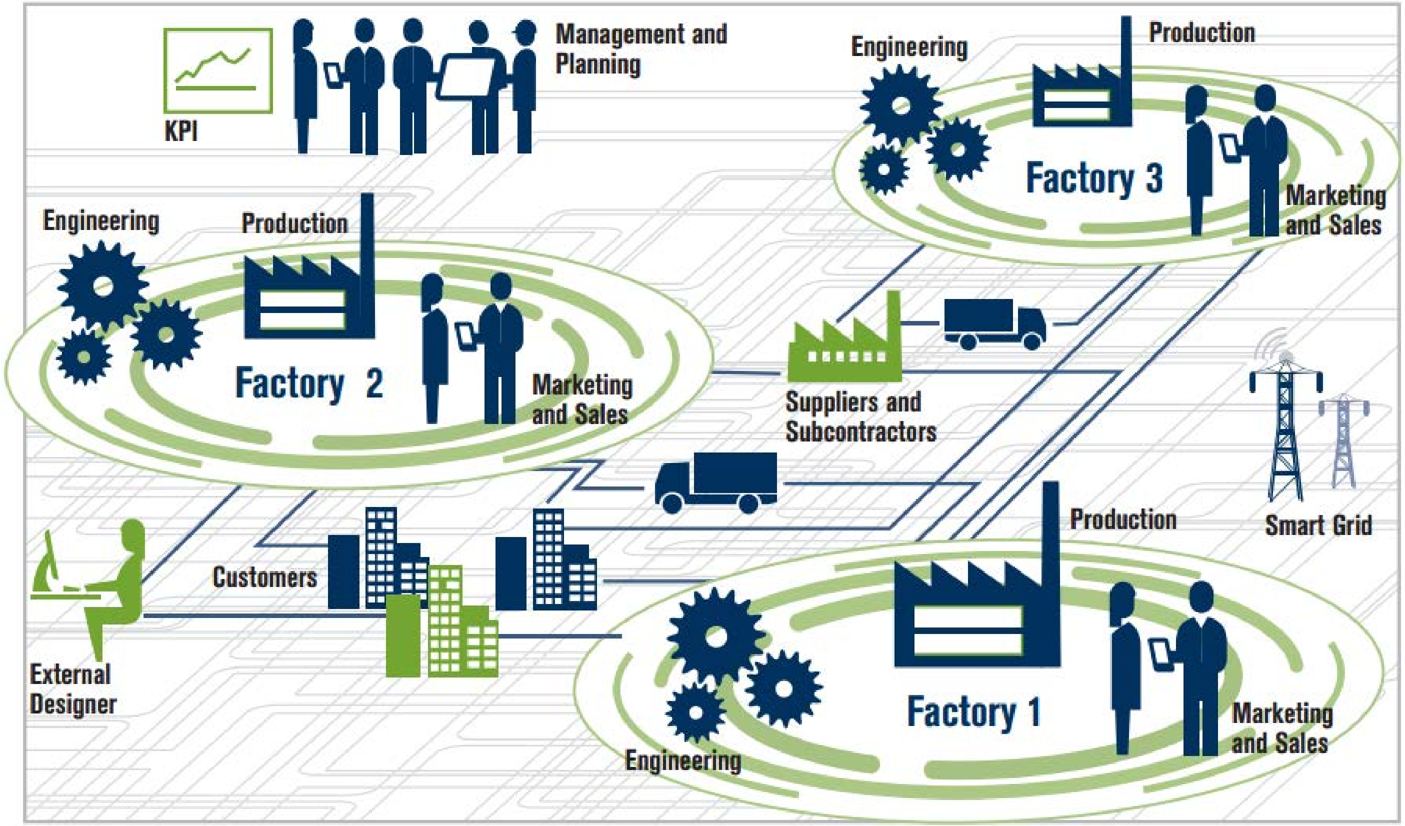
induktion

industrialisierung

Weitere Informationen

Expectations: significant decrease in interaction, clarification and escalation processes, better process knowledge and new business models.

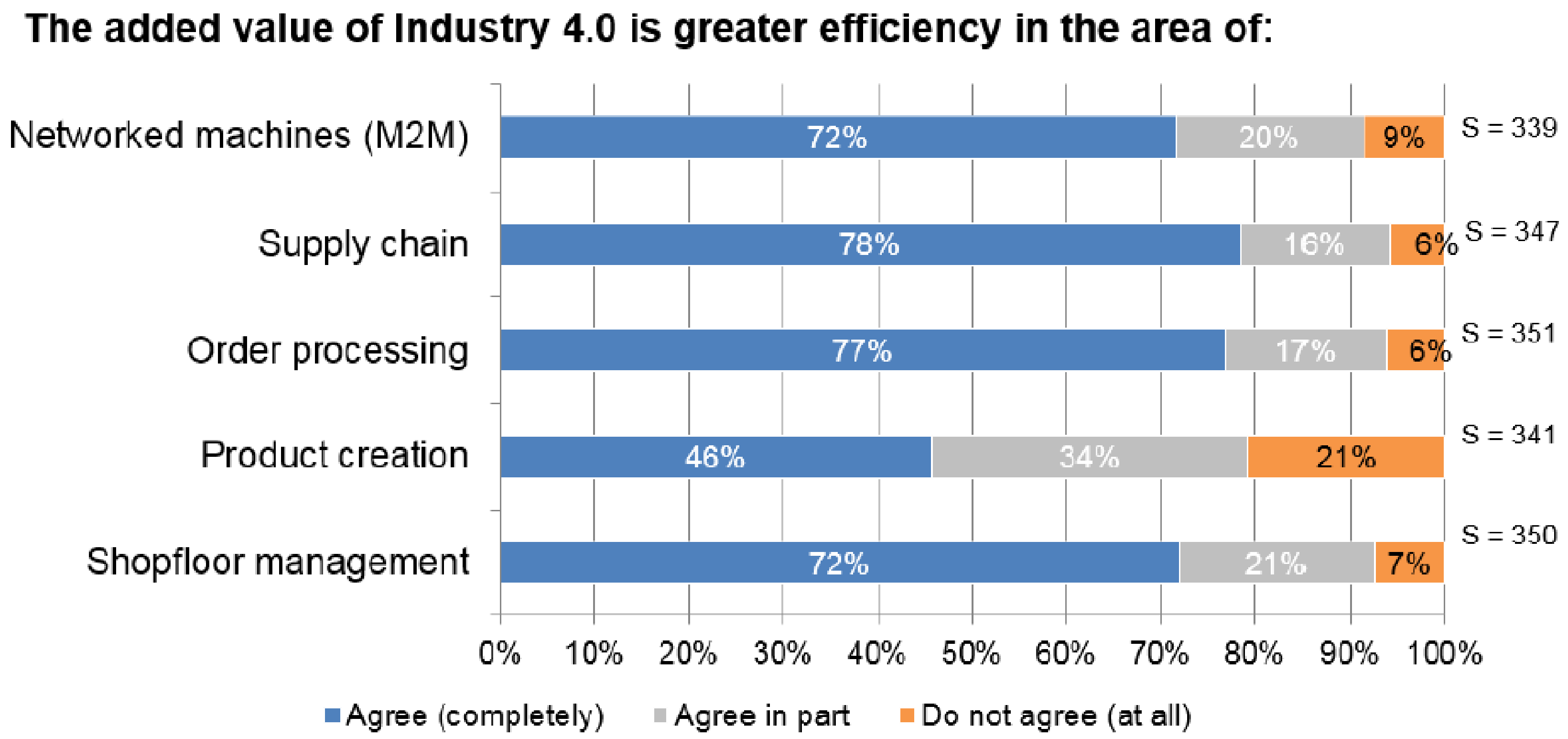
Vision #3:
Real-Time Data Integration over Value Chains



Expectations: real-time traceability and manipulation;
novel business opportunities and models.

Picture: acatech, 2013

Vision #4:
Significant added value expected



High expectations regarding efficiency gains by industry 4.0 – within own processes and across the value chain.

Source: Ingenics AG/Fraunhofer IAO (2015): Industry 4.0 – A revolution in work organization

The potential Value Effect of Industry 4.0 for Western Europe is about 420 Billion Euro*

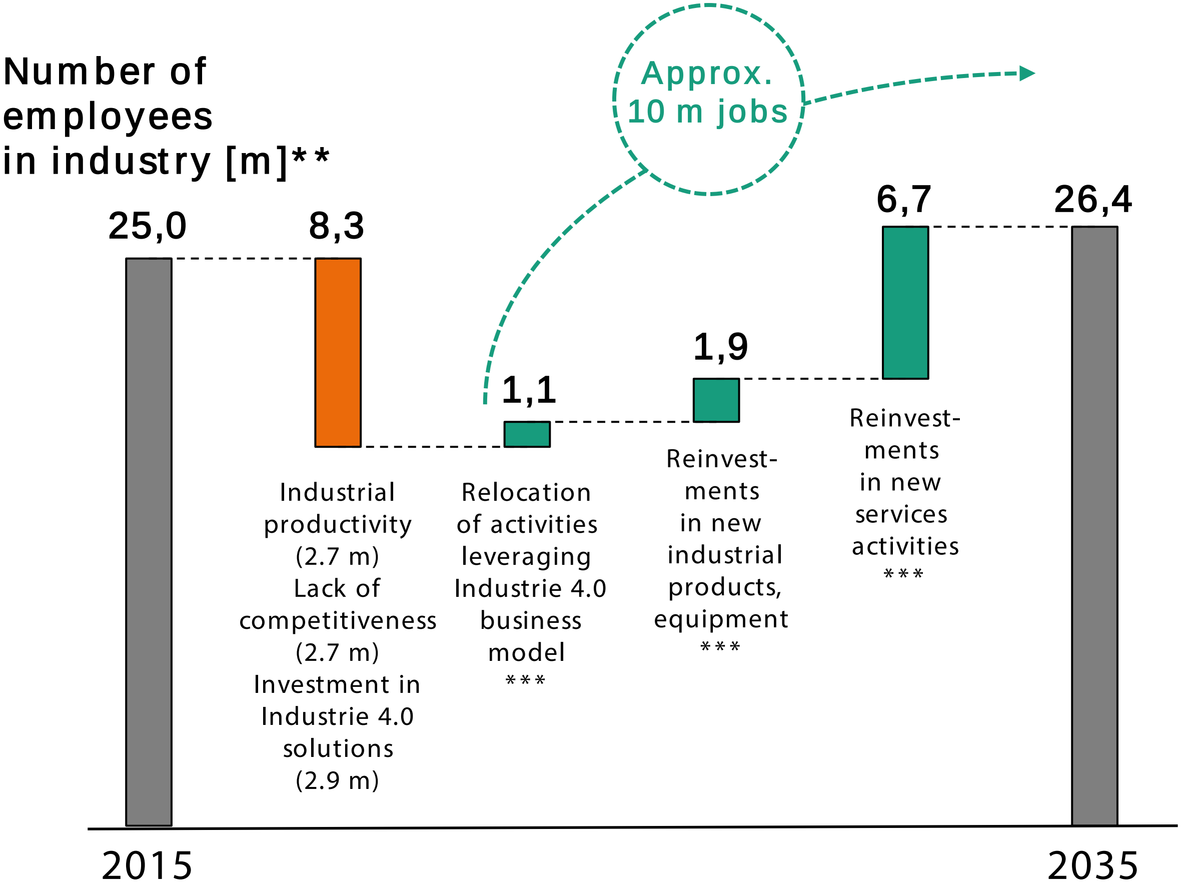
Increase of ROCE from 18 % up to 28% until 2035

* net profits and savings in capital employed would be the value effect of Industrie 4.0.

** adoption rate of 50% for Industrie 4.0 solutions until 2035.

*** The created jobs by new industrial activities bear little resemblance to old ones and are based on an entirely different business model.

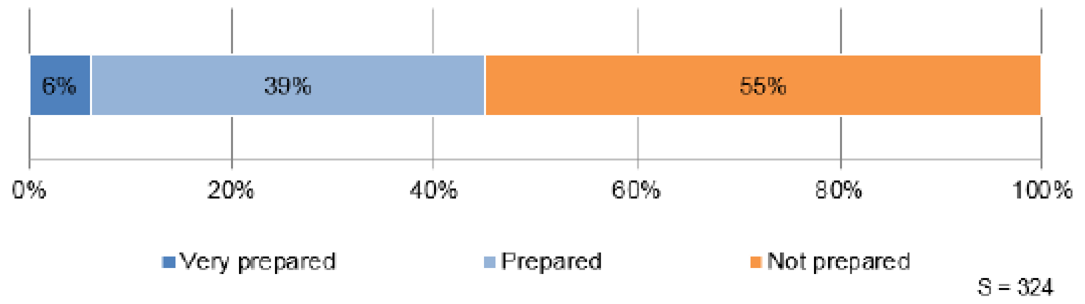
ROCE = Return on Capital Employed



Source: Roland Berger 2016

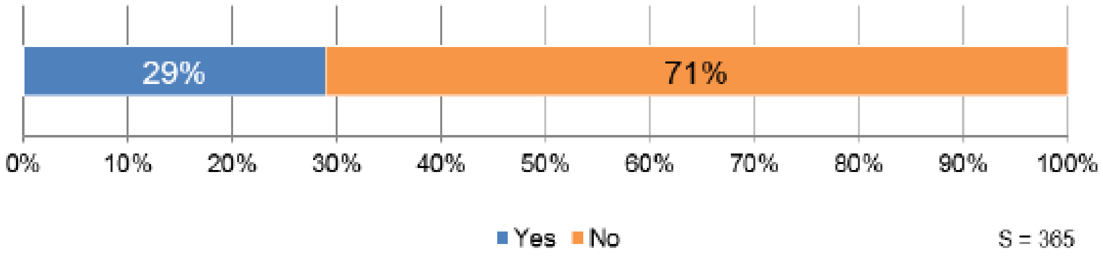
Industry 4.0 has to be worked out

How would you rate your company in terms of its preparation for Industry 4.0?



Only 6% of enterprises consider their Industry 4.0-preparations as very high.

Does your company have an Industry 4.0 strategy?



Only 29% of enterprises have implemented Industry 4.0 as strategic initiative.

**Industry 4.0 has to be worked out –
it is penetrating enterprises top-down.**

Source: Ingenics AG / Fraunhofer IAO (2015): Industry 4.0 – A Revolution in work organization

Production and Digitization

Fraunhofer

Production in former times …

Bundesarchiv, Bild 183-H0813-0600-032
Foto: Dreyer | November 1948

1948

Bundesarchiv, B 145 Bild-F003555-0004
Foto: Unterberg, Rolf | Mai 1956

1956

Source: Bundesarchiv, Germany

Production today

»Lean, clean & green«

Source: Volkswagen AG

Production of the Future

6 challenges are transforming industrial production

1 Horizontal and vertical system integration

2 Visualization

3 Augmented Reality

4 Industrial Internet of Things

5 Human-Robot interaction

6 IT-Security

Fraunhofer

Challenge 1: Horizontal and vertical system integration

Digitization of value added systems

- Further development of industrial value added systems

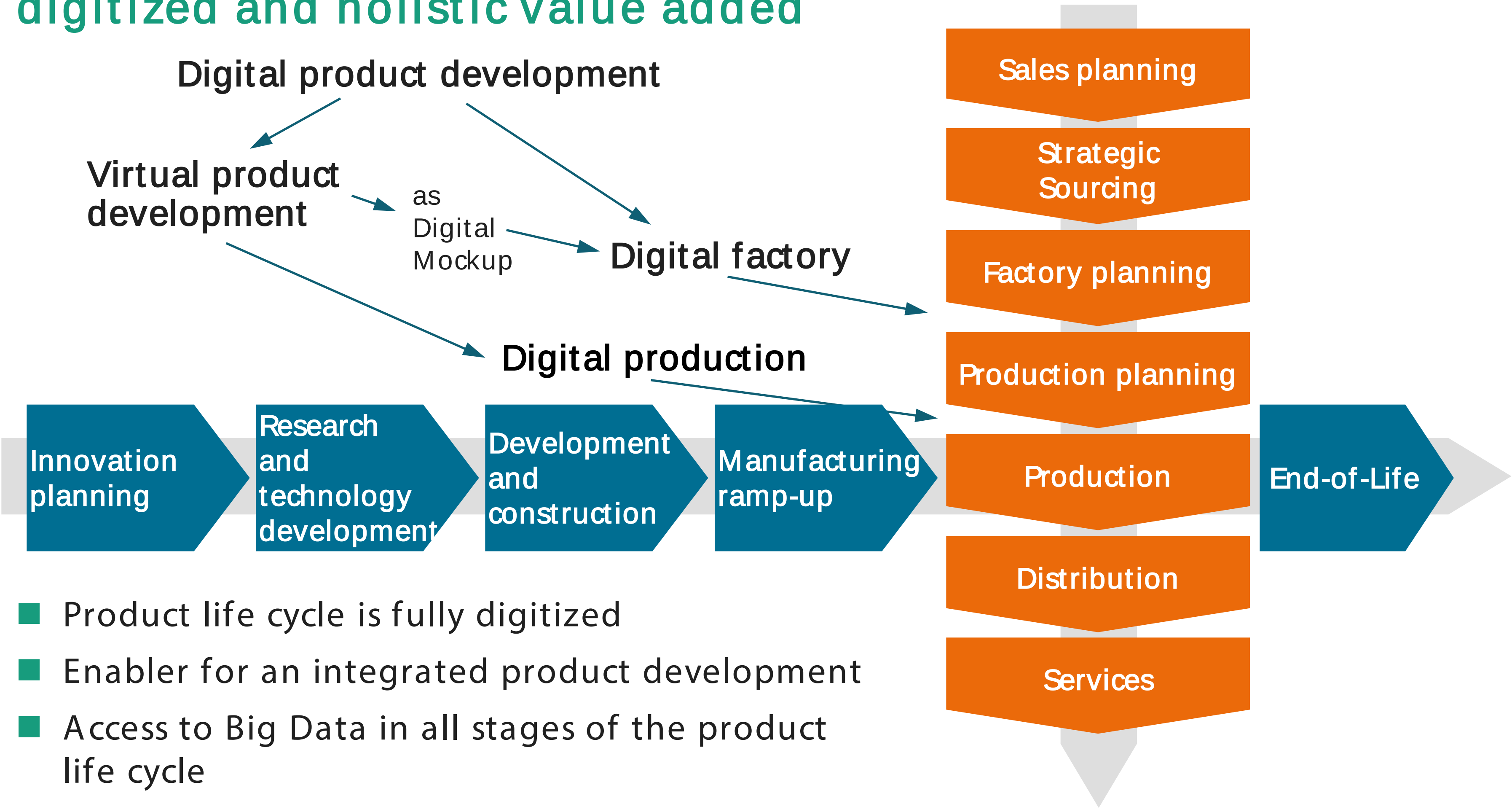
- Coupling of machines via the internet

- Technological perfection of production plants with high integration of employees, customers and users

Sources: BITKOM, Fraunhofer IAO

Challenge 1: Horizontal and vertical system integration

Digital production supports the management of a fully digitized and holistic value added



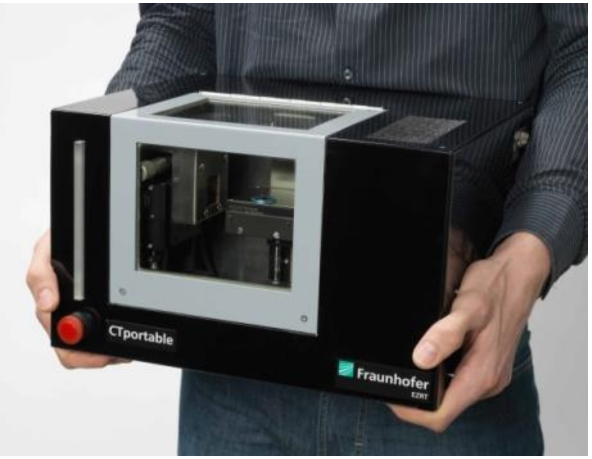
- Product life cycle is fully digitized
- Enabler for an integrated product development
- Access to Big Data in all stages of the product life cycle

Source: McKinsey Global Institute, 2013; BITKOM: Big Data und Geschäftsmodellinnovationen in der Praxis, 2015

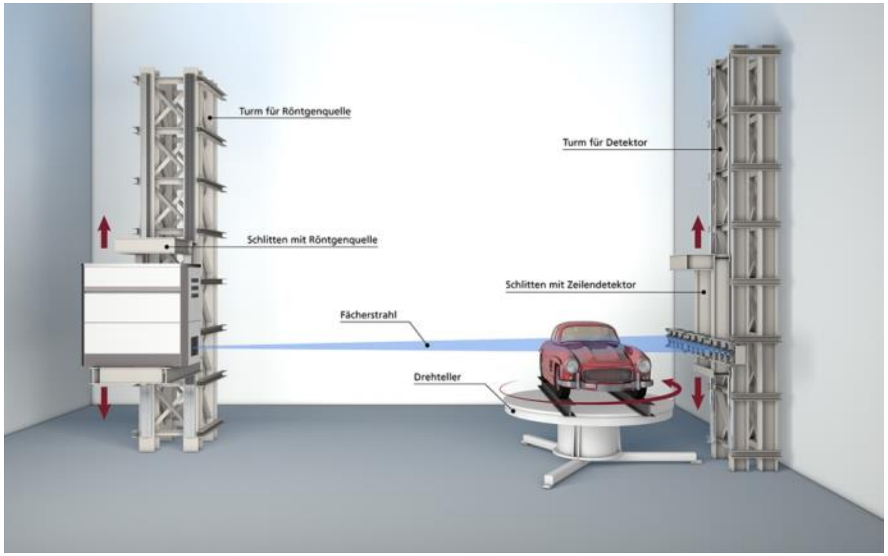
Challenge 2: Visualization

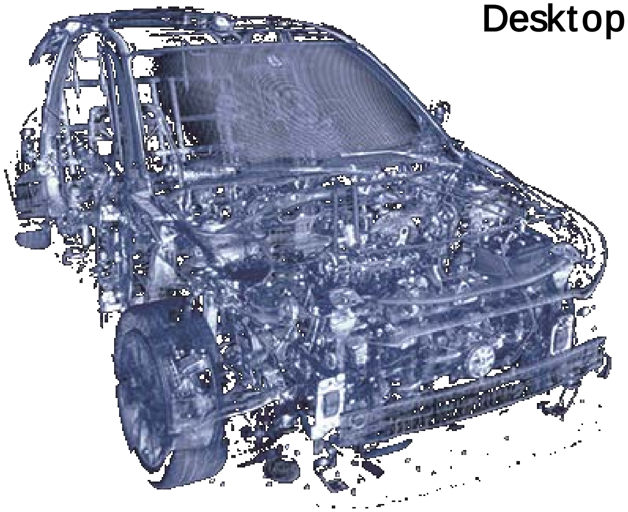
Visualization – 3D CT scans for digitization

The world´s smallest and largest CT-Scanners at the development center for X-ray technology (EZRT) in Fürth, Germany. With **two eight-meter-high steel towers and a turntable of three meters in diameter**, oversized objects can be completely and non-destructively scanned and displayed in 3D.



Desktop-CT-Scanner





Source: Fraunhofer IIS, IZFP

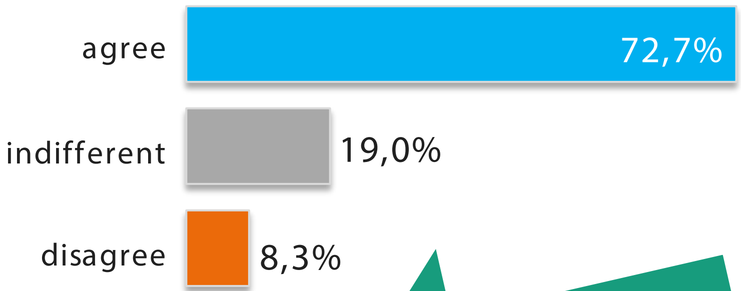
XXL-CT-Scanner

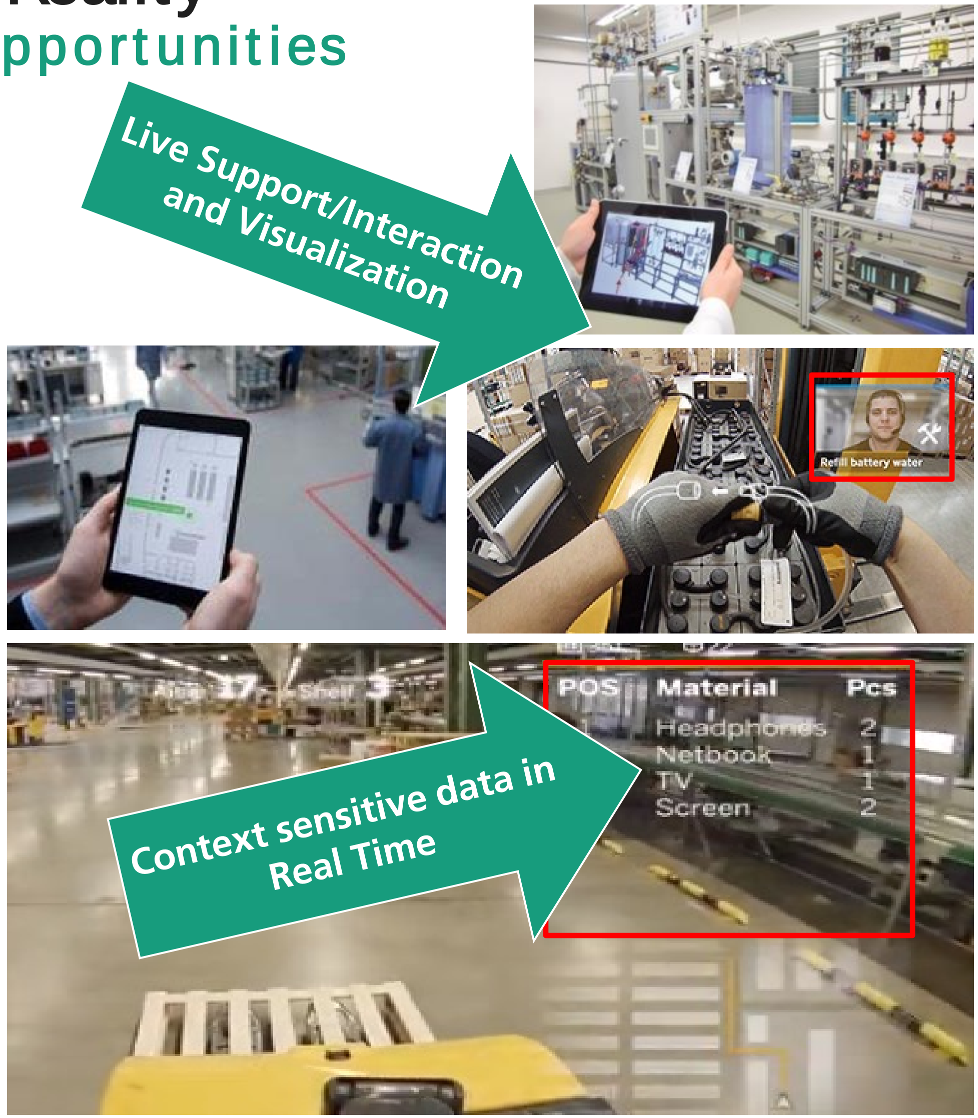
3D-Visualization of a fully assembled vehicle

Challenge 3: Augmented Reality

Mobile devices offer new opportunities due to the use of current manufacturing data

Expert survey:





Live Support/Interaction and Visualization

Context sensitive data in Real Time

Integrated QR-Scanner

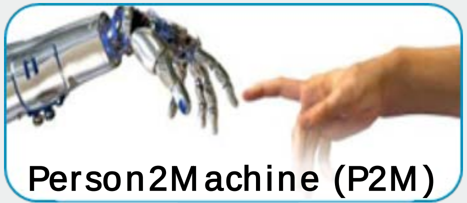
Sources: Fraunhofer IAO: Produktionsarbeit der Zukunft – Industrie 4.0; itizzimo

Challenge 4: Internet of Things (IoT)

The Internet of Things is the technical vision, to integrate any objects in an universal digital net

Who communicates with whom?

Machine2Machine (M2M)



Person2Machine (P2M)

Thing2Machine (T2M)

... and why?

➡ Best solution linking the **physical and digital world**

➡ Added value: **Simplification, improvements in productivity and improvement of the work/life-balance** via embedded systems

Technical requirements

- RFID-Chips = Intelligent localization technology
- Sensors & Actuators
- Cloud Technology
- IPv6 Advanced address for smart objects
- Data Analytics

- Internet ability for all objects
- High performance broadband infrastructure
- Joint standards & interfaces
- New business models
- Information integration & exchange platform

Industrial Data Space

Challenge 5: Human-Robot Interaction

Physical assistance with cooperating robots

- Shared working space
- Quick installation and operation in different settings

Lightweight portable robot as physical assistant

Source: Fraunhofer IPA, IOF

3D-Human-Machine-Interaction with sensor technology (e.g. with gesture)

Fraunhofer

Challenge 6: IT-Security

Why we do not perceive threats and risks of IT

- The time for a change in our perception is still too short in human evolution .
- There is no receptor for the sensory perception of digital operations.
- Our imagination is not wide enough for many threats and risky operations in IT.
- Our qualification is not sufficient for the various possibilities of global IT-networking

Awareness raising, education and training are pre-settlements to avoid hazards and risks through IT.

Challenge 6: IT-Security

»Cyber-Security 2020« - A 7-point program for IT security in Germany

1. **Digital sovereignty** - Germany needs to become independent in the core areas of IT security
2. **Application laboratories for cyber security** - security research must be proven in practical use
3. **Security by Design** - security needs to be inside from the very beginning
4. **Verifiability by third parties** - security has to be trustworthy
5. **Privacy by Design** – there has to be a responsibility for the privacy protection and confidentiality of personal data
6. **Location Images for decision-makers** - awareness of their own (in)security
7. **Human IT security** - technology must not overwhelm the people

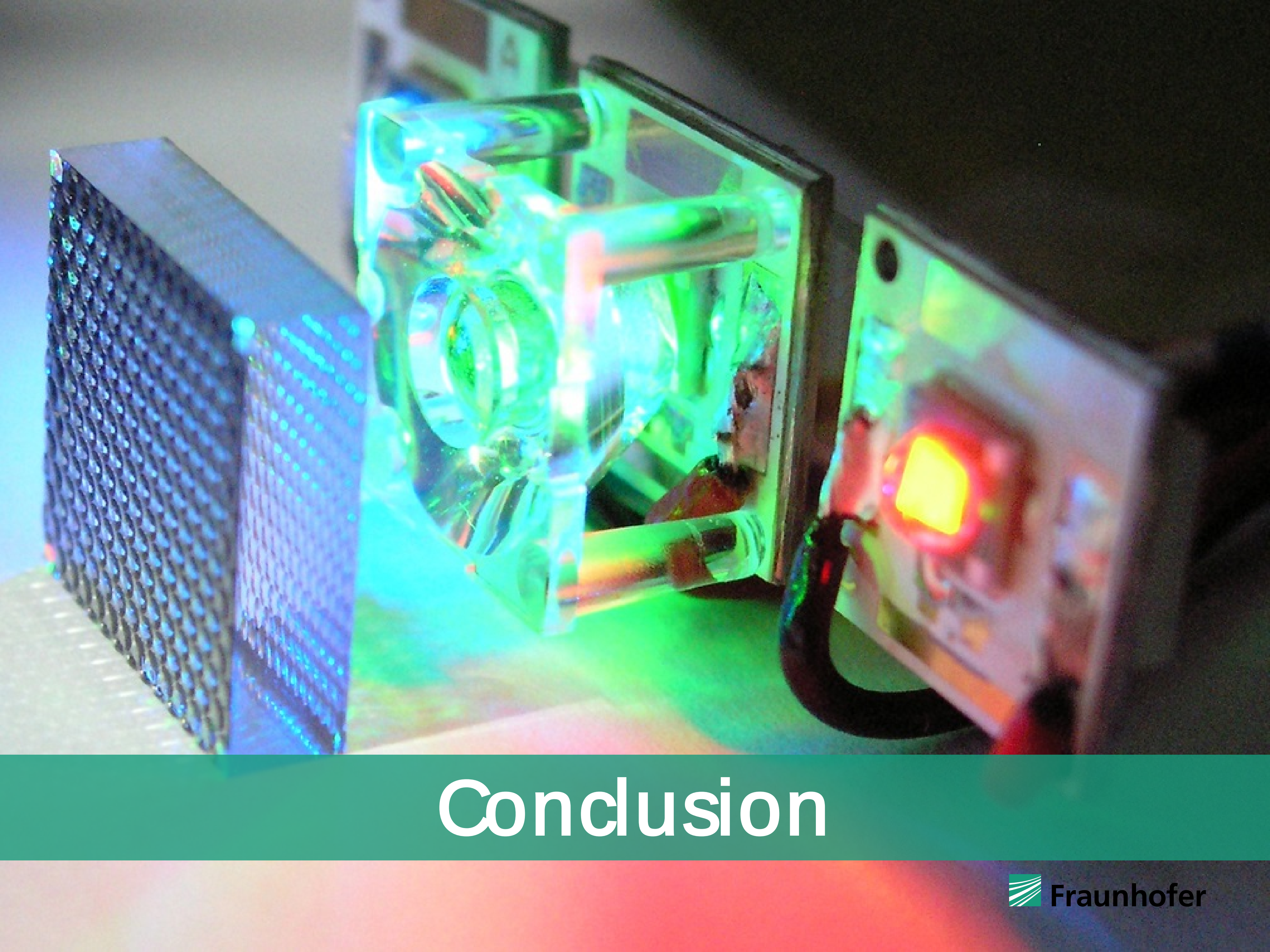
Fraunhofer

FRAUNHOFER-VERBÜNDE IUK-TECHNOLOGIE, VERTEIDIGUNGS- UND SICHERHEITSFORSCHUNG

STRATEGIE- UND POSITIONSPAPIER
CYBER-SICHERHEIT 2020:

HERAUSFORDERUNGEN FÜR DIE
IT-SICHERHEITSFORSCHUNG

Source: Fraunhofer-Gesellschaft, 2014



Conclusion

Production of the Future

6 challenges are transforming industrial production …

1 Horizontal and vertical system integration

2 Visualization

3 Augmented reality

4 Industrial Internet of Things

5 Human-Robot interaction

6 IT-Security

… and have a dramatic impact on Industry 4.0

Fraunhofer

Working for the future.

Managing Cyber Risk in an Industry 4.0 era.

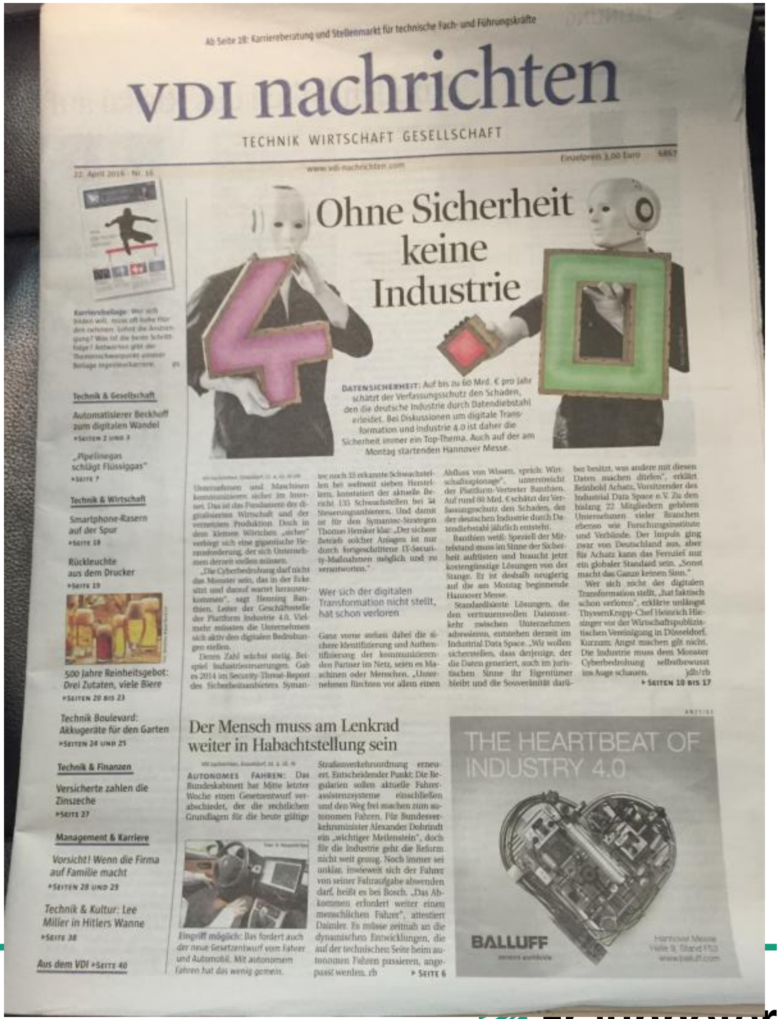
User Perspective

Thomas Hemker, CISSP, CISM, CISA
Security Strategist

AGENDA

- Cyber Security
- Risk Management
- Industry 4.0 Threat landscape
- Requirements
- Q&A

Thomas Hemker, CISSP, CISM, CISA



Ab Seite 28: Karriereberatung und Stellenmarkt für technische Fach- und Führungskräfte

VDI nachrichten

TECHNIK WIRTSCHAFT GESELLSCHAFT

22. April 2016 · Nr. 16

www.vdi-nachrichten.com

Einzelpreis 3,00 Euro 6857

Karrierebeilage: Wer sich bilden will, muss oft hohe Hürden nehmen. Lohnt die Anstrengung? Was ist die beste Schrittfolge? Antworten gibt der Themenschwerpunkt unserer Beilage Ingenieurkarriere.

Technik & Gesellschaft

Automatisierer Beckhoff zum digitalen Wandel
▸SEITEN 2 UND 3

„Pipelinegas schlägt Flüssiggas"
▸SEITE 7

Technik & Wirtschaft

Smartphone-Rasern auf der Spur
▸SEITE 18

Rückleuchte aus dem Drucker
▸SEITE 19

500 Jahre Reinheitsgebot: *Drei Zutaten, viele Biere*
▸SEITEN 20 BIS 23

Technik Boulevard: Akkugeräte für den Garten
▸SEITEN 24 UND 25

Technik & Finanzen

Versicherte zahlen die Zinszeche
▸SEITE 27

Management & Karriere

Vorsicht! Wenn die Firma auf Familie macht
▸SEITEN 28 UND 29

Technik & Kultur: Lee Miller in Hitlers Wanne
▸SEITE 38

Aus dem VDI ▸SEITE 40

Ohne Sicherheit keine Industrie

DATENSICHERHEIT: Auf bis zu 60 Mrd. € pro Jahr schätzt der Verfassungsschutz den Schaden, den die deutsche Industrie durch Datendiebstahl erleidet. Bei Diskussionen um digitale Transformation und Industrie 4.0 ist daher die Sicherheit immer ein Top-Thema. Auch auf der am Montag startenden Hannover Messe.

Unternehmen und Maschinen kommunizieren sicher im Internet. Das ist das Fundament der digitalisierten Wirtschaft und der vernetzten Produktion. Doch in dem kleinen Wörtchen „sicher" verbirgt sich eine gigantische Herausforderung, der sich Unternehmen derzeit stellen müssen.

„Die Cyberbedrohung darf nicht das Monster sein, das in der Ecke sitzt und darauf wartet herauszukommen", sagt Henning Banthien, Leiter der Geschäftsstelle der Plattform Industrie 4.0. Vielmehr müssten die Unternehmen sich aktiv den digitalen Bedrohungen stellen.

Deren Zahl wächst stetig. Beispiel Industriesteuerungen: Gab es 2014 im Security-Threat-Report des Sicherheitsanbieters Symantec noch 35 erkannte Schwachstellen bei weltweit sieben Herstellern, konstatiert der aktuelle Bericht 135 Schwachstellen bei 34 Steuerungsanbietern. Und damit ist für den Symantec-Strategen Thomas Hemker klar: „Der sichere Betrieb solcher Anlagen ist nur durch fortgeschrittene IT-Security-Maßnahmen möglich und zu verantworten."

Wer sich der digitalen Transformation nicht stellt, hat schon verloren

Ganz vorne stehen dabei die sichere Identifizierung und Authentifizierung der kommunizierenden Partner im Netz, seien es Maschinen oder Menschen. „Unternehmen fürchten vor allem einen Abfluss von Wissen, sprich: Wirtschaftsspionage", unterstreicht der Plattform-Vertreter Banthien. Auf rund 60 Mrd. € schätzt der Verfassungsschutz den Schaden, der der deutschen Industrie durch Datendiebstahl jährlich entsteht.

Banthien weiß: Speziell der Mittelstand muss im Sinne der Sicherheit aufrüsten und braucht jetzt kostengünstige Lösungen von der Stange. Er ist deshalb neugierig auf die am Montag beginnende Hannover Messe.

Standardisierte Lösungen, die den vertrauensvollen Datenverkehr zwischen Unternehmen abwickeln, entstehen derzeit im Industrial Data Space. „Wir wollen sicherstellen, dass derjenige, der die Daten generiert, auch im juristischen Sinne ihr Eigentümer bleibt und die Souveränität darüber besitzt, was andere mit diesen Daten machen dürfen", erklärt Reinhold Achatz, Vorsitzender des Industrial Data Space e.V. Zu den bislang 22 Mitgliedern gehören Unternehmen vieler Branchen ebenso wie Forschungsinstitute und Verbände. Der Impuls ging zwar von Deutschland aus, aber für Achatz kann das Fernziel nur ein globaler Standard sein. „Sonst macht das Ganze keinen Sinn."

Wer sich nicht der digitalen Transformation stellt, „hat faktisch schon verloren", erklärte unlängst ThyssenKrupp-Chef Heinrich Hiesinger vor der Wirtschaftspublizistischen Vereinigung in Düsseldorf. Kurzum: Angst machen gilt nicht. Die Industrie muss dem Monster Cyberbedrohung selbstbewusst ins Auge schauen. jdb/rb

▸SEITEN 10 BIS 17

Der Mensch muss am Lenkrad weiter in Habachtstellung sein

AUTONOMES FAHREN: Das Bundeskabinett hat Mitte letzter Woche einen Gesetzentwurf verabschiedet, der die rechtlichen Grundlagen für die heute gültige Straßenverkehrsordnung erneuert. Entscheidender Punkt: Die Regularien sollen aktuelle Fahrerassistenzsysteme einschließen und den Weg frei machen zum autonomen Fahren. Für Bundesverkehrsminister Alexander Dobrindt ein „wichtiger Meilenstein", doch für die Industrie geht die Reform nicht weit genug. Noch immer sei unklar, inwieweit sich der Fahrer von seiner Fahraufgabe abwenden darf, heißt es bei Bosch. „Das Abkommen erfordert weiter einen menschlichen Fahrer", attestiert Daimler. Es müsse zeitnah an die dynamischen Entwicklungen, die auf der technischen Seite beim autonomen Fahren passieren, angepasst werden. rb

▸SEITE 6

Eingriff möglich: Das fordert auch der neue Gesetzentwurf vom Fahrer und Automobil. Mit autonomem Fahren hat das wenig gemein.

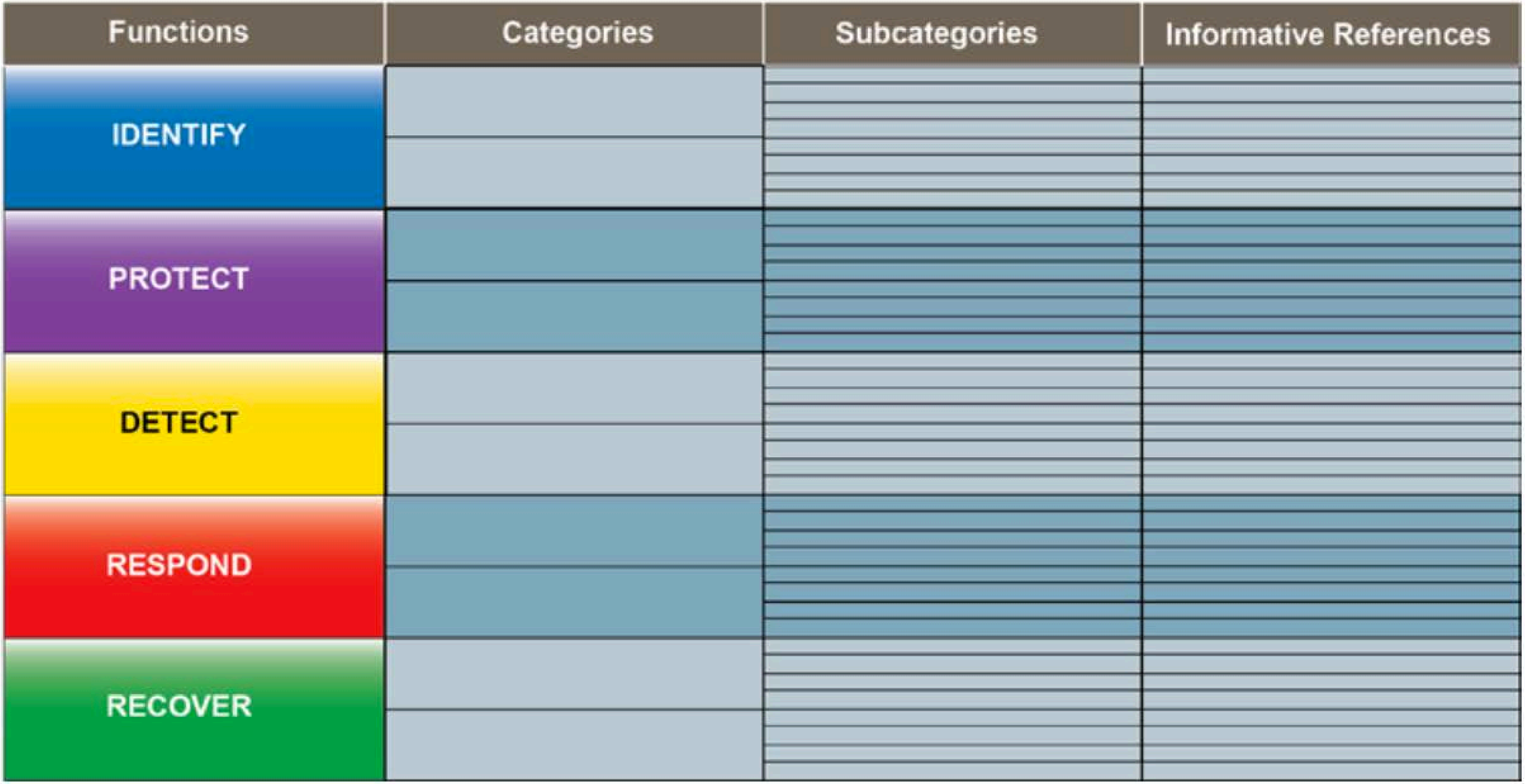
Cyber Security

Confidentiality

Integrity

Availability

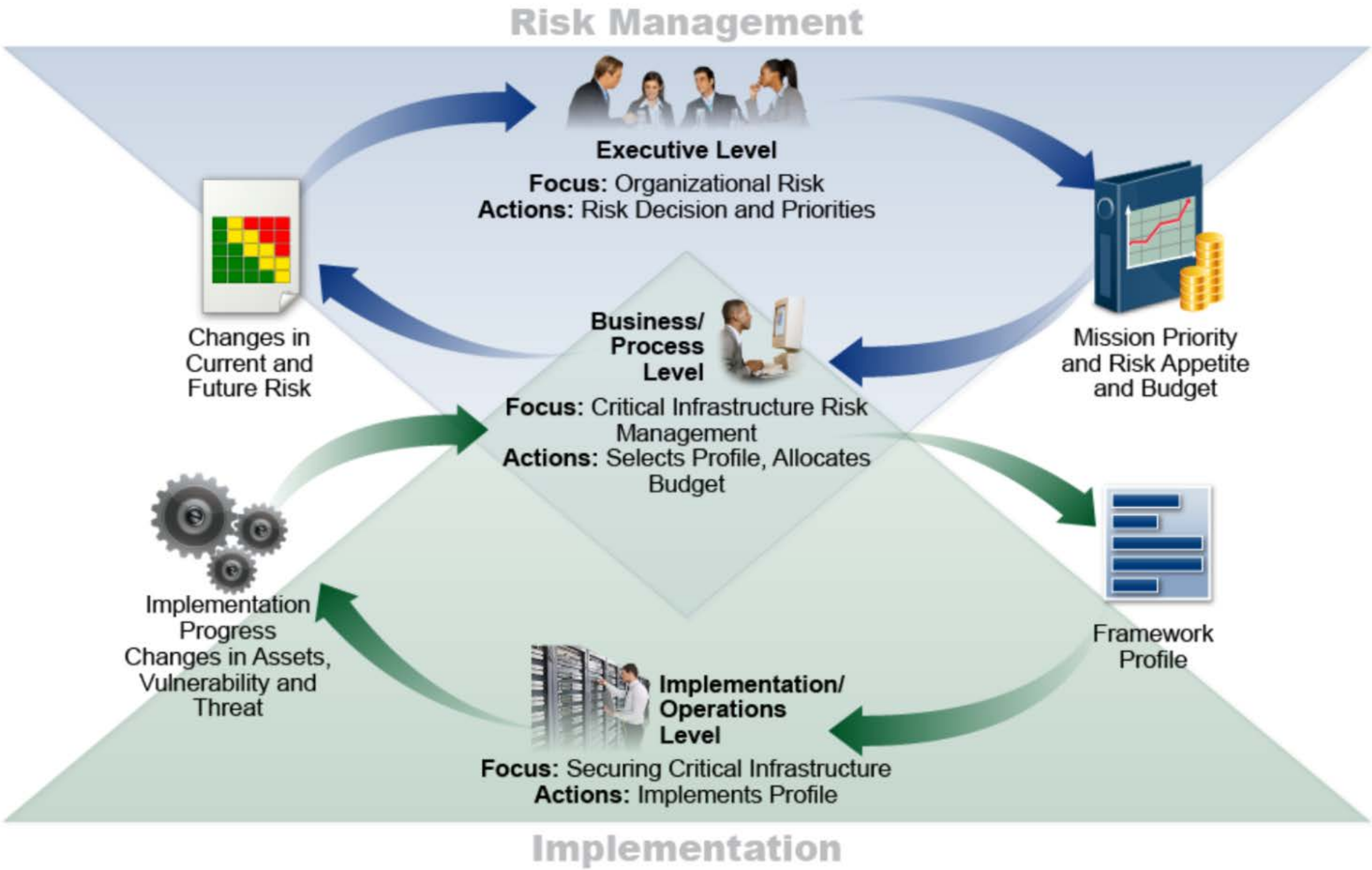
Safety



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 1: Framework Core Structure

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf



Risk Management

Executive Level

Focus: Organizational Risk
Actions: Risk Decision and Priorities

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

Business/ Process Level

Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget

Implementation Progress Changes in Assets, Vulnerability and Threat

Framework Profile

Implementation/ Operations Level

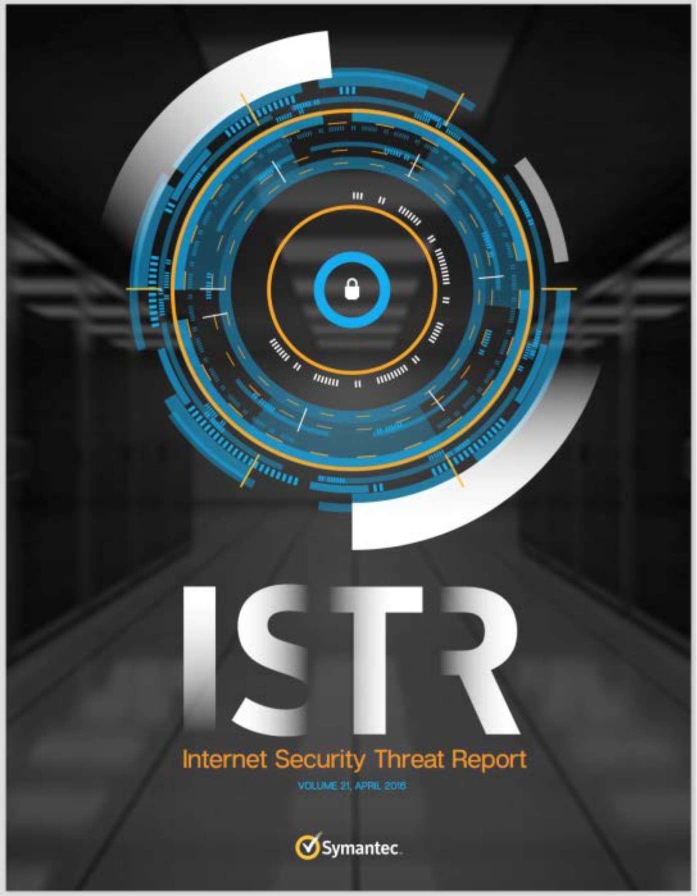
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

Figure 2: Notional Information and Decision Flows within an Organization

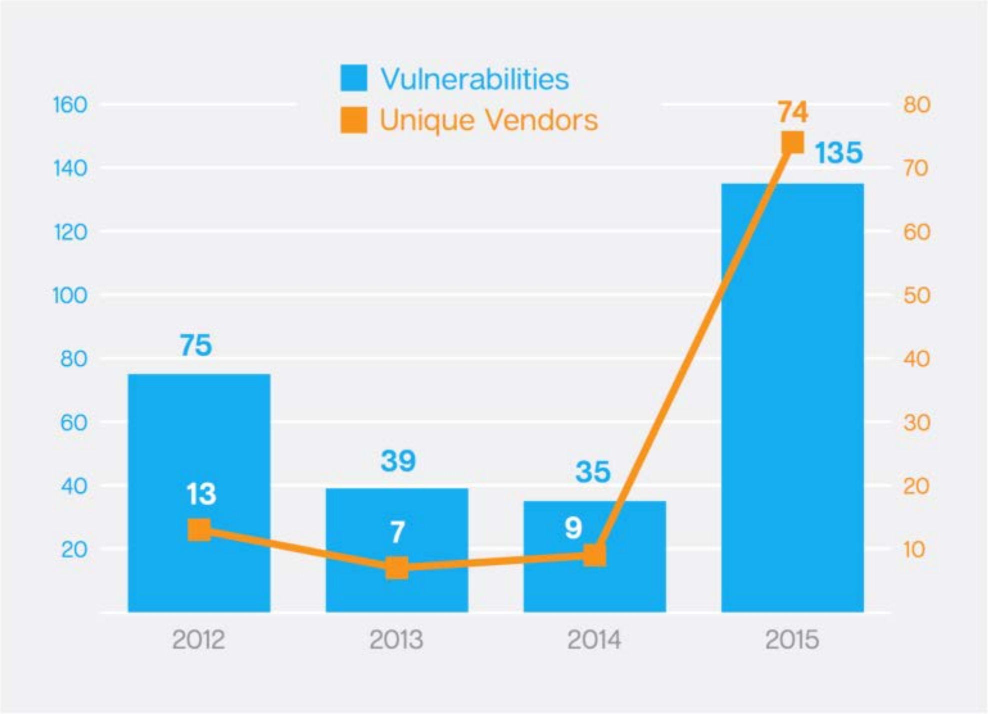
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Threat Landscape - Vulnerabilities



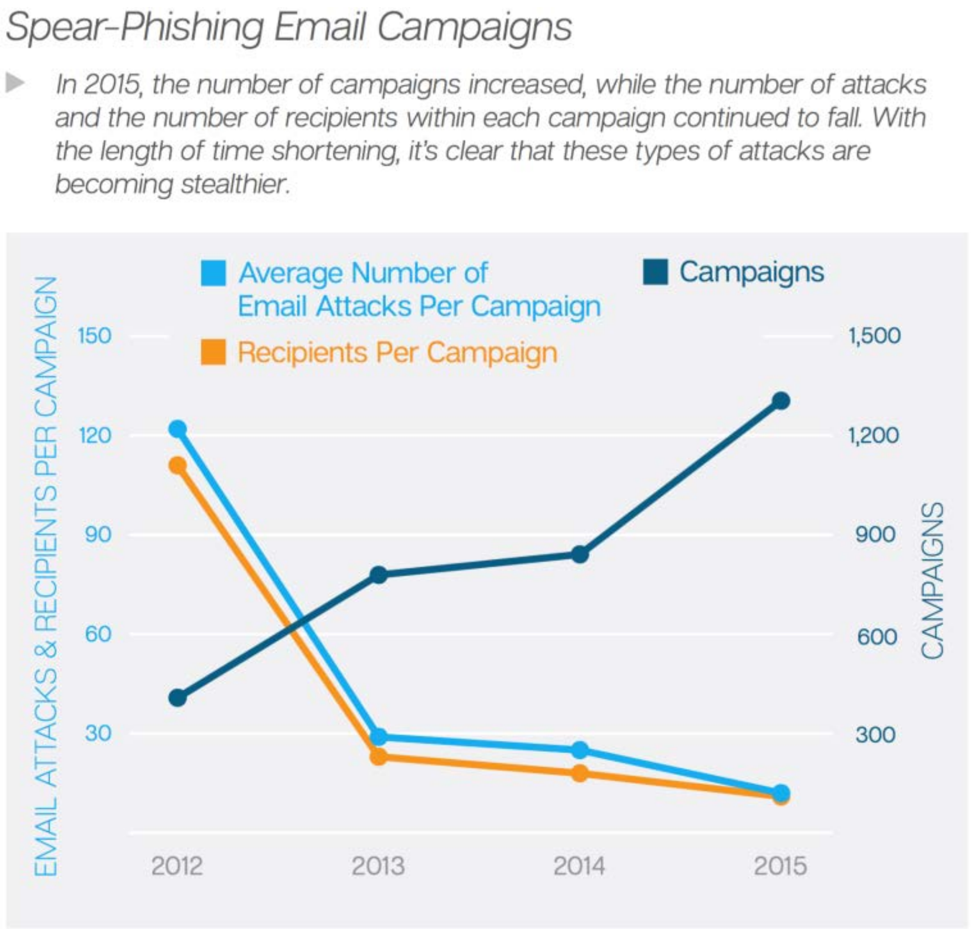
Vulnerabilities Disclosed in Industrial Control Systems

- At least seven zero-day vulnerabilities directly related to a variety of different ICS manufacturers and devices in 2015.



https://www.symantec.com/security_response/

Threat Landscape – Targeted Attacks



Spear-Phishing Email Campaigns

- In 2015, the number of campaigns increased, while the number of attacks and the number of recipients within each campaign continued to fall. With the length of time shortening, it's clear that these types of attacks are becoming stealthier.

Symantec.

SECURITY RESPONSE

Dragonfly: Cyberespionage Attacks Against Energy Suppliers

Symantec Security Response

Version 1.1: June 30, 2014, 15:00 GMT

> “Dragonfly initially targeted defense and aviation companies in the US and Canada before shifting its focus to US and European energy firms in early 2013.”

Follow us on Twitter @threatintel

Visit our Blog http://www.symantec.com/connect/symantec-blogs/sr

https://www.symantec.com/security_response/

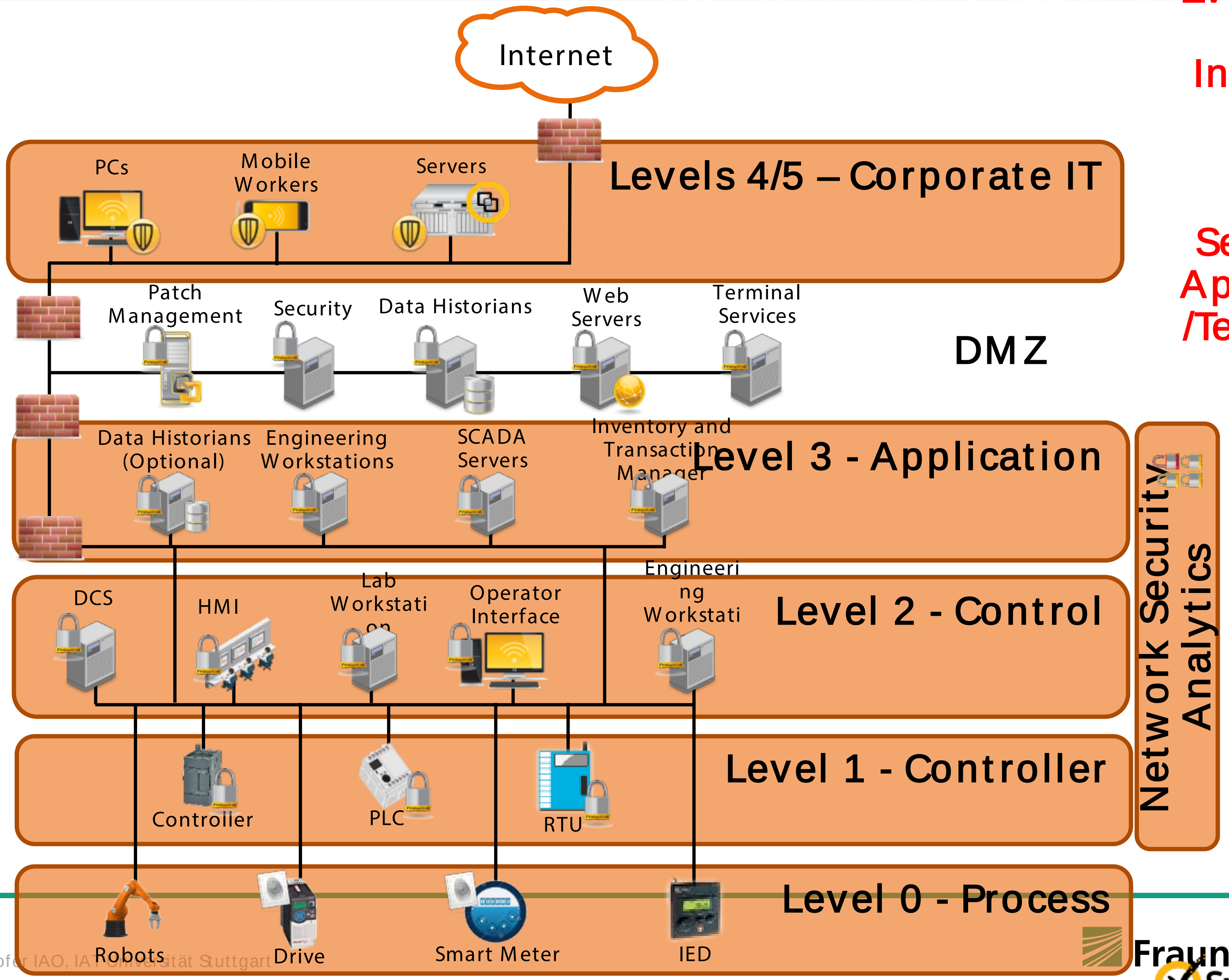
IEC 62443

Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Terminology, concepts and models	**2-1** Requirements for an IACS security management system	**3-1** Security technologies for IACS	**4-1** Secure Product Dev. Lifecycle Requirements
1-2 Master glossary of terms and abbr.	**2-2** Implementation guidance for an IACS security management system	**3-2** Security Risk Assessment and System Design	**4-2** Technical security requirements for IACS components
1-3 System security compliance metrics	**2-3** Patch management in the IACS environment	**3-3** System security requirements and security levels	
1-4 IACS security lifecycle and use-case	**2-4** Security program requirements for IACS service providers		

Evolution to Industry 4.0

New Security Approach /Technology



Extrinsic Security

Add-on Security

PC/Datacenter Era

- Bolt-On Security
- Layers of Security added to PCs, Servers, Networks and Devices

Intrinsic Security

Security-by-Design

Internet of Things Era

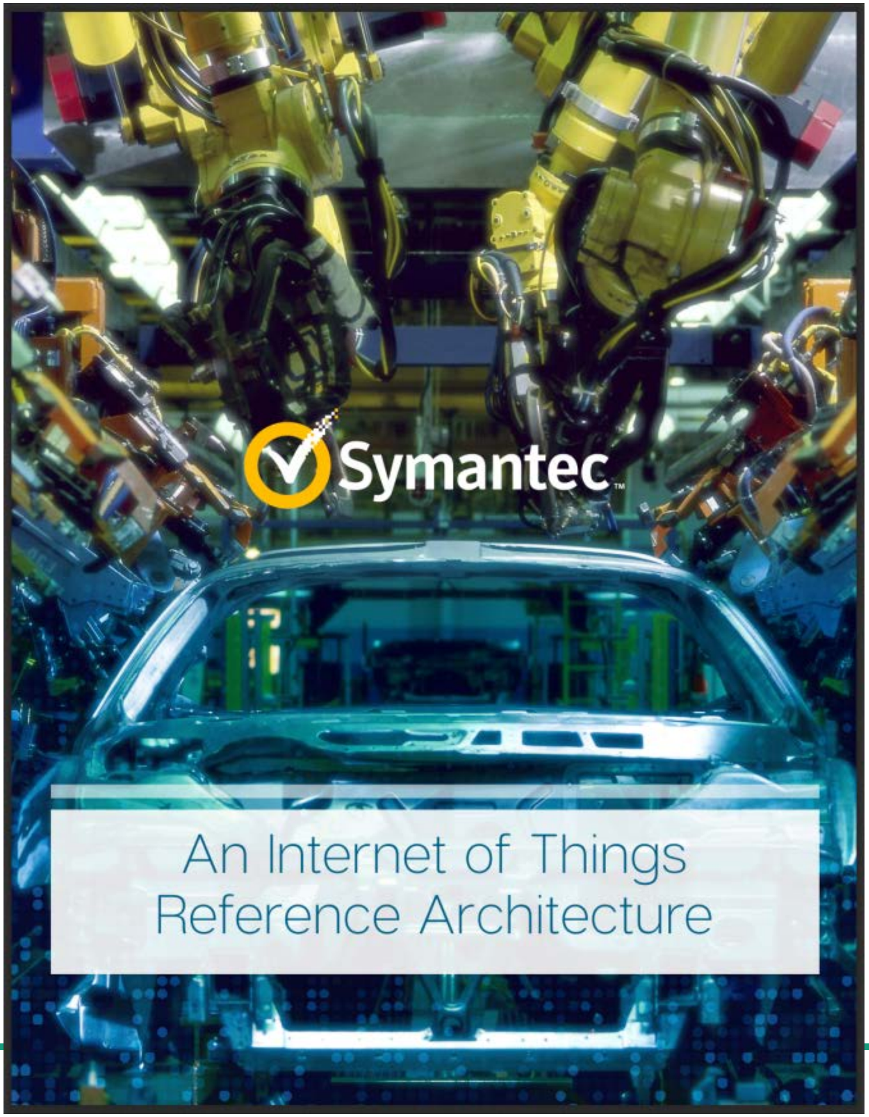
- Built-In Security
- Security built into the device at manufacturing time

Summary

- Information Security -> Safety
- Cyber Security Framework Adoption
- Risk Management Maturity
- Threat Landscape – More Bad things
- Controls, Countermeasures, Frameworks
- New Approach/Technology required
- Transferring Risk?

Q&A

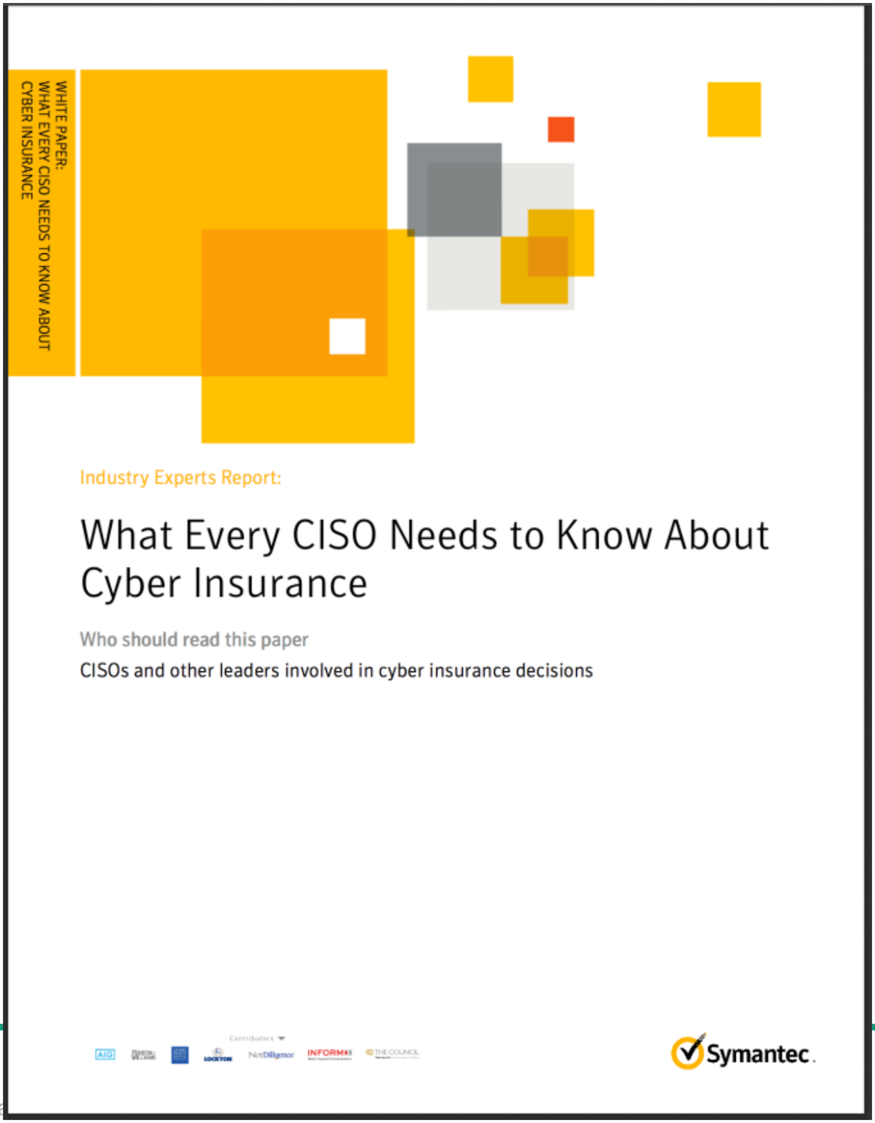
http://www.symantec.com/iot/



Symantec

An Internet of Things
Reference Architecture

http://www.symantec.com/cyber-insurance/



WHITE PAPER:
WHAT EVERY CISO NEEDS TO KNOW ABOUT
CYBER INSURANCE

Industry Experts Report:

What Every CISO Needs to Know About Cyber Insurance

Who should read this paper

CISOs and other leaders involved in cyber insurance decisions

Contributors

Symantec.

Hogan
Lovells

Liability risks industry 4.0

Dr. Sebastian Lach, Partner, Munich

Industry 4.0 - Risks

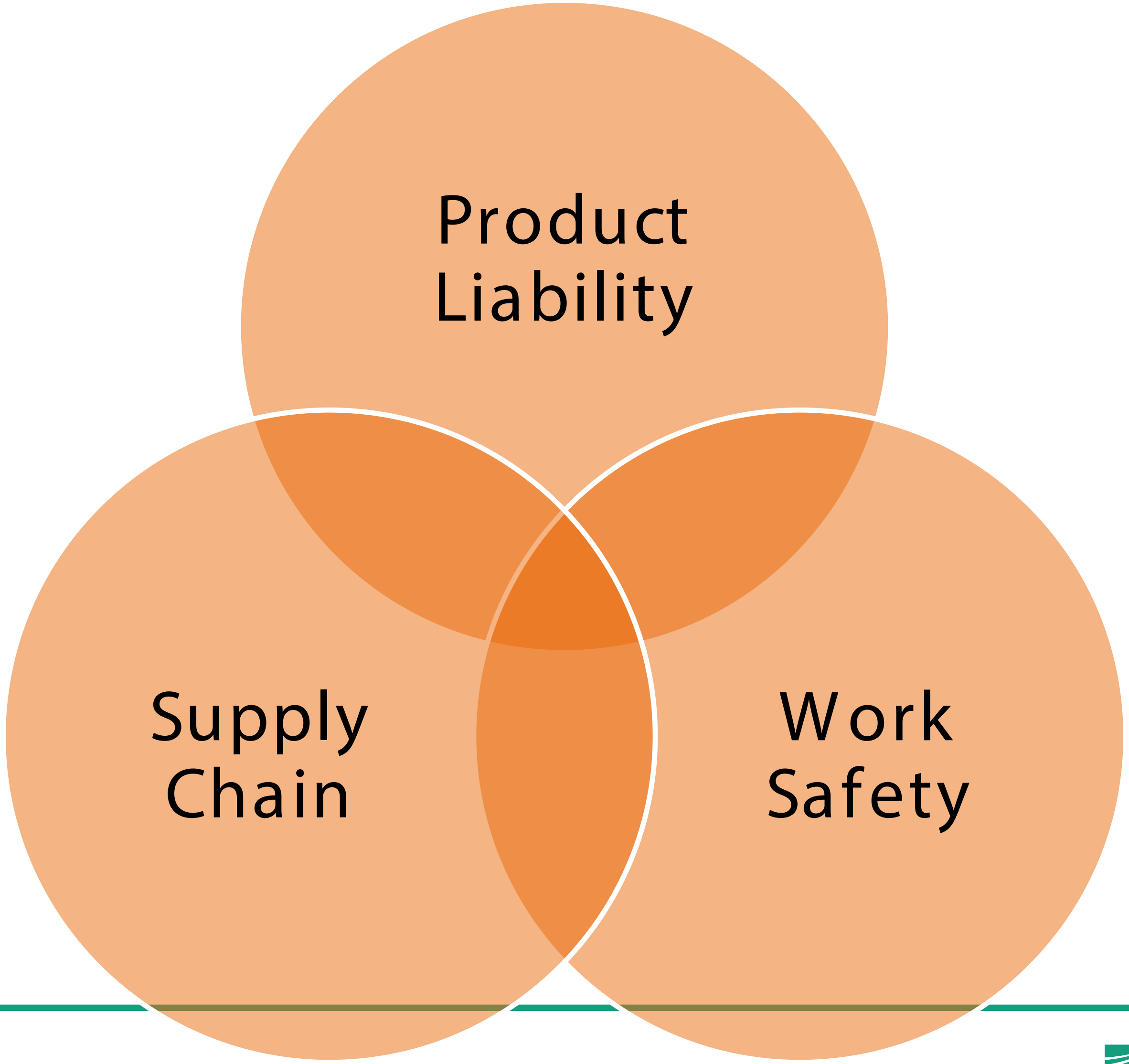
Software as new "tool" introduces new technical and legal risks

Interconnection of processes and companies can lead to new liability dimensions

Unique new issues like cyber breaches

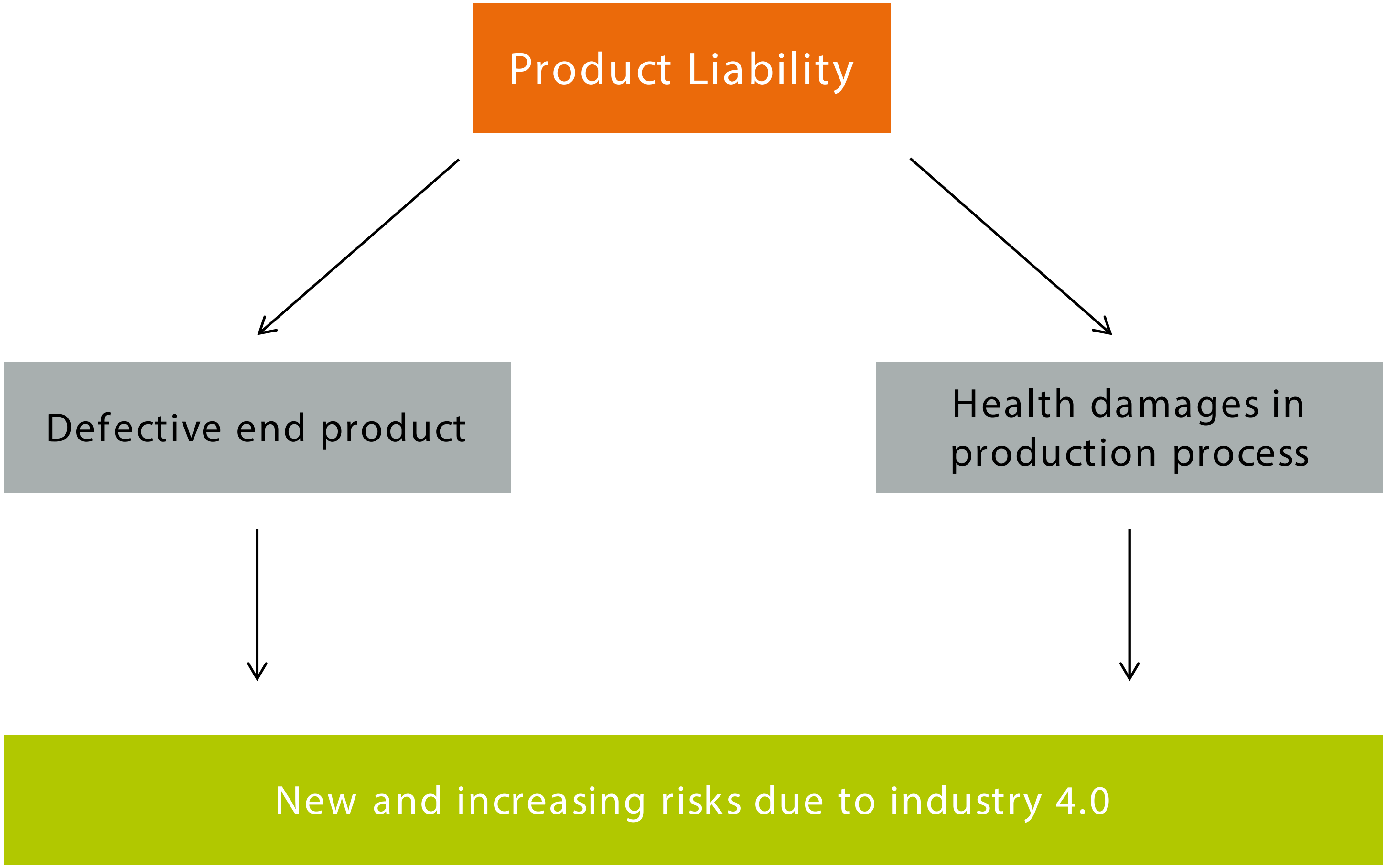
➢ Legal regimes to address risks already exist, but new issues and questions to be answered

Main legal fields of liability risks for industry 4.0



Product Liability

Scenarios – Not only consumer safety!



Product Liability

Defective end product

Health damages in production process

New and increasing risks due to industry 4.0

"Software" vs. "Product"

Product Liability Directive (85/374/EWG)

> *"For the purpose of this Directive 'product' means all movables […], even though incorporated into another movable or into an immovable […]. 'Product' includes electricity."*

Product Safety Directive (2001/95/EG)

> *"Product" shall mean any product - including in the context of providing a service […]."*

Em

hard disk) are "products" in general

Possibilities to address liability risks

Separate delivery of the product and the software

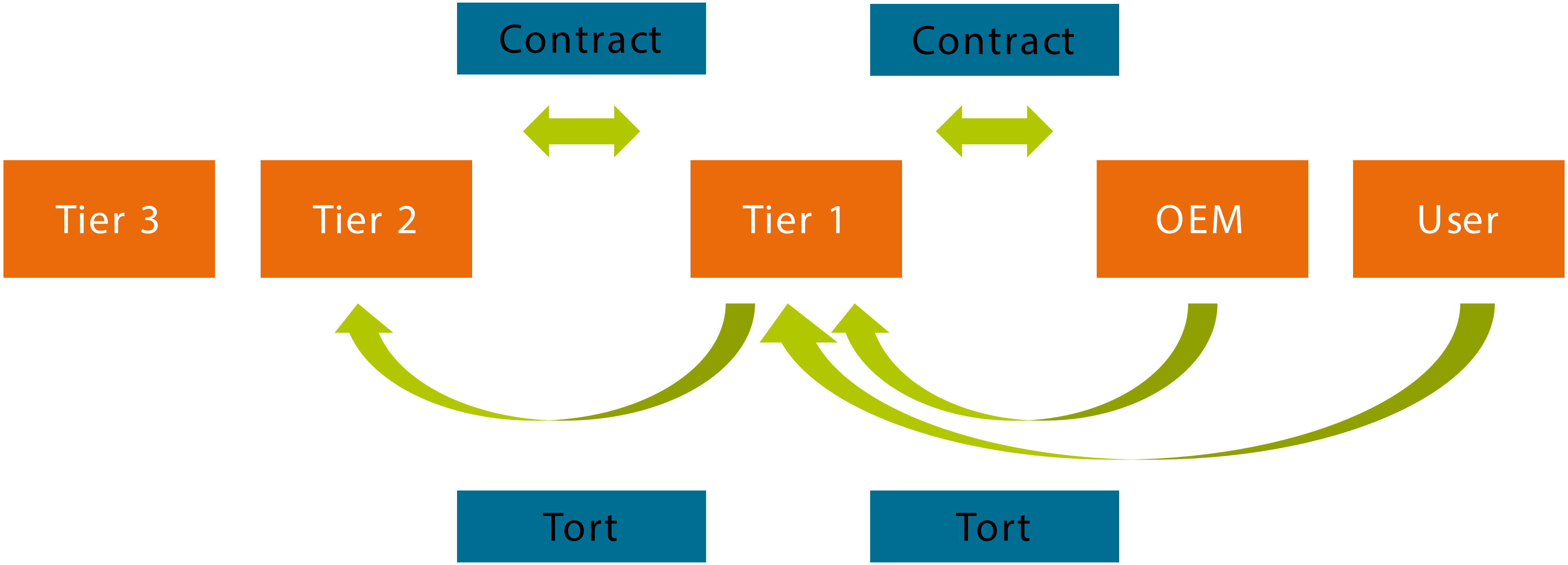
Download/stream the software

- A simple download/stream is probably no product
- But warranty rights under purchase or service contract etc.

Licensing of the software only/retain ownerships of products

Supply Chain

Allocation of risks in the supply chain



Before we start – How are contracts made?

What is communication between machines?

- Mere technical exchange or legally relevant communication?

If legally relevant communication

- Is machine messenger ("Bote") of the principal?
- Is machine agent/representative ("Vertreter") of the principal?

➢ Distinction relevant for contractual side and liability

Possibilities to address liability risks

Separate delivery of the product and the software

Download/stream the software

Licensing of the software only/retain ownerships of products

Carefully draft contracts

- Clear product description (instead of liability limitation/T&C!)
- Clear allocation of responsibilities, in particular in case of connection through or combination with software
- Clear allocation of burden of proof
- Clear provisions on inspection of incoming and out-going goods (Sec. 377 HGB)
- Applicable law and arbitration clauses

Cyber Breaches

Risk from cyber breaches (1/2)

What is a state of the art breach defense system ("Defect)?

Updates

How quickly and for how long will systems have to be updated (patches)?

Instructions

What instructions are needed for the user?

Breaches will occur!

From the outside

When is a cyber breach an inevitable attack from the outside, when is it an inacceptable weakness of the system?

From the inside

What changes if the attack comes from the inside of the company ("rogue employees")?

Fiat/Chrysler issue first major case that led to recall after cyber breach

Risk from cyber breaches (2/2)

Some potential follow on steps:

1 Review cyber security systems/separation of data from connection

2 Seek political clarification for notion of defect from law makers and through industry standards

3 Establish system for updates (+ allow access) and mirror in sales contracts

4 Check need and right of monitoring for non-updaters

5 Quick action force for cyber-breaches (notification requirements)

6 Review product instructions in this regard and clarify internal access to systems/data and safeguards

Work Safety

Work safety and industry 4.0

Work safety related risks can be triggered by various factors

- Breaches
- Bugs
- " Miscommunication" /Interruption/Incompatibility
- Development Risks

➢ High focus on topic by authorities with significant risks for individuals and company

The "Thyssen Krupp" case (1/2)

Accident in Turin plant (Dec 2007)

Death of 7 workers due to severe burns

- Alleged violation of health and safety standards

Criminal Court in Turin, 15 April 2011:

- 16.5 years imprisonment for ThyssenKrupp's director in Italy
  - Guilty of voluntary manslaughter
- 10 – 13 years imprisonment for other managers
- Company: EUR 1 million fine; EUR 21 million damages; Legal costs
- Prohibition from advertising products in Italy

Court of Appeals in Turin reduced sanctions, 28 February 2013:

- 10 and 7 - 9 years
- Negligent homicide instead of voluntary manslaughter

The "Thyssen Krupp" case (2/2)

Supreme Cassation Court, 24 April 2014:

- Annulled sanctions but referred case back to Court of Appeals to recalculate sentences

Court of Appeals in Turin, 29 May 2015:

- Reduced sentences of all six Defendants:
  - 9 years and 8 months for director
  - From 6 years and 8 months to 7 years and 6 months for the other five managers

The Yates Memorandum (1/2)

Department of Justice announces guidance on pursuing managers in investigations against companies (9 September 2015):

- Investigations can be conducted against managers and employees, who could face criminal prosecution and lengthy prison sentences
- Companies being investigated are obliged to disclose all relevant facts about their own employees in order to demonstrate sufficient cooperation with the authorities

The Yates Memorandum (2/2)

Relevance for companies:

- Effects on internal investigations
  - Employees could be hesitant to take part in interviews
  - Tolling agreements " should be the rare exception"
- Disruption of day-to-day business
- Additional costs for the company

" *One of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing.*"

Sally Yates, Deputy Attorney General

Criminal liability of individuals

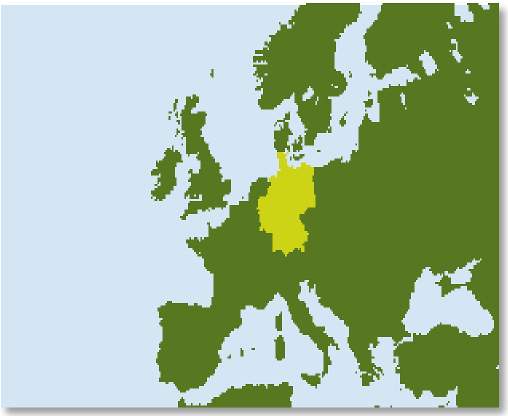
- Increasing exposure to criminal liability
- Trend to severe sanctions
- Example for Germany
  - Provisions on causing bodily harm in the criminal code (" StGB") can address product safety issues that lead to health damage
  - Sec. 130, 30 OWiG can address corporate fines
  - Fraud provisions (sec. 263 StGB) can address safety and non-safety issue and currently represent the most crucial risk

➢ Personal criminal liability one of major worries of senior executives

Civil liability of individuals

Contract law liability

- Towards company
- For breaches of duty
- Responsibility



Corporate law liability

- Towards company
- Sec. 93 of the German Stock Corporation Act (AktG)
- Sec. 43 of the German Limited Liability Companies Act (GmbHG)
- For violation of the legal responsibility of care (e.g. taking unnecessary liability risks)

Establish robust product compliance system

Robust global complia ss with written guidelines

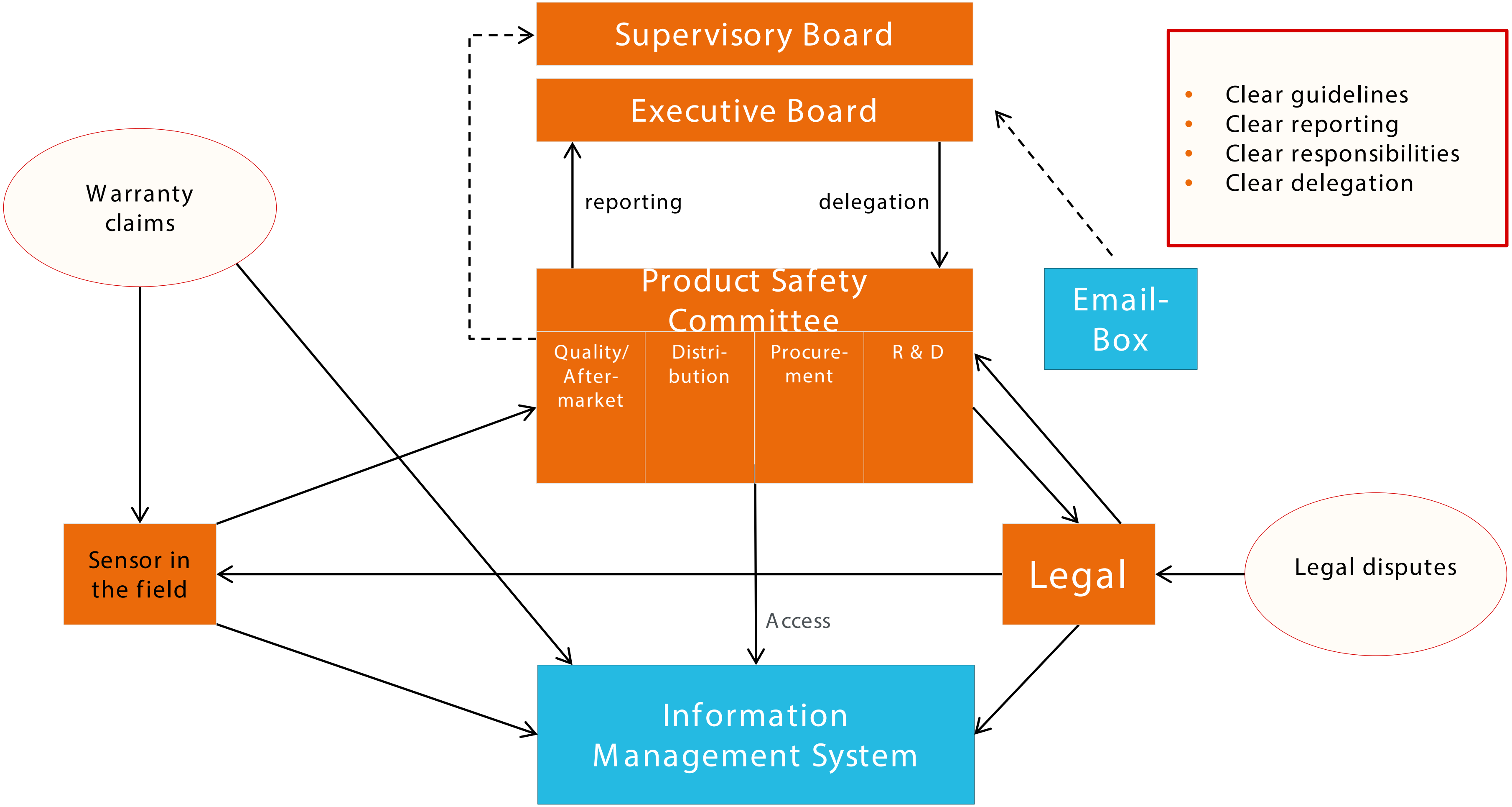
Structure of compliance surveillance (compliance department, internal auditing) with spot test

Codes of conduct that establish clear rules for employees for design, manufacture, product information and product monitoring

Regular compliance education/training for employees

Specific assessment of possible health risks and their avoidance (e. g. HSE system, workers protection)

Example of robust product safety system



- Clear guidelines
- Clear reporting
- Clear responsibilities
- Clear delegation

Summary

Summary

Industry 4.0 raises new legal questions and introduces new risks

Innovation speed will increase which might make risk management harder to handle

Regulators and public are more aggressive in their approach

Data will lead to new risks (cyber breach) and will make infractions traceable (storage of information)

- ➢ Companies are looking for answers for company and individual liability to feel comfortable about taking the risks of a faster and globalized world

Liability risks industry 4.0

Dr. Sebastian Lach, Partner, Munich