Federal Institute for Occupational Safety and Health

Safety verification of digitally networked machinery and plants in the context of Industry 4.0

Dipl.-Ing. **Björn Kasper**
Dr.-Ing. **Stefan Voss**
Federal Institute for Occupational Safety and Health,
Unit Workplaces, Safety of Machinery, Operational Safety, Dresden, Germany

6th EUROSHNET Conference, 12 - 14 June 2019

Characteristics of „digitalization“

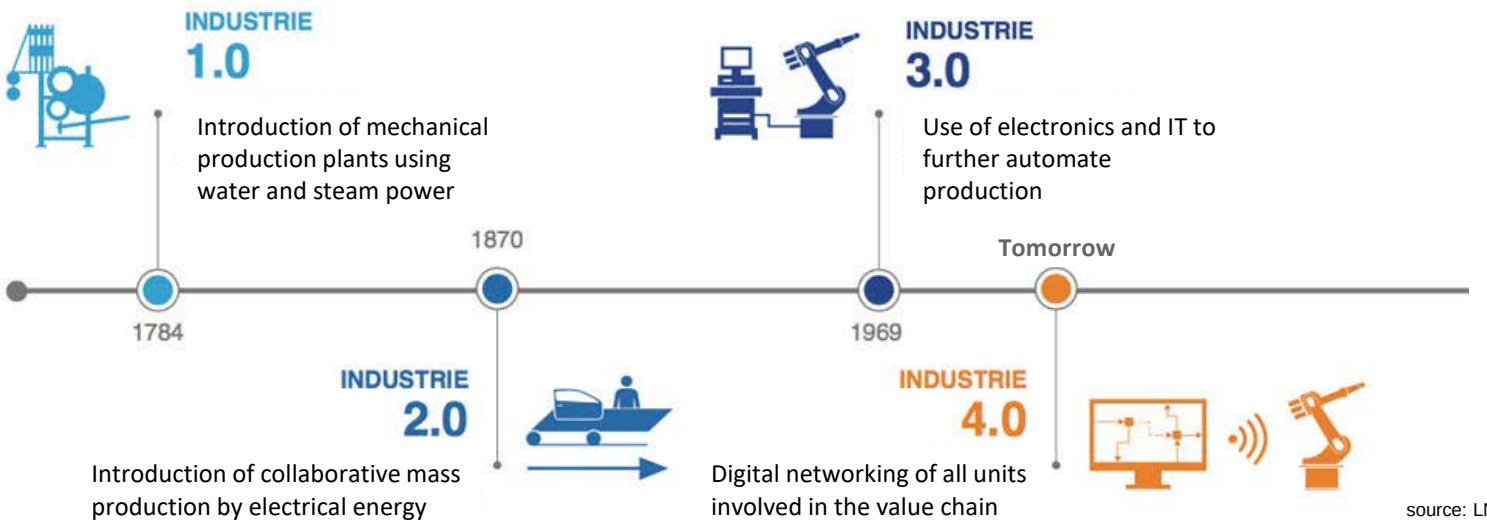
source: VDMA Forum Industry 4.0

- Integrated automation of complete value chains
- Accompanying production data over the entire product life cycle
- Interaction of natural science, engineering, social science and humanities and their scientific methods

⇒ **Complexity ⇑ + Transparency/Traceability for employees/users ⇓**

baua:

Industry 4.0 in manufacturing and production technology

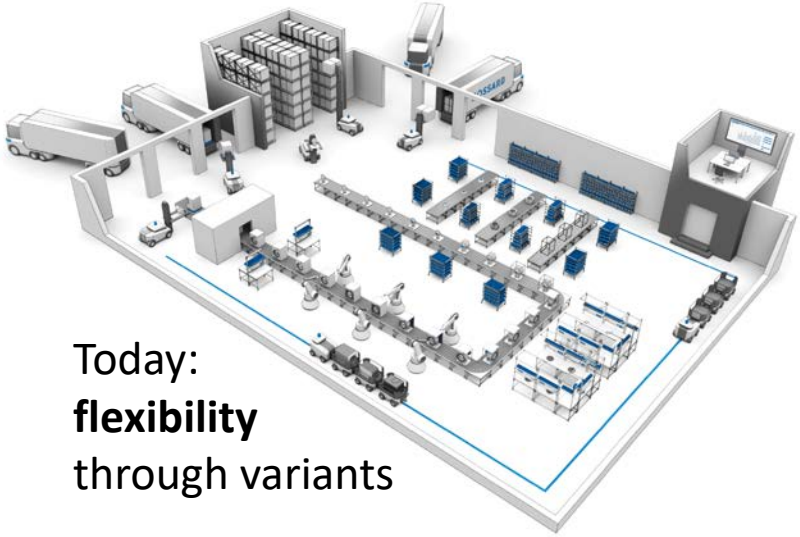


source: LNI 4.0

Industry 4.0

- Introduced as part of the German government's high-tech strategy in 2011
- Digital networking in manufacturing and production technology
- Central challenges in the industry
  - Flexibility,
  - Quality and efficiency increase,
  - Time-to-market reduction
- Many industrial nations have similar ambitions (e.g. smart manufacturing, connected industries)

Industry 4.0 in manufacturing and production technology



Today:
flexibility
through variants

source: Bossard Smart Factory Logistics

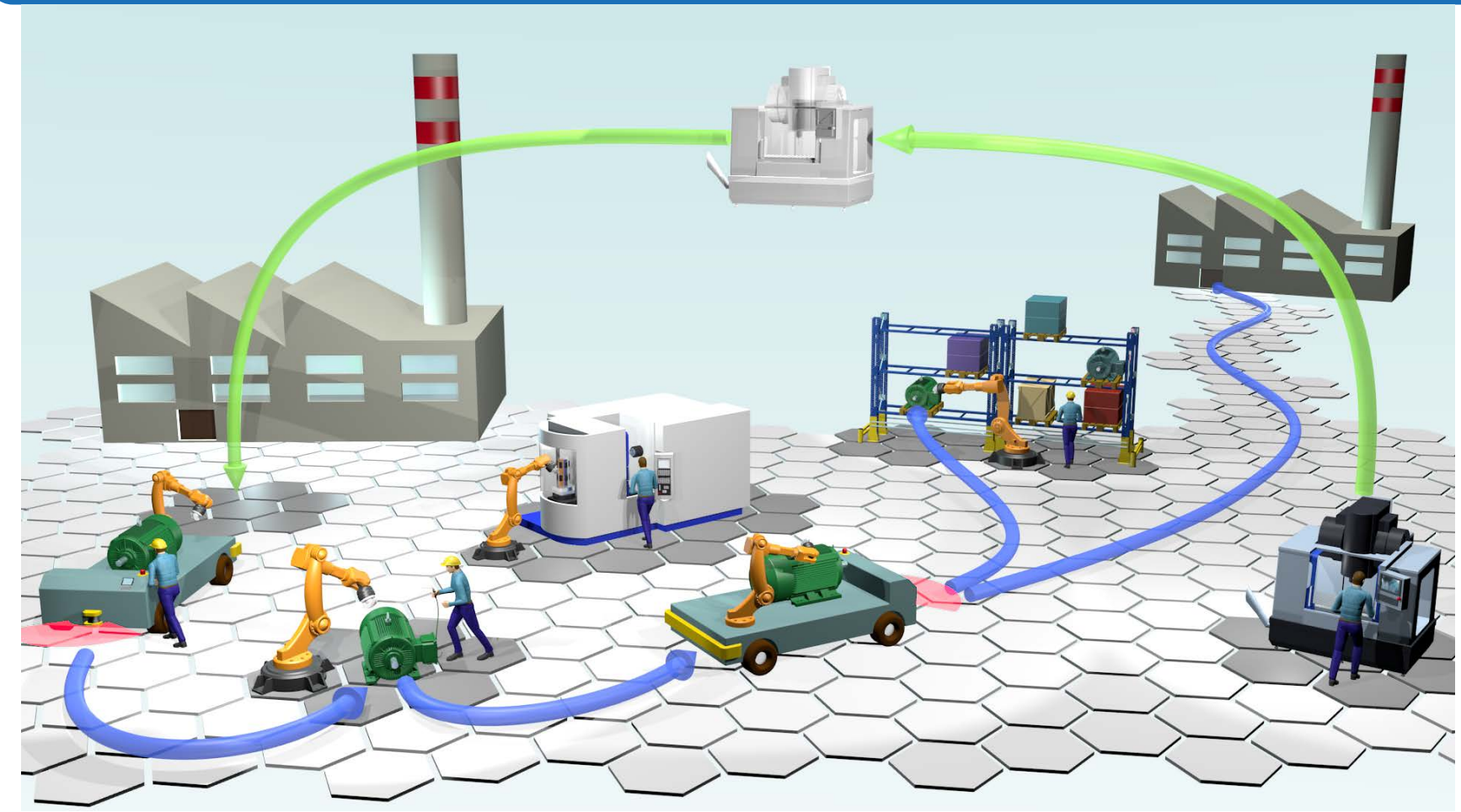
source Kasper, license: CC BY-SA 4.0

Tomorrow: **versatility** through modularization

Radio-based **networking**

Industry 4.0: modular, intelligent, digitally networked cyber-physical systems combined with dynamic recombinability / versatility

Industry 4.0: versatility through modularization



Blue: **Modularization** of production by e.g. networked production islands
Green: **Versatility** of production: product controls manufacturing process

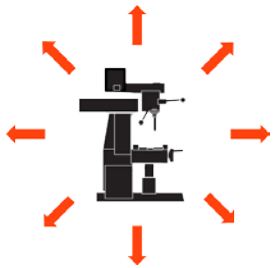
Industry 4.0 in manufacturing and production technology

Safety technology:

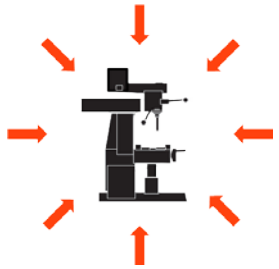
technical & organizational measures to achieve machinery safety

Distinction of 2 aspects:

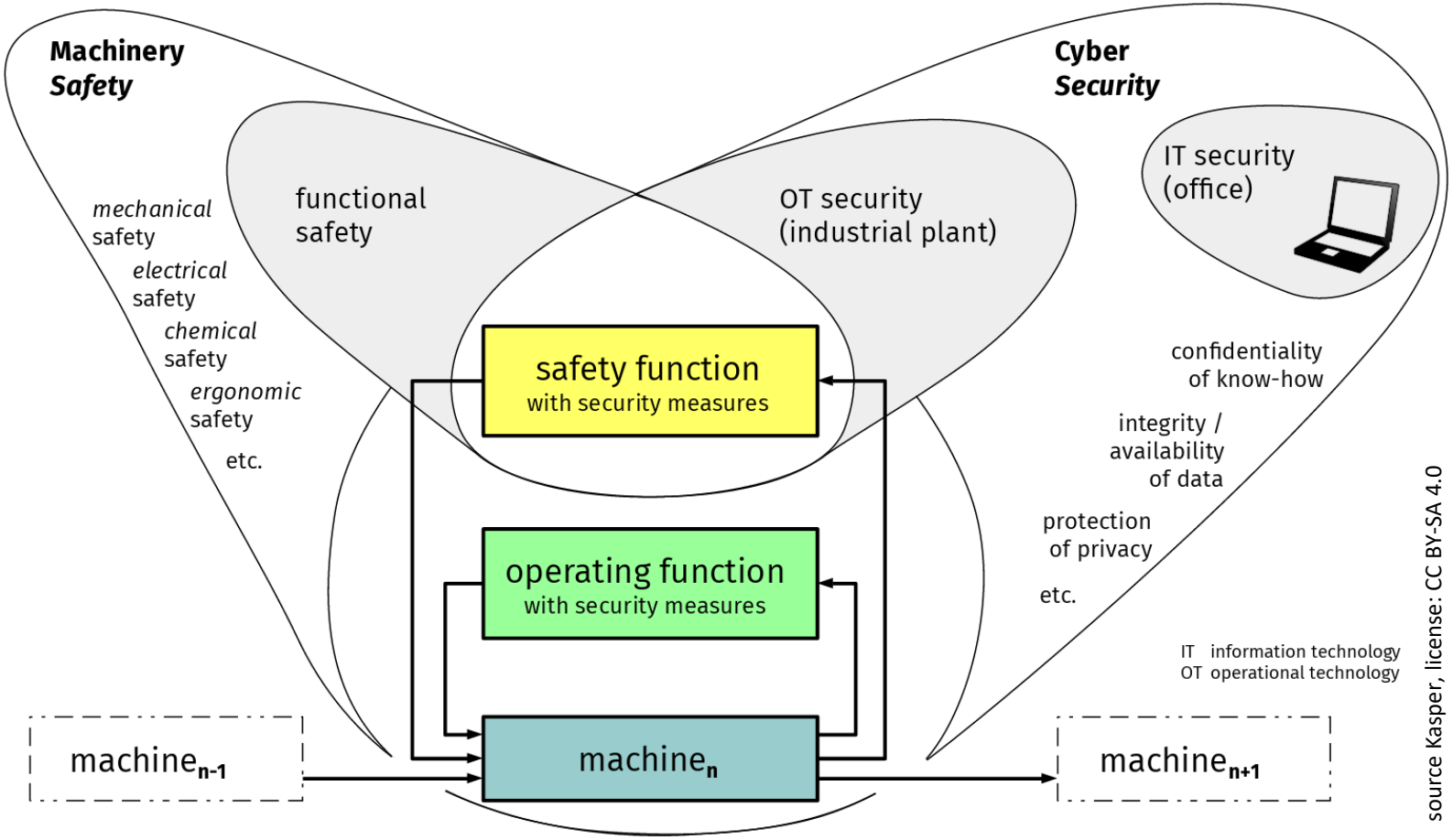
- Product / operational safety: ***„Safety“***



- Attack / manipulation security: ***„Security“***



Industry 4.0 in manufacturing and production technology



Operational and safety functions of machines and plants

Goal: Establish risk assessment as a combined process!

Industry 4.0 in manufacturing and production technology

Industry 4.0: intelligent, real-time capable, digitally networked cyber-physical systems combined with dynamic recombinability / versatility

Goal:

It is the task of the machinery safety to ensure
the functional safety with the inclusion of the
industrial security (OT).

Safety & Security

These can influence each other:

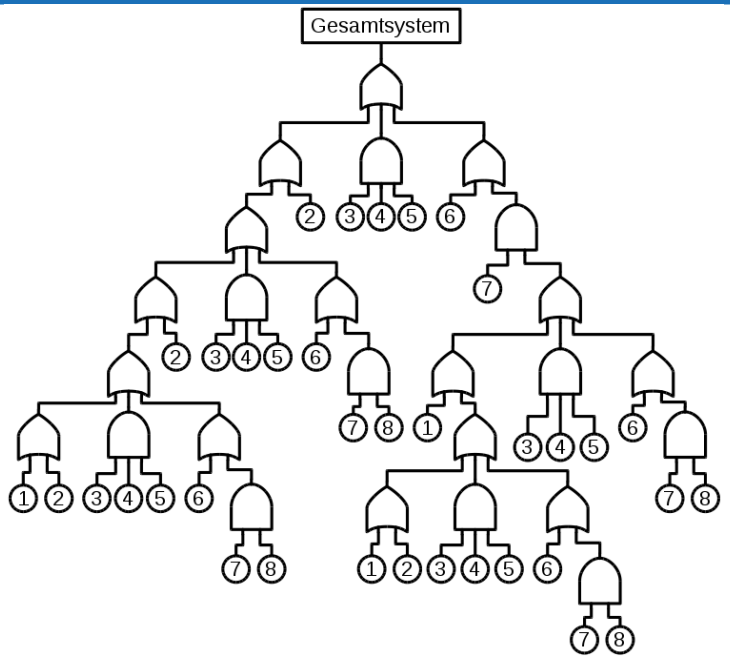
from security-related events risks for safety can emerge
(so-called *„safety related security aspects“*)

⇒ **Establish risk assessment as a combined process!**

Safety verification: today

1. Defining the physical and temporal limits of the machine
2. Identification of hazards, risk assessment and valuation
3. Assessment of the risk for each identified hazard and hazardous situation
4. Assess risk and set risk mitigation decisions
5. Elimination of hazards or reduction of the risk associated with the hazard by the method:
   - inherently safe construction
   - technical protective measures
   - user information

General principles according to ISO 12100

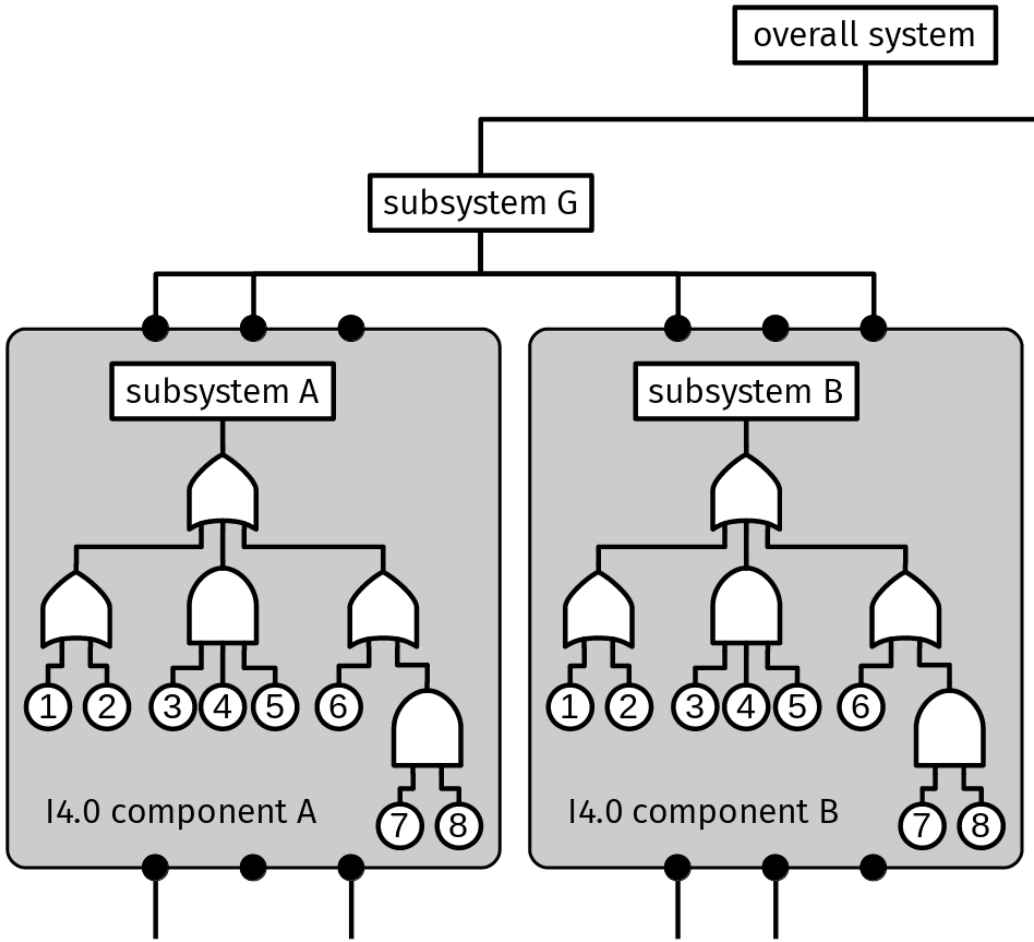


source Kasper, license: CC BY-SA 4.0

- Validation via the description of deterministic states
- Central (manual) validation methods (here: FTA) during system design and before machine acceptance

⇒ Reactions to changes to Runtime are **not** possible

Safety verification in context of Industry 4.0



safety function
supported by
machine learning?

operating function D
supported by
machine learning

Goal:
Appropriate risk assessmentand validation of safety functions of intelligent, real-time capable, networked and versatile machines and plants at runtime

baua:

Industry 4.0 in manufacturing and production technology

Goal:
Appropriate risk assessmentand validation of safety functions of intelligent, real-time capable, networked and versatile machines and plants at runtime

Recombinability / versatility
number of variants ***n*** = 1

Assumption:
Deterministic conditions in manufacturing and production technology remain.

Need for action:
Safety verification can be carried out using existing methods during system design (construction, commissioning).

Recombinability / versatility
number of variants ***n*** = few

Assumption:
Flexible manufacturing systems combined with a small number ***n*** of variations

Need for action:
Safety verification can be carried out using existing methods combined with increased effort.

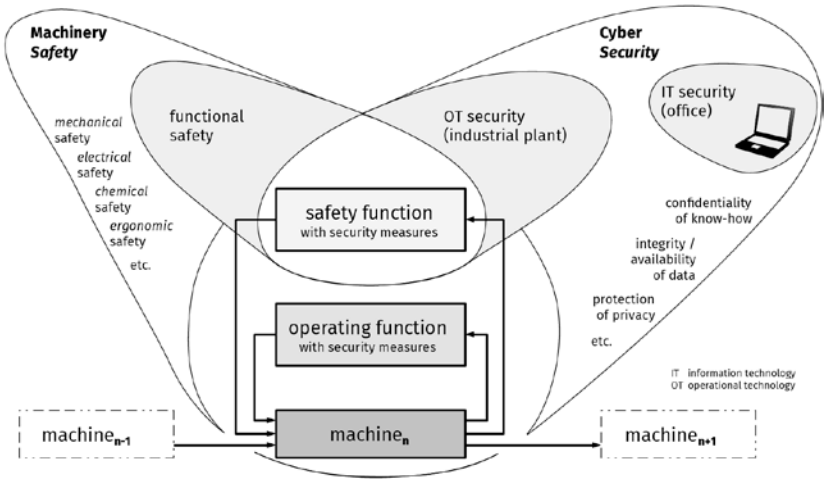
Recombinability / versatility
number of variants ***n*** = many

Assumption:
Recombinable / versatile manufacturing and production systems (without predictable sequence of deterministic states), combined with a high number n of possible variations

Need for action:
Safety evidence can not be carried out using existing methods according to current standards. A possible approach is a proof of probabilistic considerations supplemented by elements of *machine learning*.

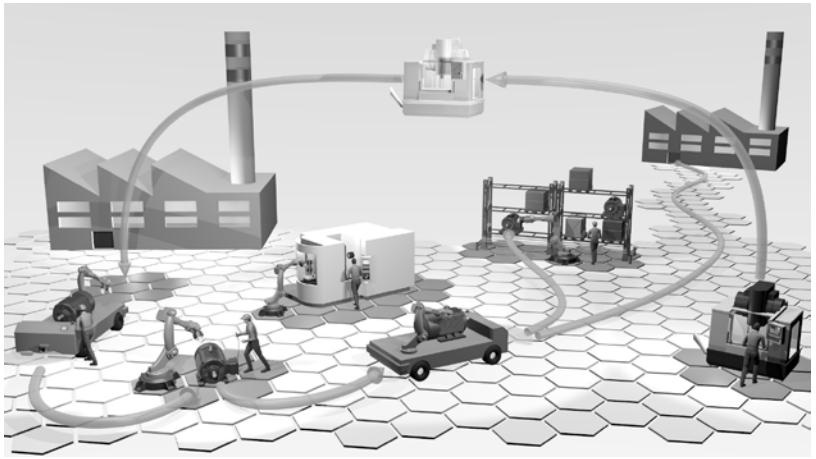
Summary

- Safety technology of innovative technologies in the context of Industry 4.0
- Industry 4.0: modular, intelligent, digitally networked cyber-physical systems combined with dynamic recombinability / versatility



Relevant questions

- Machinery safety: functional safety has to involve industrial security (OT)
- Appropriate risk assessment and validation of safety functions of intelligent, networked and versatile machines and plants at runtime

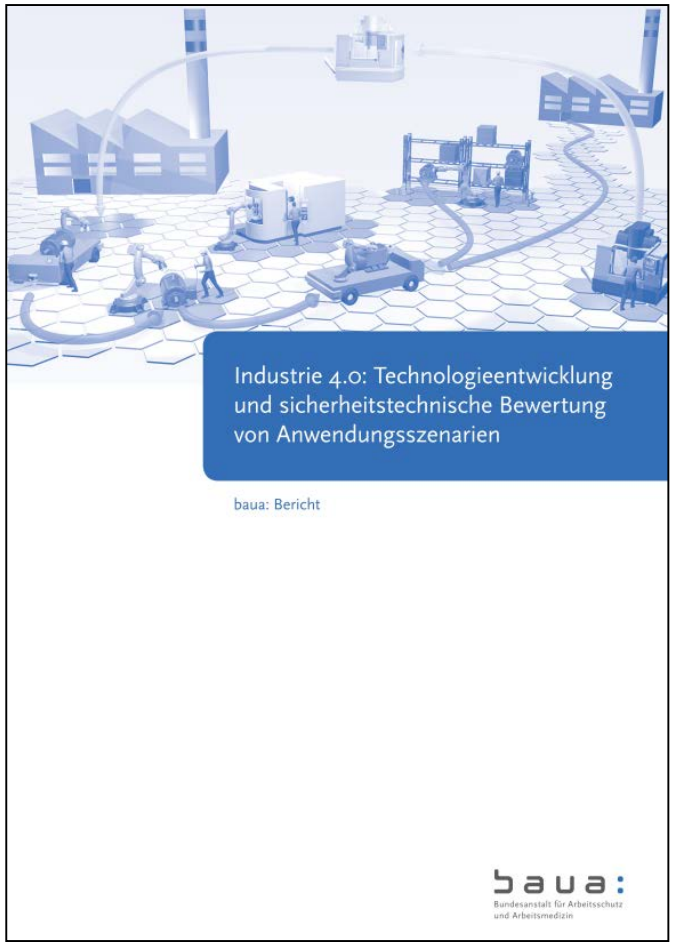


baua:

Additional information

- B. Kasper. 2019. Industrie 4.0: Technologie-entwicklung und sicherheitstechnische Bewertung von Anwendungsszenarien. 1. Auflage. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin 2019. DOI: https://doi.org/10.21934/baua:bericht20190204

- B. Kasper und S. Voss. Neue Anforderungen an die Sicherheitsnachweisführung von Maschinen und Anlagen im Kontext von Industrie 4.0, sicher ist sicher, 09.18, 368-371, 2018 https://www.baua.de/DE/Angebote/Publikationen/Aufsaetze/artikel2093.html



Thank you for your kind attention

contact: Björn Kasper and Dr. Stefan Voss
Federal Institute for Occupational Safety and Health
kasper.bjoern@baua.bund.de
voss.stefan@baua.bund.de

BACKUP

source: Wikipedia; 05.07.2018

Schwerpunktprogramm „Sicherheit und Gesundheit in der digitalen Arbeitswelt“

IM FOKUS: DIGITALE ARBEIT

Programmziele und -struktur

Übergreifende Programm-komponenten

Monitoring der digitalen Arbeitswelt

Erfassung / Bewertung

Tätigkeitscluster

Objektbezogene Tätigkeiten

Informations-bezogene Tätigkeiten

Personen-bezogene Tätigkeiten

Führung und Management

Ist-Stand und aktuelles Gestaltungswissen / zukunftsgerichtete Leitbilder / Handlungsbedarfe

Technischer und organisatorischer Arbeitsschutz

Herausforderungen / Zielvision / Anpassungsbedarfe

- Stand: Programmgruppentreffen 12.02.2019

Industry 4.0 in manufacturing and production technology

Industry 4.0: modular, intelligent, digitally networked cyber-physical systems combined with dynamic recombinability / versatility

Safety & Security

e.g. Use of industrial field buses

- Open (wireless / 5G) standard networks: (e.g. PROFIsafe based on PROFINET, Modbus/TCP, Ethernet/IP)
- Real-time capability (especially in star-shaped radio topologies)?
- Security?
- Safety monitoring clock cycles?
- Present security strategies (network separation / packet filtering / access authorisations) applicable?

Wireless communication of distributed control systems

Requirements of Industry 4.0

- versatile, mobile production islands ⇒ wireless networked control systems
- distributed control systems ⇒ safety related real-time communication

As of today:

- industrial use of non-real-time radio protocols (e.g., WLAN IEEE 802.11.x)
- guaranteed real-time cycle can only be achieved via massive oversizing (e.g., bandwidth) and very small data packet lengths for small latencies ⇒ in industrial RT* fieldbus protocols (e.g. PROFINET IO, Ethernet Powerlink), **cycle times** are currently reachable with a minimum of **approx. 8 - 10 ms**

- **Safety:**
  - extension of the fieldbus protocols necessary
  - transmission takes place in safety channel (so-called "Black Channel" principle) on non-safe standard communication channel (e.g. Ethernet)
- **Security:**
  - encryption in the radio protocol (e.g. WLAN with WPA2)
  - in real-time fieldbuses today no normative security measures (for example authentication, authorization, encryption) are provided

RT .. Real time

Wireless communication of distributed control systems

Requirements of Industry 4.0

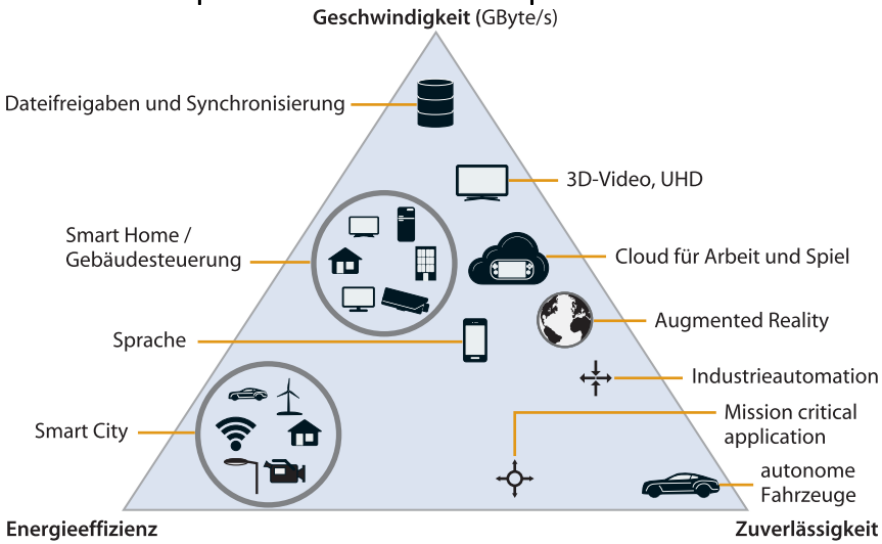
- versatile, mobile production islands ⇒ wireless networked control systems
- distributed control systems ⇒ safety related real-time communication

Outlook 5G:

- end of 2017 first standard for the new mobile generation "5G" published by 3GPP
- “Non-Stand-Alone Operation” (NSA) ⇒ LTE network required as backbone
- “Standalone operation” (SA) since 06/2018 ⇒ autonomous island operation of individual production sites possible

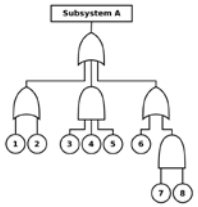
- significant improvement for **hard real-time** requirements:
  - shorter latency ⇒ more reliable real-time data transmission
  - better prioritization of time-critical data packets (including overtaking) ⇒ **Cycle times** down to **0.5 ms** possible

- **Beamforming:**
  - spatially targeted transmission / reception of radio beams
  - network-side positioning possible in the decimeter range ⇒ indoor navigation for driverless transport systems without GPS possible

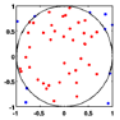


Hoymann und Meyer. 2018. Vielfachfunk - Was die fünfte Mobilfunkgeneration besser macht als LTE. In: c’t 2018, Heft 20, S 178 ff

Possible methods for future risk assessments

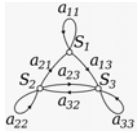


- Changes in the system architecture
  ⇒ **Dynamic Fault Trees DFT**

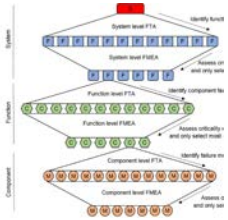


- Modeling the system dynamics

  ⇒ Evaluation of **FTAs using Monte Carlo**



  ⇒ Implementation of **stochastic processes** (e.g. Markov processes) in **FTAs**



- Acquisition structurally complex systems

  ⇒ **recursive FMEA and FTA***

Consideration of Industry 4.0 sub-aspects

Addressing of all 3 types of complexity possible?

⇒ **machine learning methods**

*Peeters, J. F. W. et al., Reliability Engineering & System Safety, **2018**

baua:

Requirements for new methods

Industry 4.0: increasing system complexity ⇒ Adaptation risk assessment*

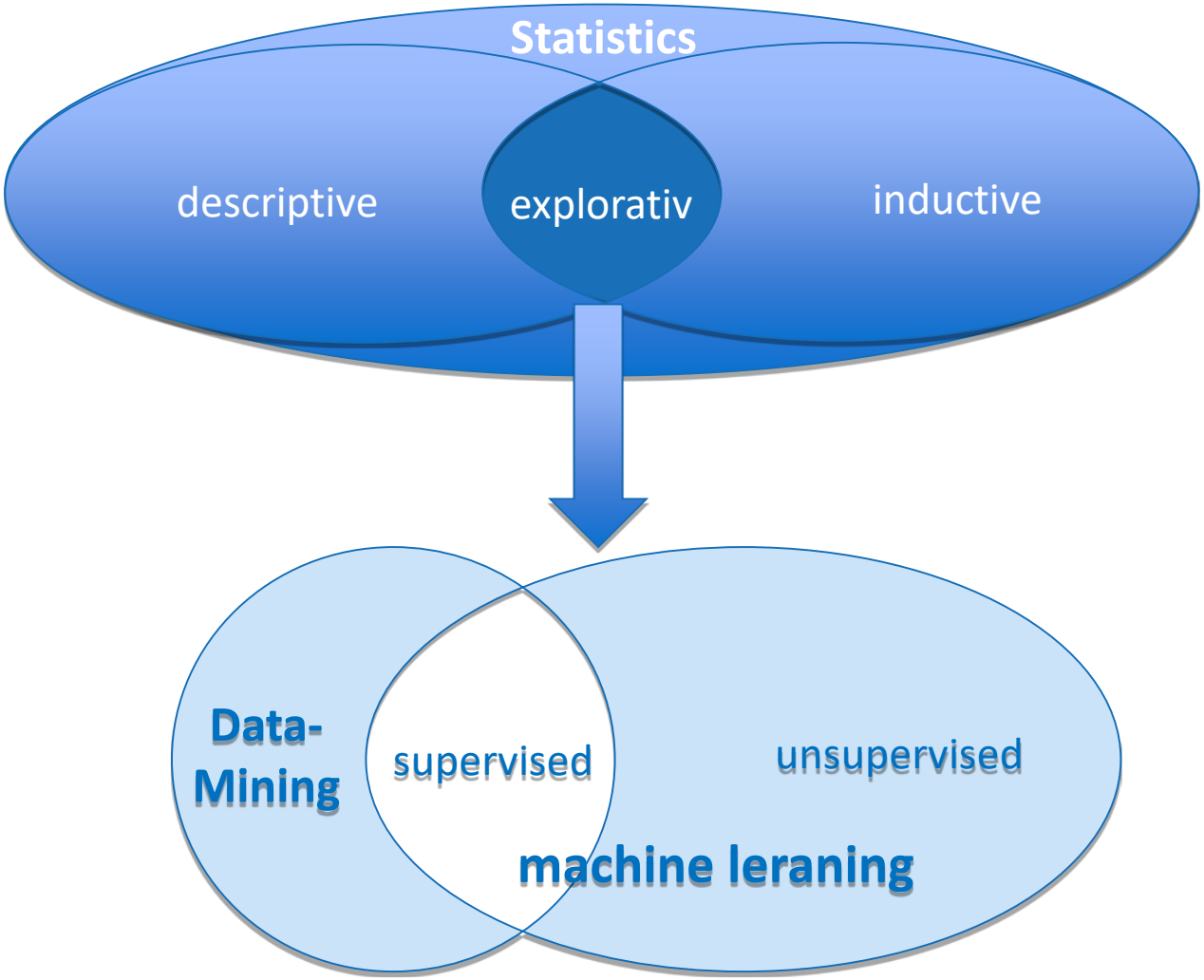
Complexity type	Source
structurally	heterogeneity
	interoperability
	networking
	Software-Intensity
	Human in the loop
dynamically	Time-dependent developments
	Dynamic reconfiguration
	Autonomous decisions
organizational	Complexity of the development and operation team - interdisciplinarity

* V. Bolbot et al., Reliability Engineering and System Safety, **2018**

Machine Learning methods: A Selection

Method	Task / Goal
K-Nearest Neighbor	Classification
Naive Bayes	Classification
Decision Trees	Classification
Classification Rule Learners	Classification
Linear Regression	Numerical prediction
Regression Trees	Numerical prediction
Model Trees	Numerical prediction
Art. Neural Networks	Combined use
Support Vector Machines	Combined use
Association Rules	Pattern recognition
k-means Clustering	Clustering / Grouping

Classification of machine learning methods



Terms: Safety funktions and realtime

The term ***real time*** characterizes the operation of information technology systems that can deliver certain results reliably within a predetermined period of time, for example in a fixed time grid.

The definition of DIN 44300 (Information Processing), Part 9 (Processing Procedures), which has been replaced in the meantime by DIN ISO / IEC 2382, was as follows:

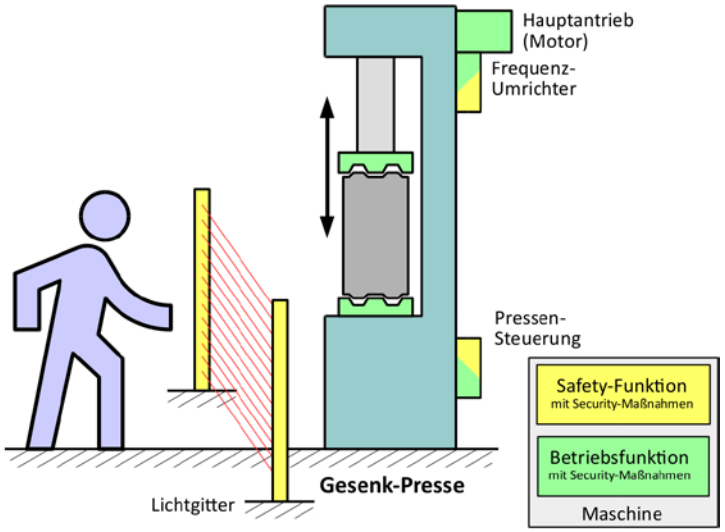
> *"Real-time means the operation of a computing system in which data processing programs are always operational, such that the processing results are available within a given period of time. Depending on the application, the data may be generated randomly or at predetermined times."*

The hardware and software must ensure that there are no delays that could prevent compliance with this condition. The processing of the data does not have to be very fast, it just has to be done fast enough for the respective application.

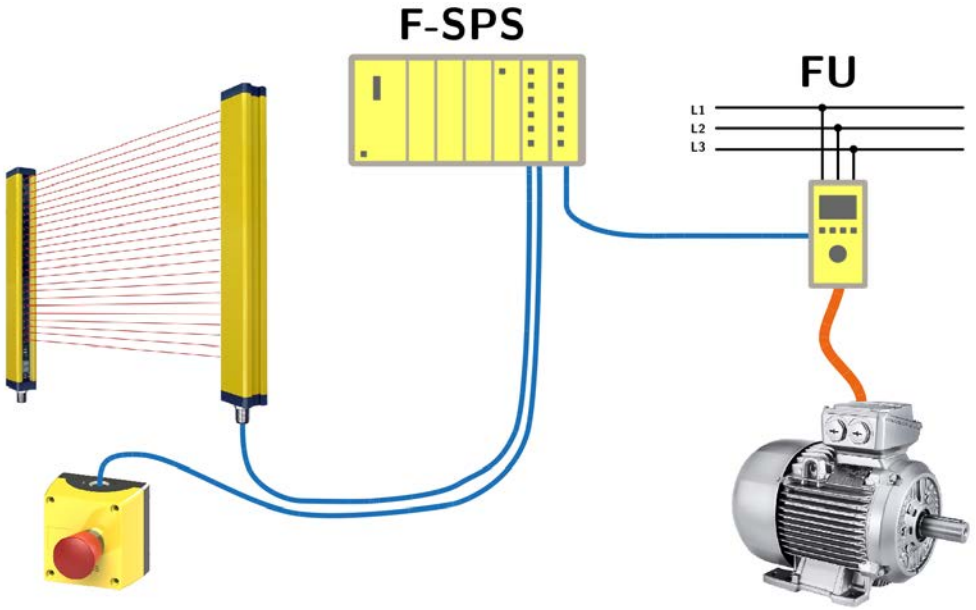
source: Wikipedia; 05.07.2018

Industry 4.0 in manufacturing and production technology

Safety function "Safe operating stop (SOS)" according to EN 61800-5-2



source Kasper, license: CC BY-SA 4.0



source Kasper, license: CC BY-SA 4.0

baua:

Introduction - Digitization

Driver of dynamics:
technological development

Influence on the socio-technical system

source: A. Tisch, BAuA, 2018

Current technical innovations

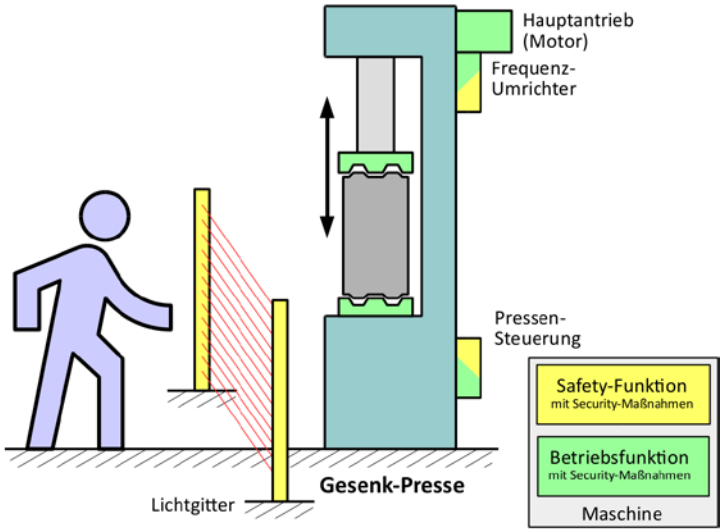
- Intelligent automation; e.g. cyber physical systems
- Mass dissemination of new technologies; e.g. data glasses
- Real-time networking, e.g. Smart factory
- Platforms and big data, e.g. Smart Services

Change of the working world

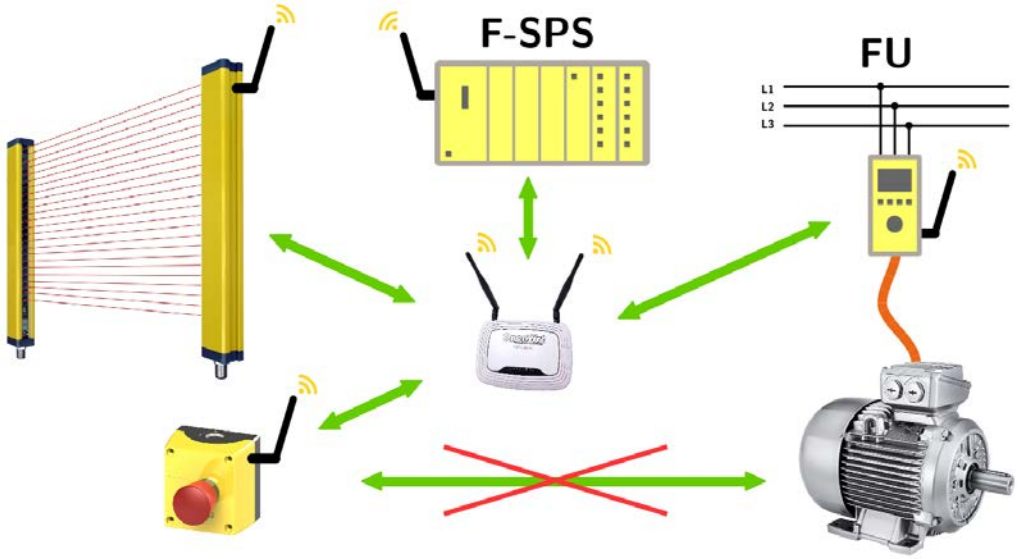
- Social change, e.g. Individualization of work
- Increase in the diversity and variety of the workforce
- Globalization, e.g. Increase in competition
- Change in organizations and forms of work and their impact on employees

Industry 4.0 in manufacturing and production technology

Safety function "Safe operating stop (SOS)" according to EN 61800-5-2



source Kasper, license: CC BY-SA 4.0



source Kasper, license: CC BY-SA 4.0

baua: