Choose certainty.
Add value.

TÜV SÜD Digital Service CoE Singapore
Safe and Secure Migration to Industry 4.0

Eley Querner
Senior Vice President,
TÜV SÜD Digital Service CoE
23 June 2016

Industry 4.0 – Why it happens?

Pic Ref: McKinsey and Company

Industry 4.0 – How it happens?

Not a “revolution” but a “migration” process

1. industrial revolution

Mechanisation

- Mech. control (cam disc, cam)
- Energy: water / steam power

Industry 1.0

2. industrial revolution

Electrification

- Punch cards as program memory
- Conveyer belts
- Master shafts
- Energy: electrical

Industry 2.0

3. industrial revolution

Digitization

- Freely programmable control units
- PLC and PC based control units
- Field busses (ethernet based)
- Flexible production systems
- Electronical data storage

Industry 3.0

4. industrial revolution

Connection / Internet

- People as key players
- Distributed intelligence
- Fast integration and flexible configuration
- Open standards
- Virtual real-time representation
- Digital life-cycle management
- Secure value-creation network

Industry 4.0

The transformation of industry 3.0 to industry 4.0 (connected industry) occurs gradually

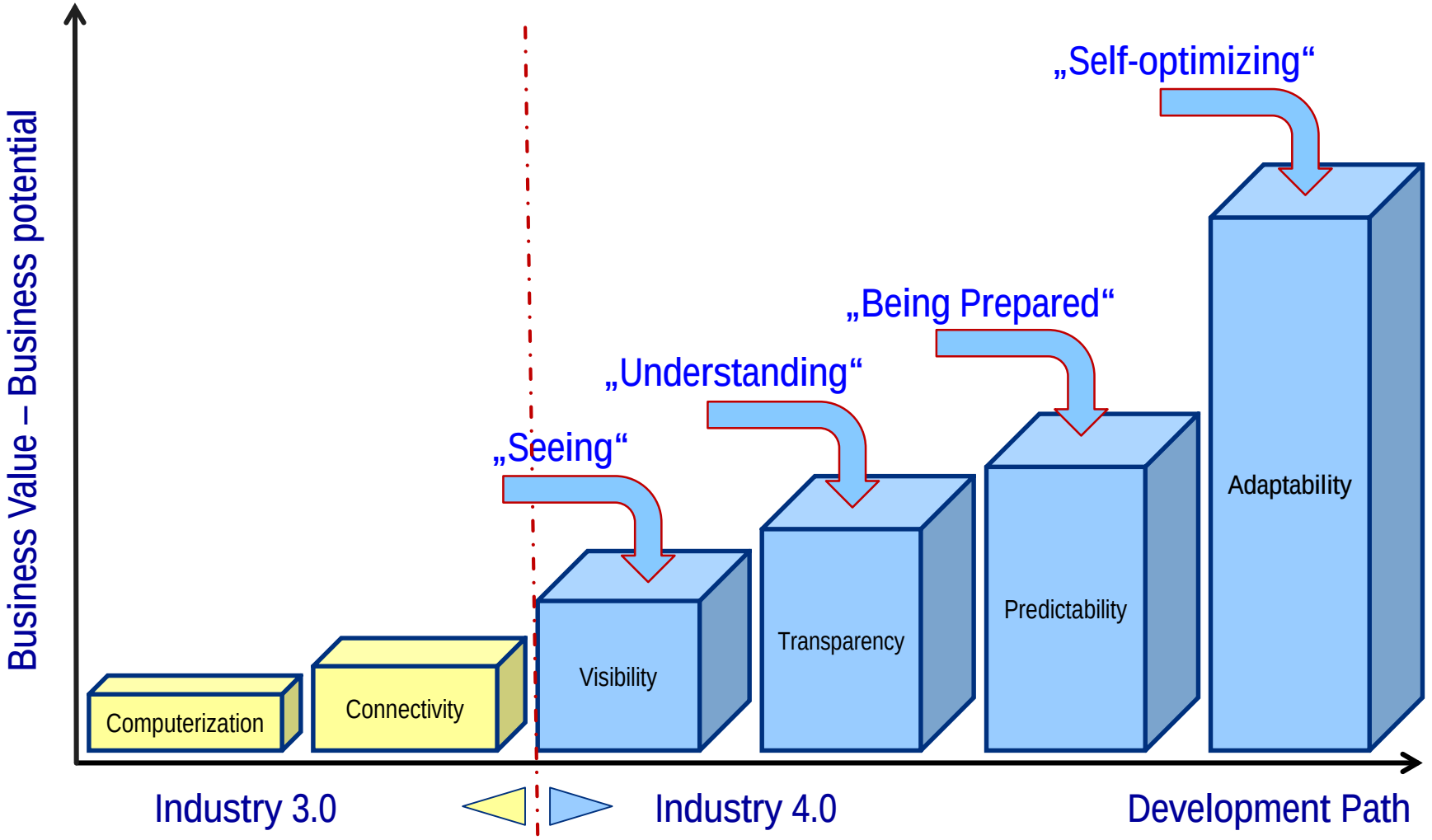
Principles: Connectivity, Modularity, Interoperability

Cyber-physical systems communicate in real time not only with one other but also with humans; affecting all the value chain processes in the organisation.

Smart Factory – reconfigurable, self optimized production

Pic. Ref: Bosch Industry 4.0 Generic Presentation

Smart Factory Migration Path

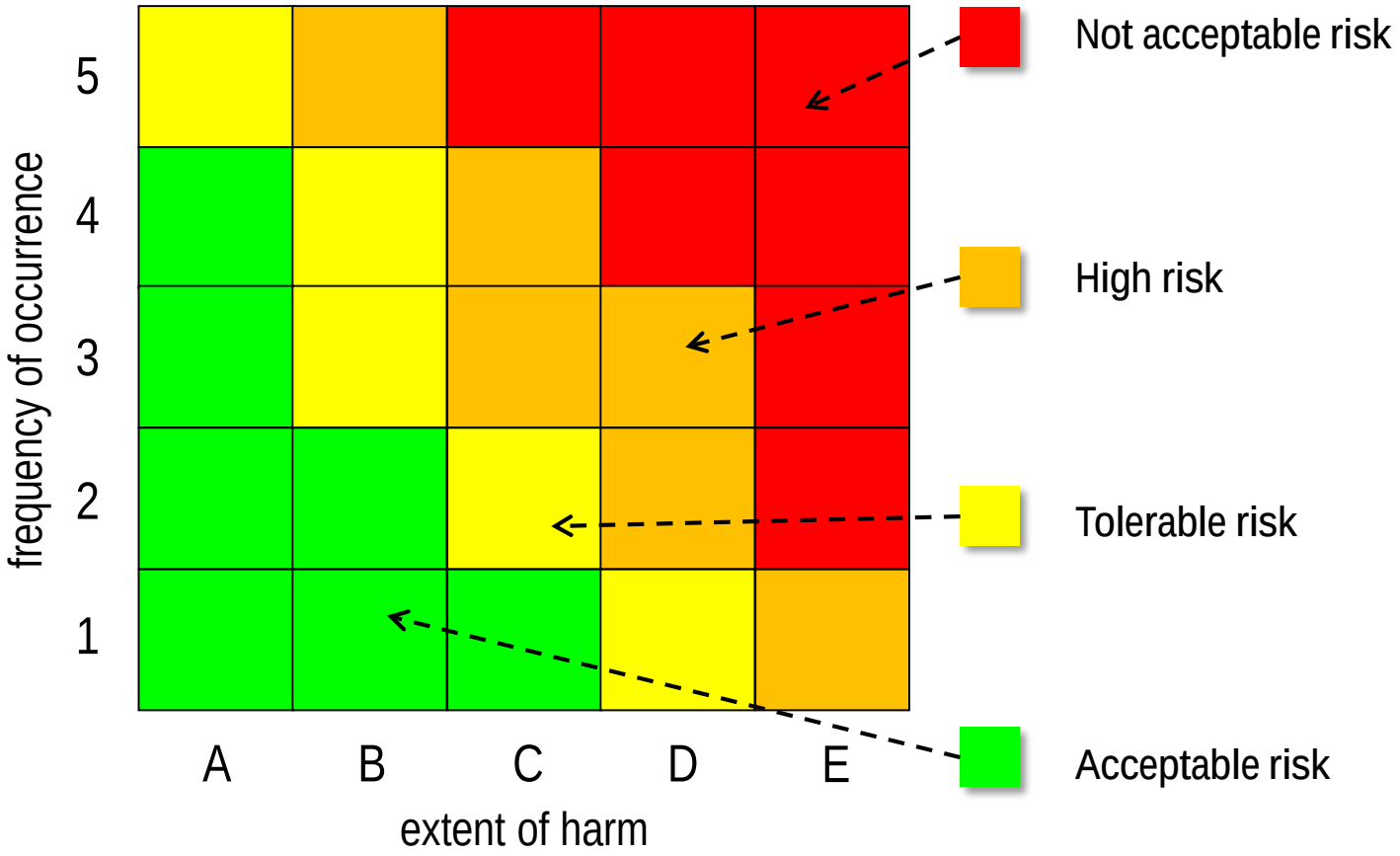


Managing the Migration - Challenges

Technology suppliers provide products and solutions for manufacturers to design, implement, and operate complex systems (robots, platforms, IT/OT convergence, data analytics)

- Safety
- Security
- Reliability (Performance and Interoperability)
- Scalability

Key Safety Approach - Functional Safety



Reconfigurable and Self-optimized Production

From a world of not connected things ...

... to the Internet of Things

Two trends impact the production line (green and brown field):

⇒ *Individualization/customizing of products – sample size one*

⇒ *Digitalization of everything – the concept of Cyber Physical Systems*

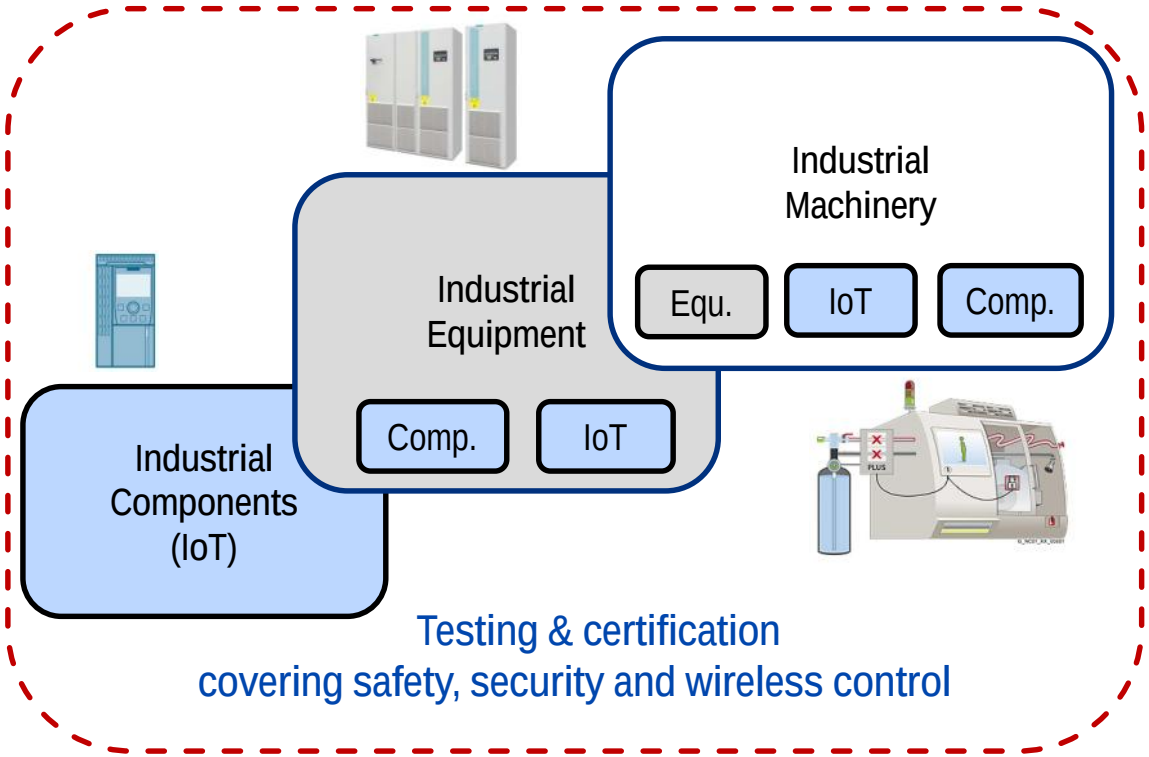
- Individualization requires:
  - Flexibility of production assets
  - Transformation ability
  - Availability based on wireless connections
  - Reliability and Repeatability

- Digitalization enables:
  - Smart Components (self-describing)
  - Smart Sensor systems and unlimited data availability (real time data processing)
  - Cognitive computing is becoming part of Automatization and production control

- We analyze the safety impact on different SMART production concepts
  - Smart Factory, Smart Cell and Smart Machine

Safety Management from Component to System Level

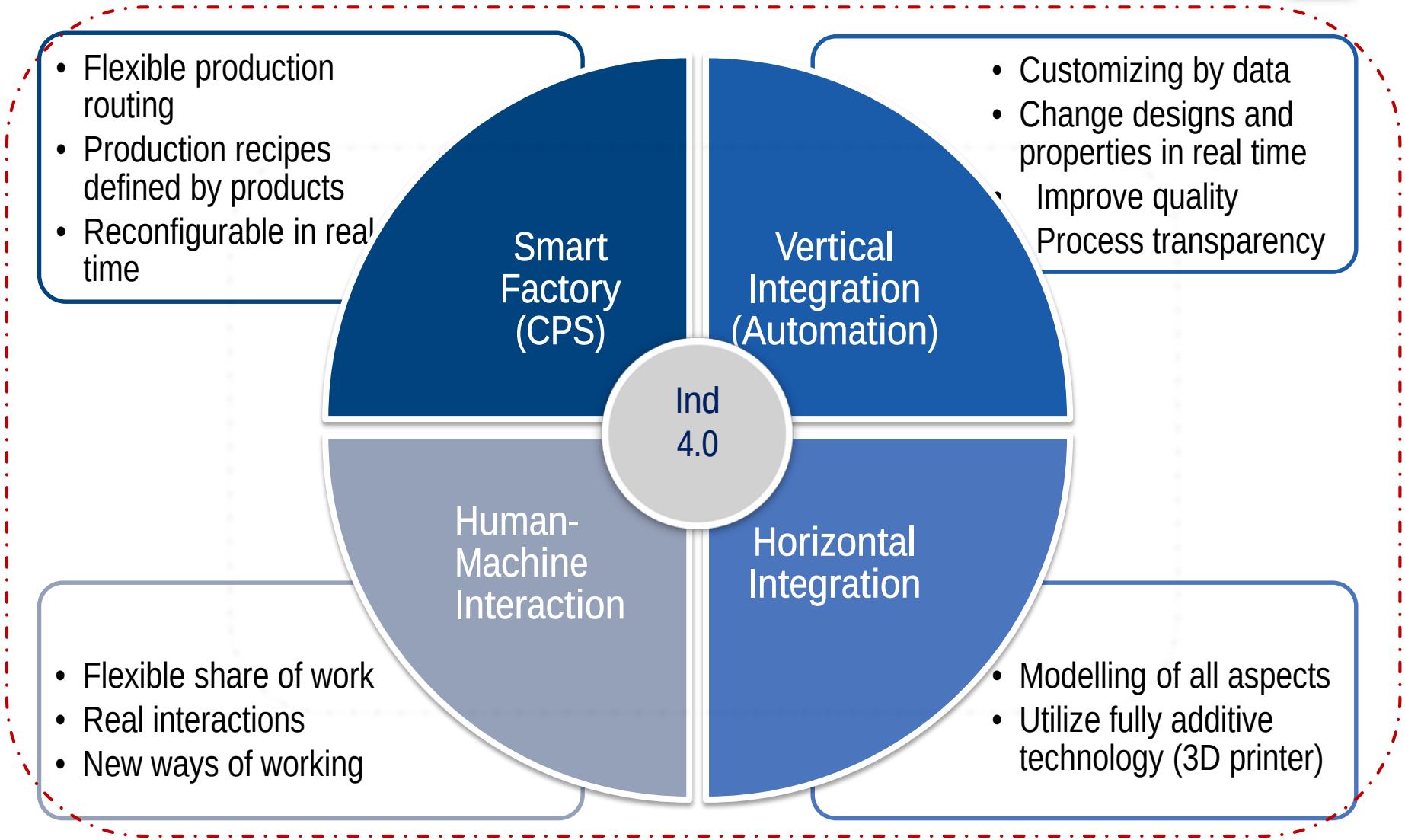
Component Safety → Equipment Safety → Machinery Safety → Connectivity / Interoperability → System Safety



Product safety
Electrical safety
Functional safety
Explosion protection
Environmental testing
EMC testing
Wireless communication & interoperability
Machinery safety
Global Market Access

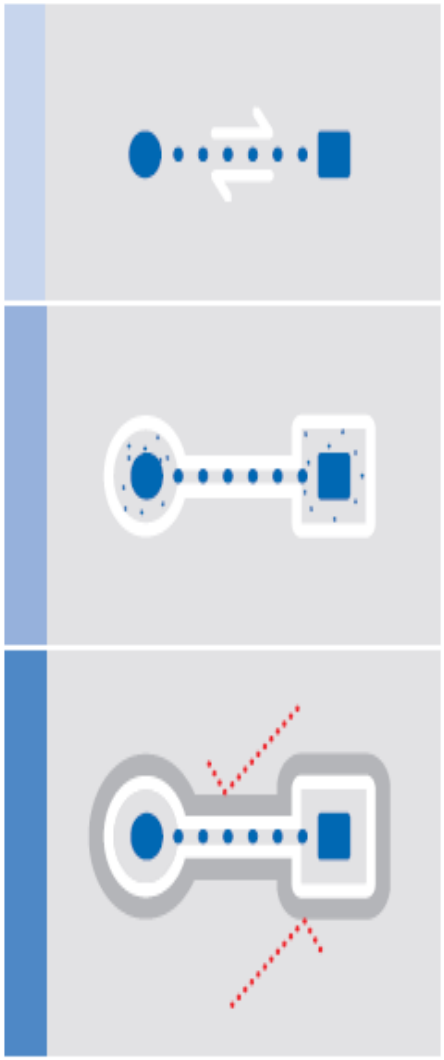
System safety
Functional safety
Wireless communication & interoperability
Process safety
Security

Safety Solutions for Reconfigurable and Self-optimized Production



Safety & Security – New Kind of Challenge for Industry 4.0

Embedded systems are key components in smart, automated installations



Communication
Ability of different systems to work together

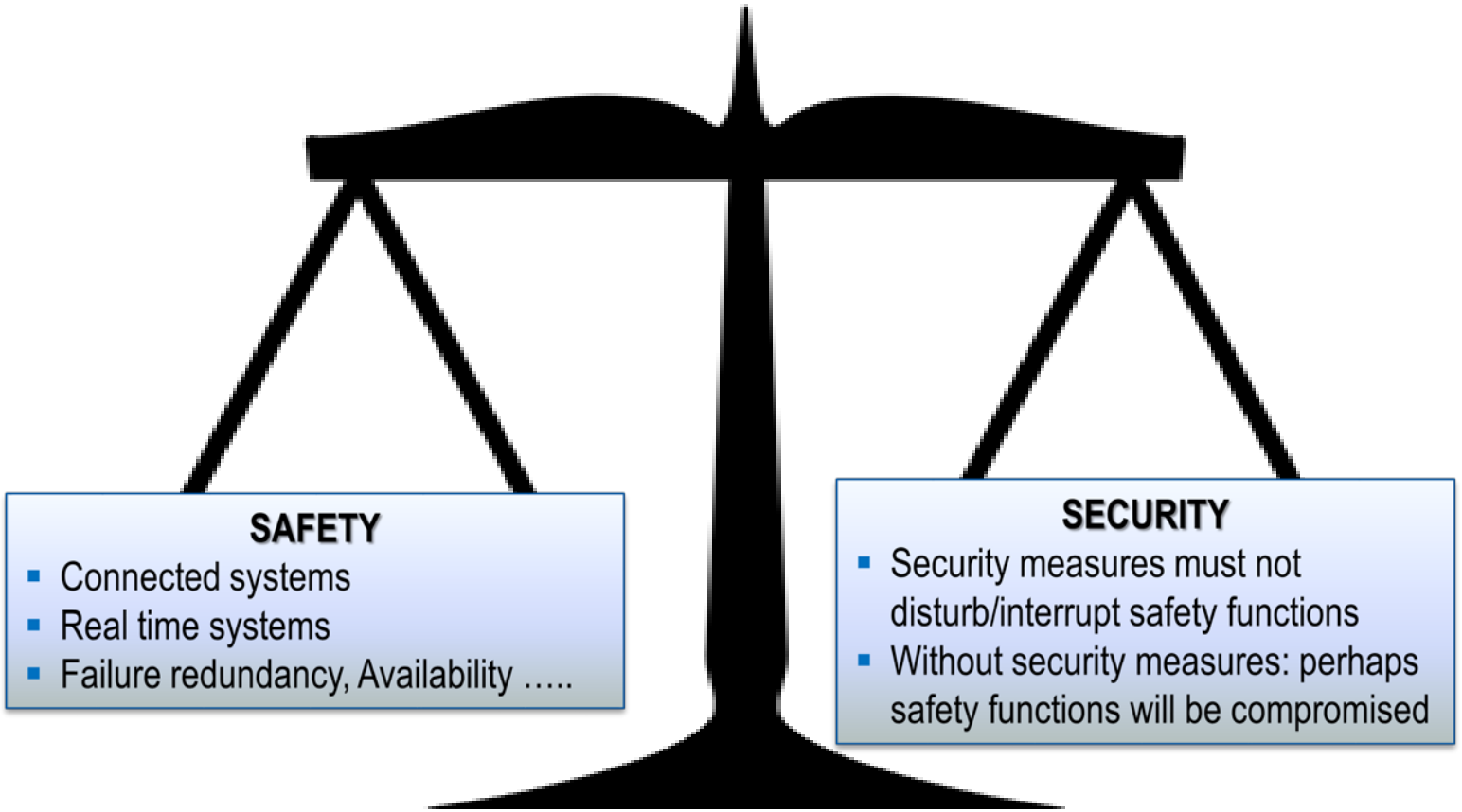
Safety
Reliability for the environment (user, environment, functionality)

Cyber Security
System security (Security for Safety)

- Embedded systems are widely used for **measuring, regulating and controlling** of all types of devices and systems.
- As information exchange between these systems (networks) increases, **new issues of security and availability arise** not only for the individual device but for the whole system.
- Need for **conformance testing** of the single component as well as in **testing communication** between devices (interoperability) up to the **safety concept** of the overall system (Security for Safety).

Safety and Security are Inherently Connected

In connected systems suddenly the weakest security point becomes the weakest safety point

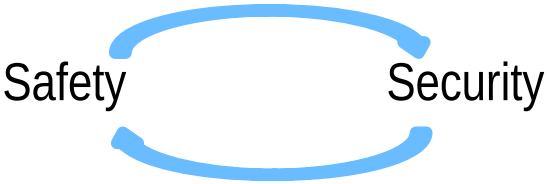


Smart Factory – Industry 4.0 Safety and Security

Paradigm change of industrial key solutions on the way to Industrie 4.0 – complexity increase

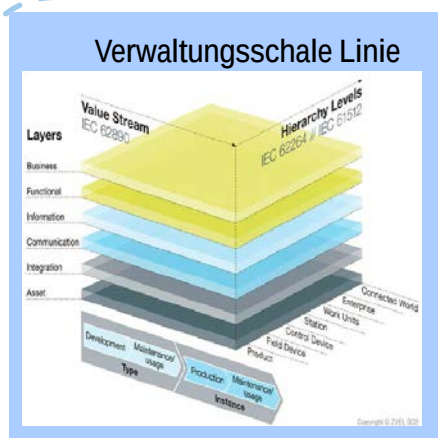
Industry 3.0	Industry 4.0	
Centralized control	Decentralized self-organization	Safety
Fixed Value Added Chain	Ad-hoc Value Added Chain	
Mass production	Individualized production	Safety
Proprietary systems	Open systems	Safety and Security
Automation pyramid	Service oriented network	Safety
Specific and dedicated solutions	Cloud-based resources	Safety and Security
Systematic based on hierarchy	Flexible and changeable concepts	Safety
Fixed systems with customization	Decentral and modular software	Safety
Database and software suites	Cloud and individualized Apps	Safety and Security

- Future Interaction (Ind. 4.0)



Ref:: [Dais 2014, S.630f], [Bauernhansl et al. 2014, S.26f], [Pötter et al. 2014, S. 161], [Müller 2015, S. 126], [Kleinmeier 2014, S.572 ff], [Bildstein 2014, S.581 ff]

Smart Production – Holistic Approach



Process layer

System Layer (Linie)

Module Layer

Smart Components

Smart Machinery Equipment

Smart Factory

Smart Industry Industrie 4.0

Virtual World => Software

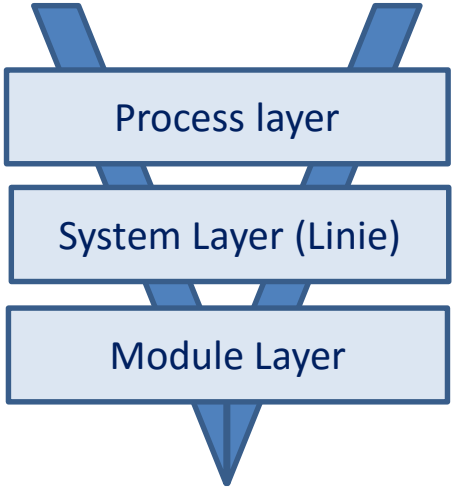
Industry => Hardware

All digital data on process, system and machinery module level are available within RAMI 4.0 – **virtual modeling**, **testing** and **certification** can be executed on the **virtual representation** of the line.

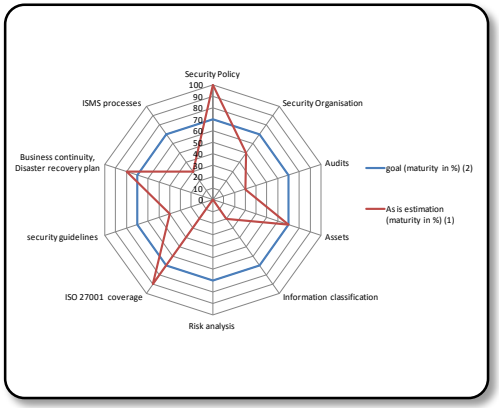
Smart Production – Holistic Approach – Virtual Testing

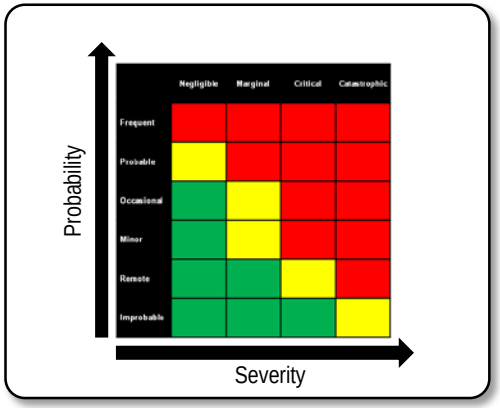
VIRTUAL & PHYSICAL TESTING

- Risk analysis
- Threat analysis
- Security testing
- Process analysis



Risk analysis



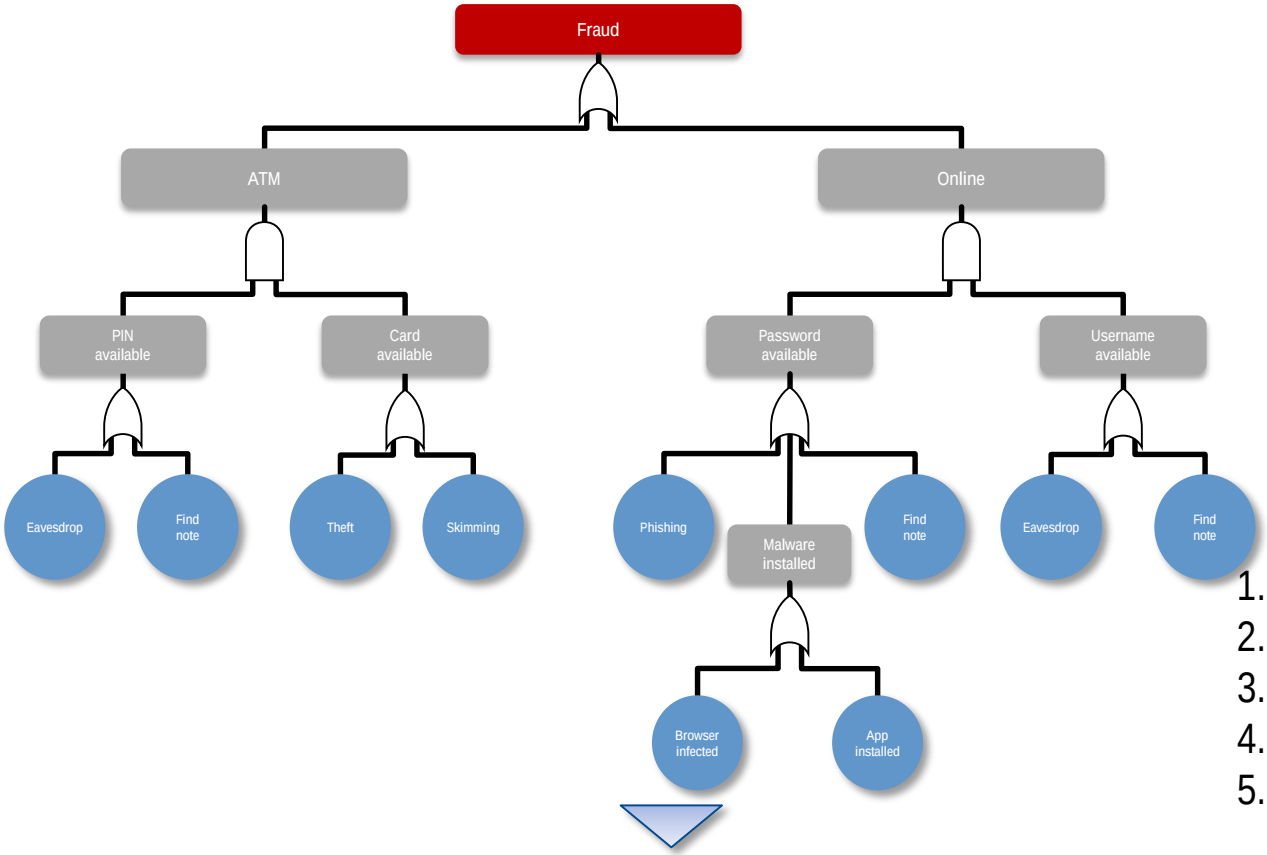


Analysis of current status for Target of Evaluation → Risk Analysis → Definition & implementation of counter measures → Residual risks → Continuous Controlling, Monitoring, Benchmarking

Security Concept

- Identified security requirements
- Defined security measures

Threat analysis

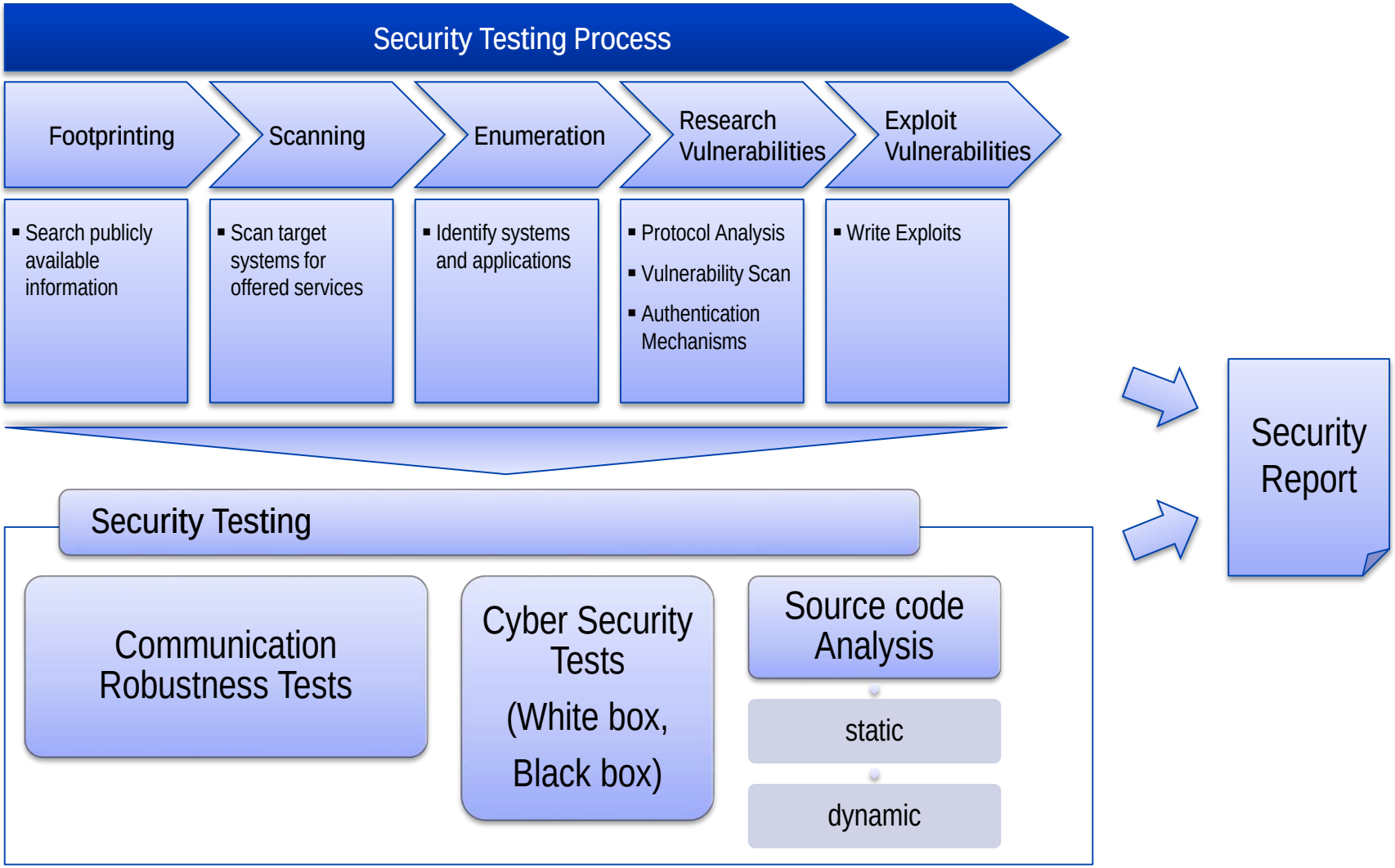


1. Definition Scope
2. List of relevant threats
3. If needed: attack tree
4. Threat and vulnerability analysis
5. Derivation and definition of security measures

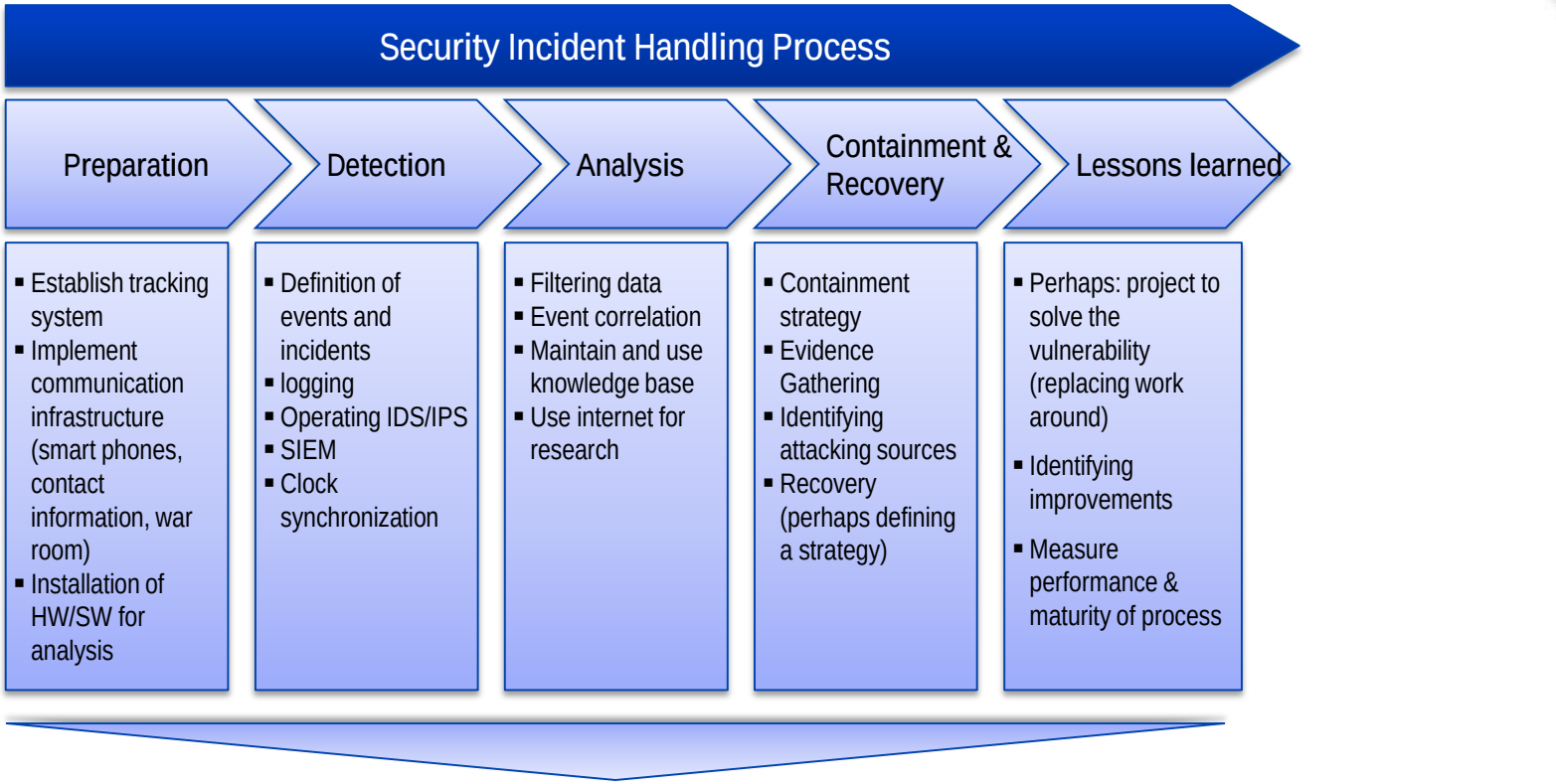
Security Concept

- Identified security requirements
- Defined security measures

Security Testing



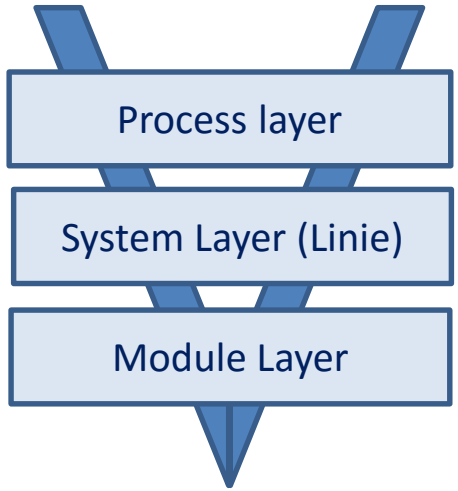
Process analysis



Holistic Approach to Industry 4.0
- Basis of a Successful Business Case

VIRTUAL & PHYSICAL TESTING

- Risk analysis
- Threat analysis
- Security testing
- Process analysis

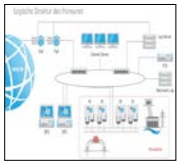


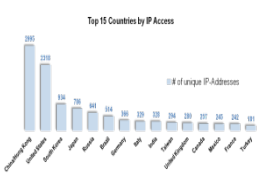
SAFE
SECURE
RELIABLE
•PERFORMANT
•INTEROPERABLE
SCALABLE

Key Take Aways

- Industry 4.0 implementation is a migration process to a system:
  - Affects complete organizational value chain
- And it must be managed with a holistic approach
  - Component, equipment,system, process levels
  - Safety, security, reliability, scalability
- Safety and security are inherently connected
- Reliability and scalability involve safety and security
- Holistic approach methodology:
  - Risk and threat assessment
  - Safety and Security assessment
  - Process assessment
  - Virtual and Physical testing
- Expertise of an Independent third party to introduce Industry 4.0:
  - Focuses on manufacturer‘s business case

Honeynet

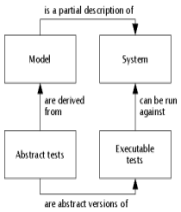




Autonomous Driving

Drone Qualification

Software based testing



Choose certainty.
Add value.

TÜV SÜD Digital Service CoE Singapore

Your partner on the way to excellence

www.tuv-sud.com/digitalservice

Dr. Andreas Hauser
Director, CoE Digital Service
TÜV SÜD, Singapore
andreas.hauser@tuv-sud.sg

Eley Querner
SVP, CoE, Digital Service
TÜV SÜD Asia Pacific
Singapore
eley.querner@tuv-sud.sg