

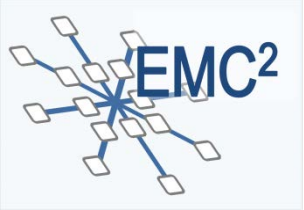
# HiPEAC Conference 2017

## EMC² - Workshop

Stockholm, January 24th, 2017

**Upcoming Standards for Open Adaptive CPS, IoT  
and Cloud-based Systems**  
**Safety & Security & Tool Interoperability & others**

Erwin Schoitsch  
[Erwin.schoitsch@ait.ac.at](mailto:Erwin.schoitsch@ait.ac.at)



# IEC TC 65: Industrial Automation & Control: Family of Standards



Consistent mapping from enterprise top level down to device

- **SC 65A:** System Aspects - **Functional safety** (IEC 61508, 61511, 62061 ...) – well established
- **SC 65B:** Measurement and control devices (covering device/unit level (3)): measurement devices, analyzing equipment, actuators, and programmable logic controllers, covering **interchangeability, performance evaluation, functionality definition and safety** (e.g. 61131-3, -6, -9)
- **SC 65C:** Industrial networks (covering **communications, safety, industrial communications security** – fieldbus profiles, IEC 61743-4-x etc.)
- **SC 65E:** **Devices and integration in enterprise systems** (enterprise level):
  - IEC 62264-1 Ed. 2.0: Enterprise-control system integration
  - IEC 62541-10 Ed.1.0 OPC Unified Architecture Specification
  - IEC 62769 Ed. 1.0 Devices and integration in enterprise systems
- **WG 10:** Security for industrial process measurement and control - Network and system security, with IEC 62443 – Security for Industrial communication and control systems - in close co-operation with ISA (International Society for Automation, ISA 99 committee) – **industrial cyber-security**

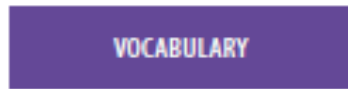


# IEC TC56 Dependability (formerly: Reliability and Maintenance)

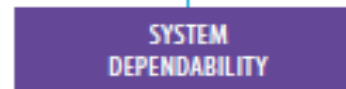
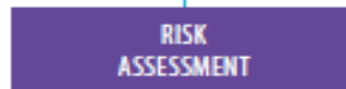
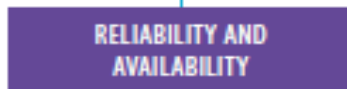


“Dependability” includes all aspects of availability, reliability, recoverability, maintainability, and maintenance support performance , as well as other attributes such as usability, testability and durability (IEC 60300-1)

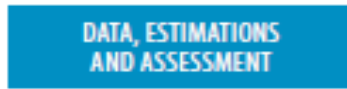
## CORE STANDARDS

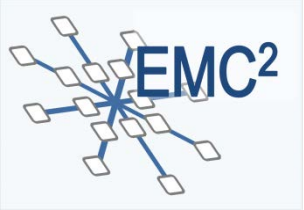


## PROCESS STANDARDS



## SUPPORT STANDARDS





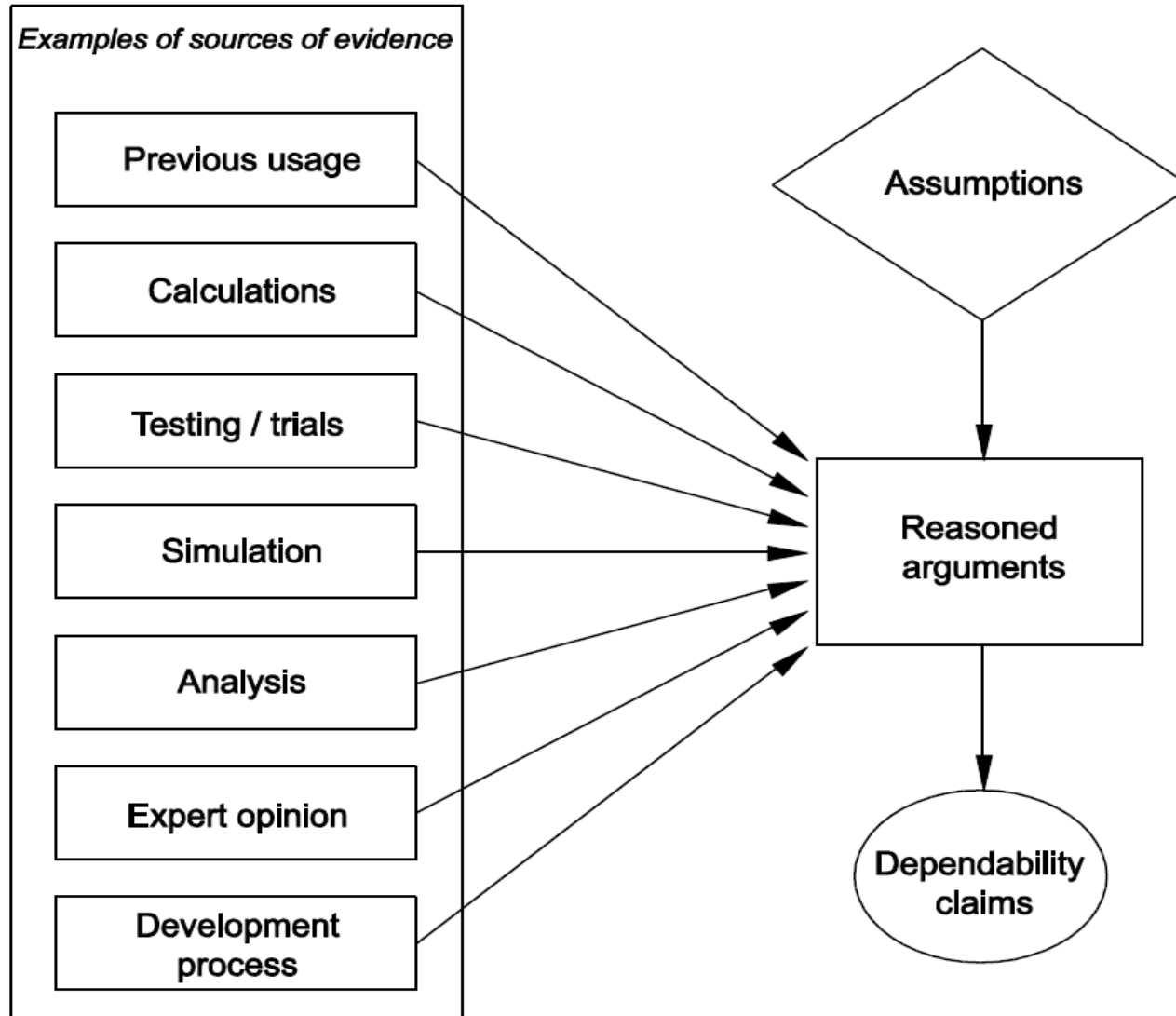
# IEC 62741:2015 The Dependability Case

Guide to the demonstration of dependability requirements - The dependability case

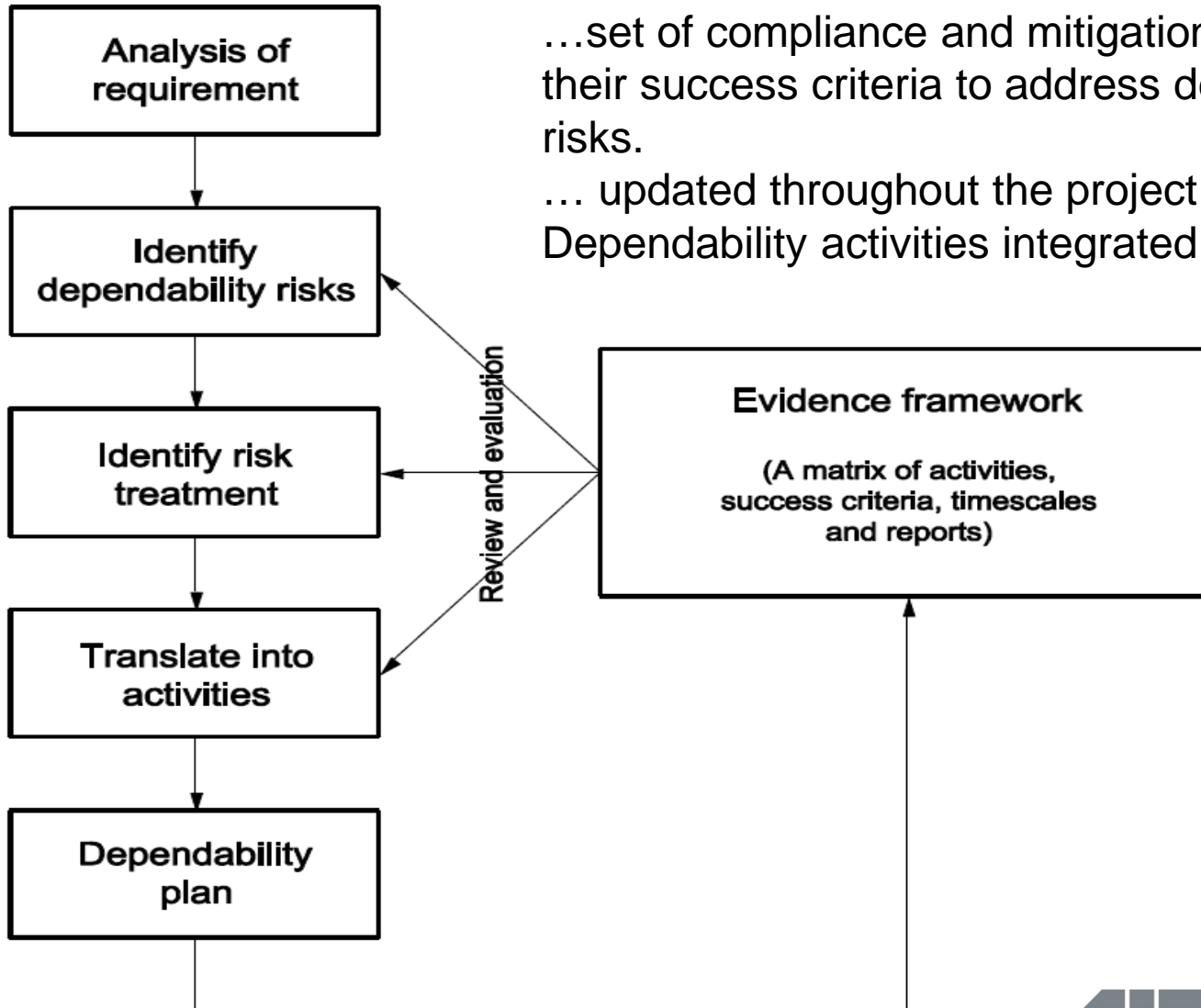


- Is an evidence-based, reasoned, traceable argument that a defined system does and/or will satisfy the dependability requirements (**rather a process, not prescriptive**)
- gives guidance and establishes general principles for the preparation of a dependability case → *a very general, holistic approach*
- written in a basic project context where a customer orders a system that meets dependability requirements from a supplier and then manages the system until its retirement.
- methods provided in this standard may be modified and adapted to other situations as needed, normally produced by the customer and supplier but can also be used and updated by other organizations.
- For example, certification bodies and regulators may examine the submitted case to support their decisions and users of the system may update/expand the case, particularly if used the for a different purpose.
- Keywords: dependability, reliability, availability, maintainability, supportability, usability, testability, durability → *extendable to safety & security as part of dependability and performance*

# Dependability Case Example Development of Claims



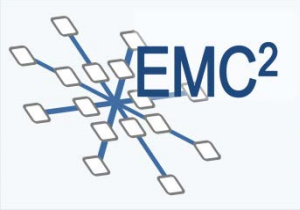
# Example Dependability Case: Develop Evidence Framework



...set of compliance and mitigation activities and their success criteria to address dependability risks.

... updated throughout the project...

Dependability activities integrated in general PM

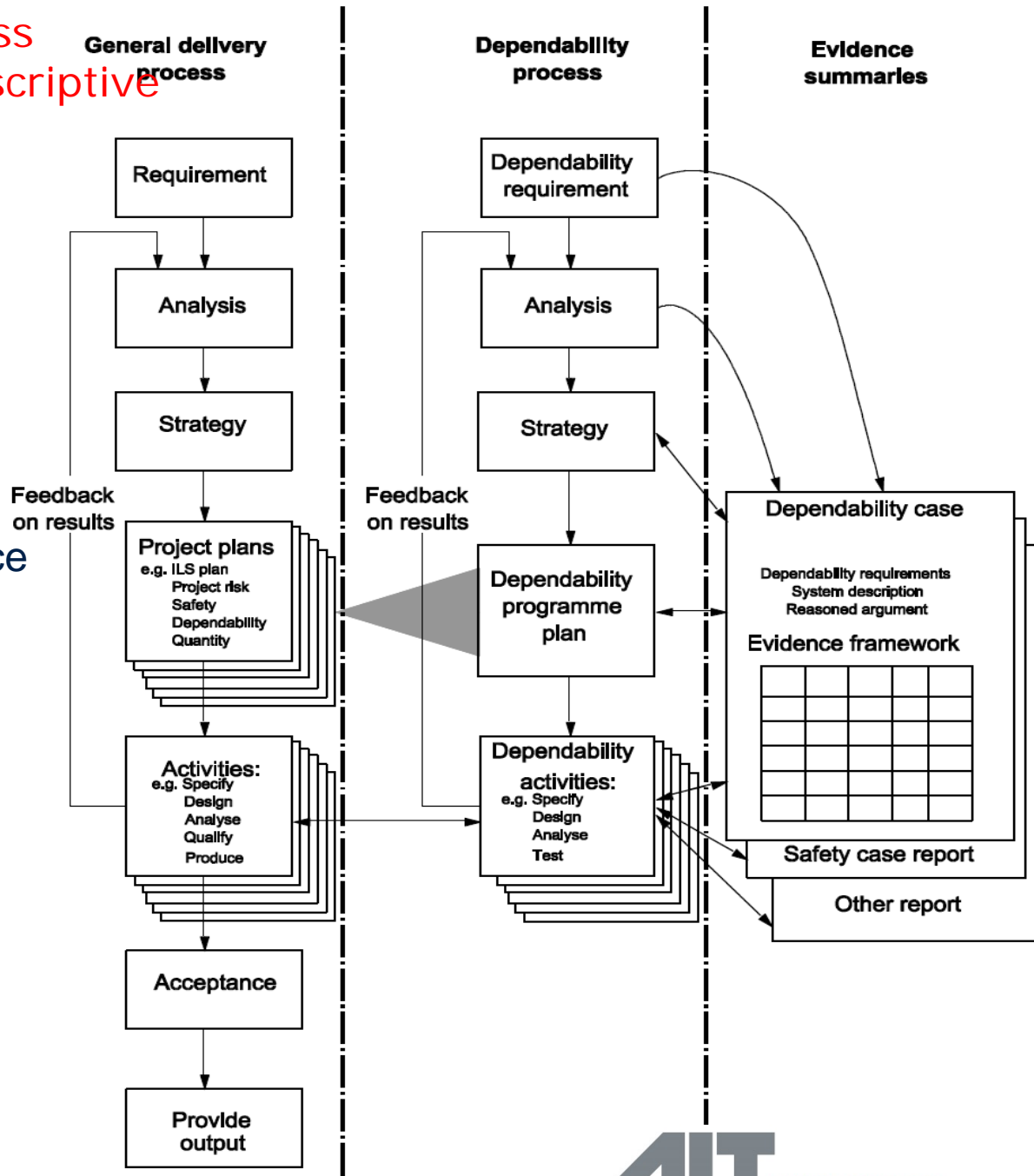
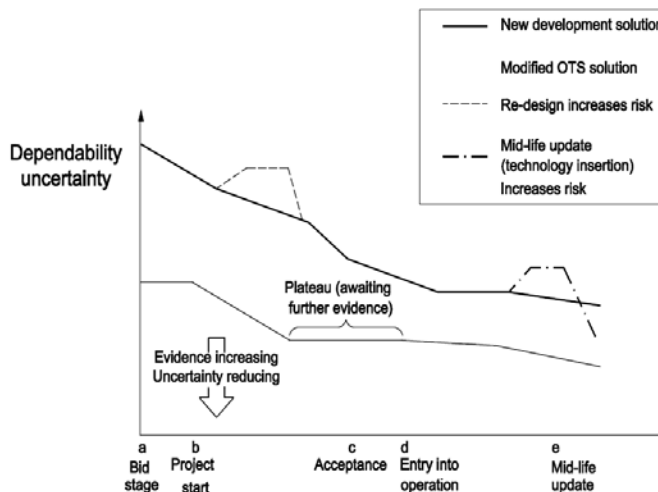


Defines a process rather than prescriptive requirements

# Dependability Case

Dependability process, overall delivery process and evidence produced:

- Analysis of Dep. Requ.
- Dependability strategy
- Dependability plan
- Progressive Dep. Assurance
- Dependability case review








# Industrial Automation Security: IEC 62443 (in close cooperation with ISA 99)

<b>General</b>	ISA-62443-1-1 Concepts and models	ISA-TR62443-1-2 Master glossary of terms and abbreviations	ISA-62443-1-3 System security conformance metrics	ISA-TR62443-1-4 IACS security life-cycle and use-cases
----------------	--------------------------------------	---	--	---

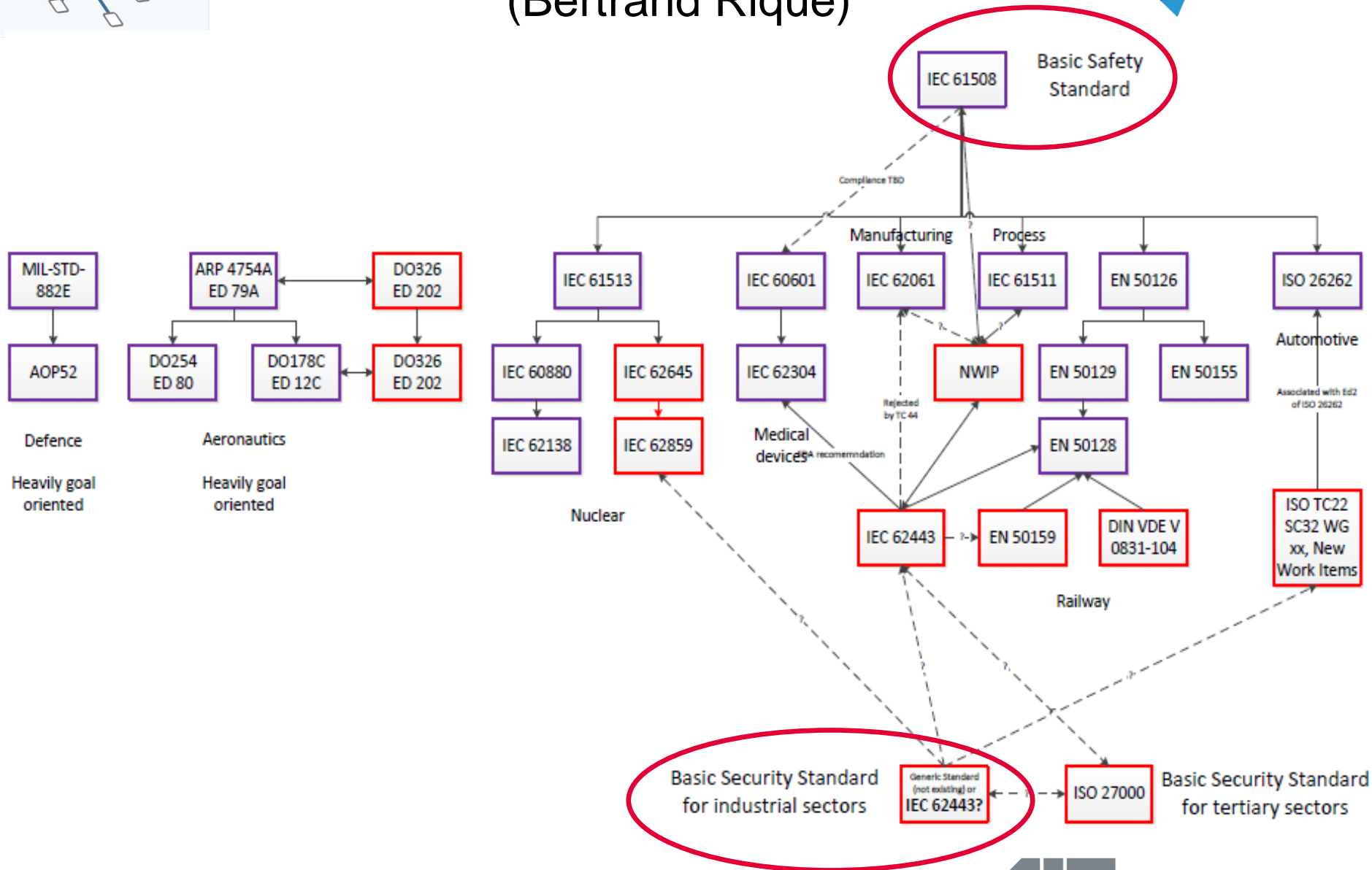
<b>Policies &amp; Procedures</b>	ISA-62443-2-1 Requirements for an IACS security management system	ISA-TR62443-2-2 Implementation guidance for an IACS security management system	ISA-TR62443-2-3 Patch management in the IACS environment	ISA-62443-2-4 Requirements for IACS solution suppliers
----------------------------------	--	---	---	---

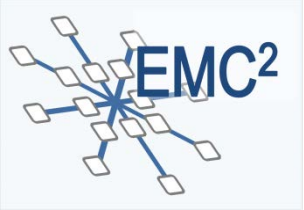
<b>System</b>	ISA-TR62443-3-1 Security technologies for IACS	ISA-62443-3-2 Security risk assessment and system design	ISA-62443-3-3 System security requirements and security levels
---------------	---	---	---

<b>Component</b>	ISA-62443-4-1 Product development requirements	ISA-62443-4-2 Technical security requirements for IACS components
------------------	---	--

<b>Status Key</b>	 Published	 In development	 Planned
	 Published (under review)	 Out for comment/vote	



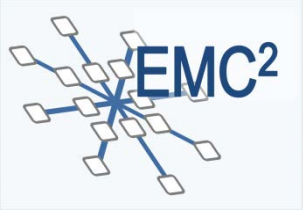




# Safety & Cybersecurity in existing Standards and Committees



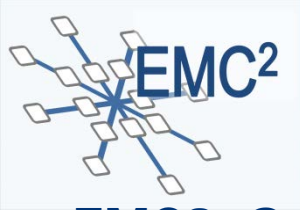
- **IEC 61508-3** Ed 3.0 preparation: Security aware safety guidelines – first proposals for IEC 61508-3, needs consideration in part 1 and 2 as well!!
- **ISO 26262**, Ed. 2.0: AIT proposal presented Jan. 2015 to consider security aware safety issues particularly because of “connected car” and “highly automated driving” → proposal for Part 2 and Part 4, now part of CD, DIS
- **“Road Vehicles – Automotive Security Engineering”**: **TWO new Work Items** proposed: **DIN, SAE (basis J3061)**
- **EN 50129, EN 50159** (Railway): particularly in Germany (DIN VDE V 0831-104 - **EMC<sup>2</sup>**)
- **ISA 84, ISA 99 and ISA 100** (process industry, industrial process control and communication), IEC 62443 (industrial automation, network and communication security), ISA 95 production
- **IEC TC44** – Safety of machinery, electro-technical aspects: **new work item** started: Security aspects related to functional safety of safety-related control (for safe machine operation despite cybersecurity threats)
- **Do 326A/ED 202A**: Airworthiness Security Process Specification, Do 355A/ED 204A Information Security Guidance for continuing Airworthiness
- **IEC 62589** (*Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity*) **AND new project**: “Nuclear power plants - Instrumentation and control-systems – Security controls”
- **MISRA-C: 2012 Amendment 1: Additional Security Guidelines**



# EMC<sup>2</sup>: Certification of Safety & Security in adaptive dynamic systems @ run-time



- Safety critical open adaptive system cooperate to provide functionalities not achievable by a single system
- However, the overall constituents and configuration of a (super-) system evolving over time cannot be assessed a-priori at development time
- Solution: shift parts of the safety certification activities into runtime, and perform automated safety checks for dynamic systems integration and adaptation, using pre-certified artefacts and contract-based design methodology
- ConSerts: modular conditional certificates that are issued at development time for each system
- Basic difference between safety and security: Safety = never change if possible; security = frequent updates
- Investigating support for security assurance between safety critical open systems by using Conserts and Run-time certification
- **Alternative:** VM (Virtual Machine) – Virtualization-based security and fault tolerance (changing roles at run time: active, stand-by, cleansing)



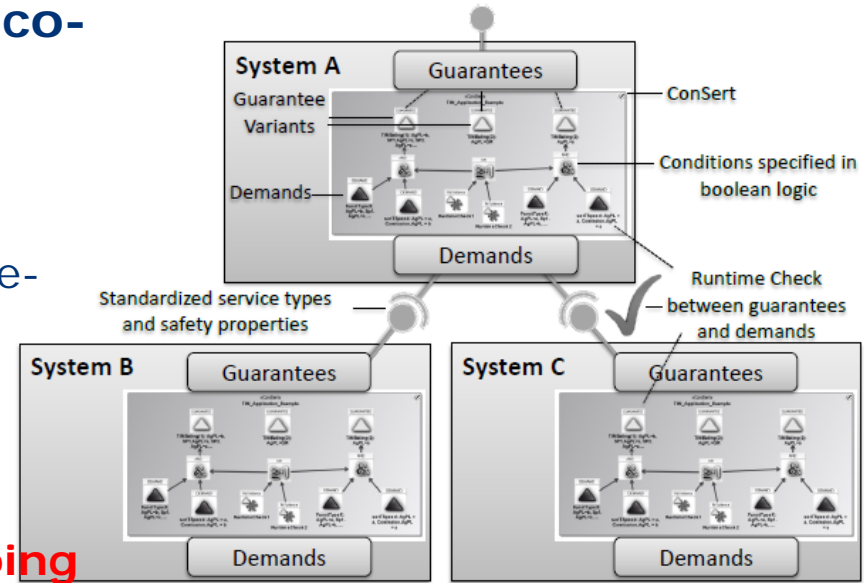
# Standardisation Cyber-Security-aware Safety



## EMC²: Safety, Security and Quality co-engineering and Certification by Design and at Run-Time

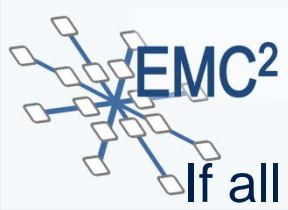
Consequences for methods, techniques and tools: extend them to include security-aware-issues in V&V, RHA, Workflow of certification/qualification process – Cyber-Security particularly requires incremental and life-time (run-time) approach

→ Positioning in IEC 61508 Ed.3.0 ongoing



- **By Design:** Safety & Security Assurance Case @ design time, Traceability from claims to requirements to evidence → **EMC²: e.g. FMVEA, WEFAC Tools**
- **At Run-Time:** Shift parts of the safety and security certification activities into runtime, and perform automated safety checks for dynamic systems integration and adaptation
- **ConSerts:** modular conditional certificates that are issued at development time for each system – assurance at run-time (adaptive)
- Support for **security assurance** between **safety critical open systems**

**NEW**



# Adapting a System during Run Time (Example)



If all used contracts are valid (conserts=conditional contracts) → subsequent incremental Certification at Run-Time – **also for security updates (Safety=never change, security=frequent updates)**

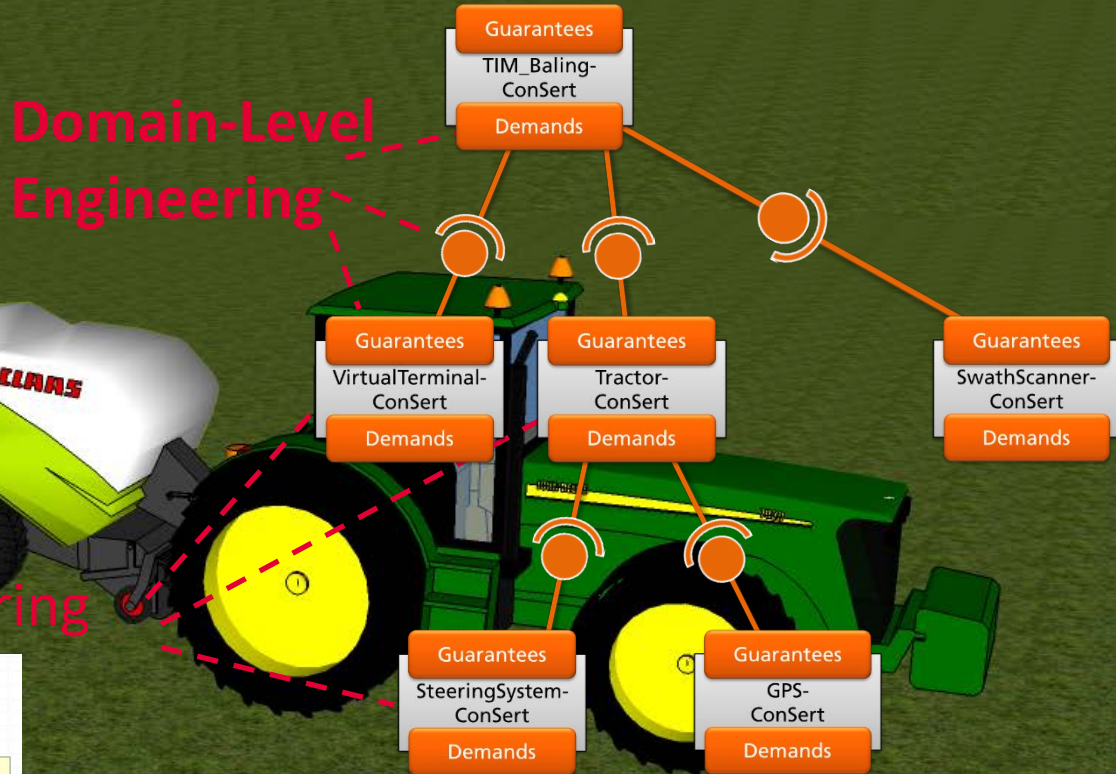
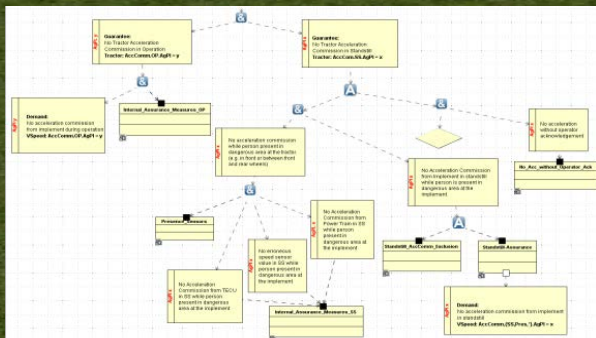
© Fraunhofer IESE, project EMC<sup>2</sup> - different supplement systems attached to same tractor engine

No.	Interface Function	Guideword	Deviation from correct function (effect that is associated with guideword)	Possible Causes	Possible consequences in the TIA baling scenario
1	Auxiliary Valves – Valve state	Omission	No hydraulic flow even though it would be required	Communication failure. Sensor failure. ECU (/SW) failure (tractor or implement).	Rear gate (of the round baler) does not open (or close) even though it must.
2		Commission	Hydraulic flow commissioned even though it is not wanted	Sensor failure. ECU (/SW) failure (tractor or implement). VT failure. "Third party" device issuing unwarranted request.	Rear gate does open (or close) even though it must not.

Domain-Level Engineering

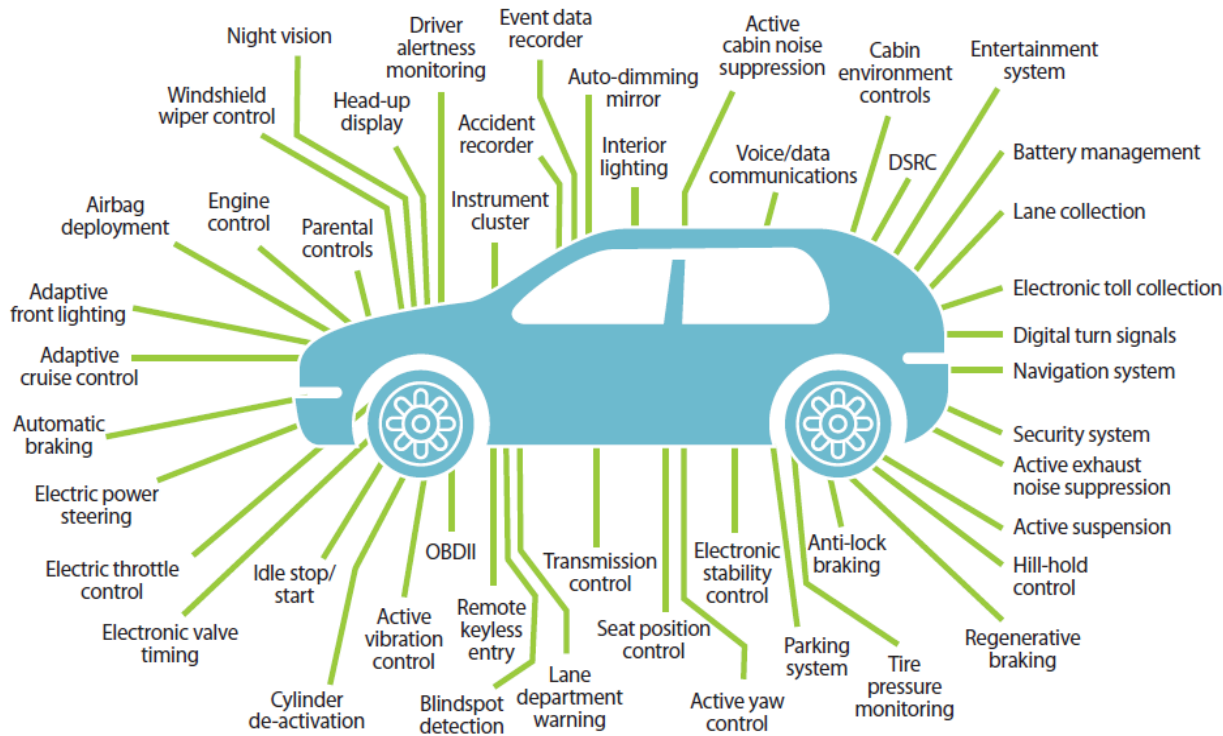


System-Level Engineering



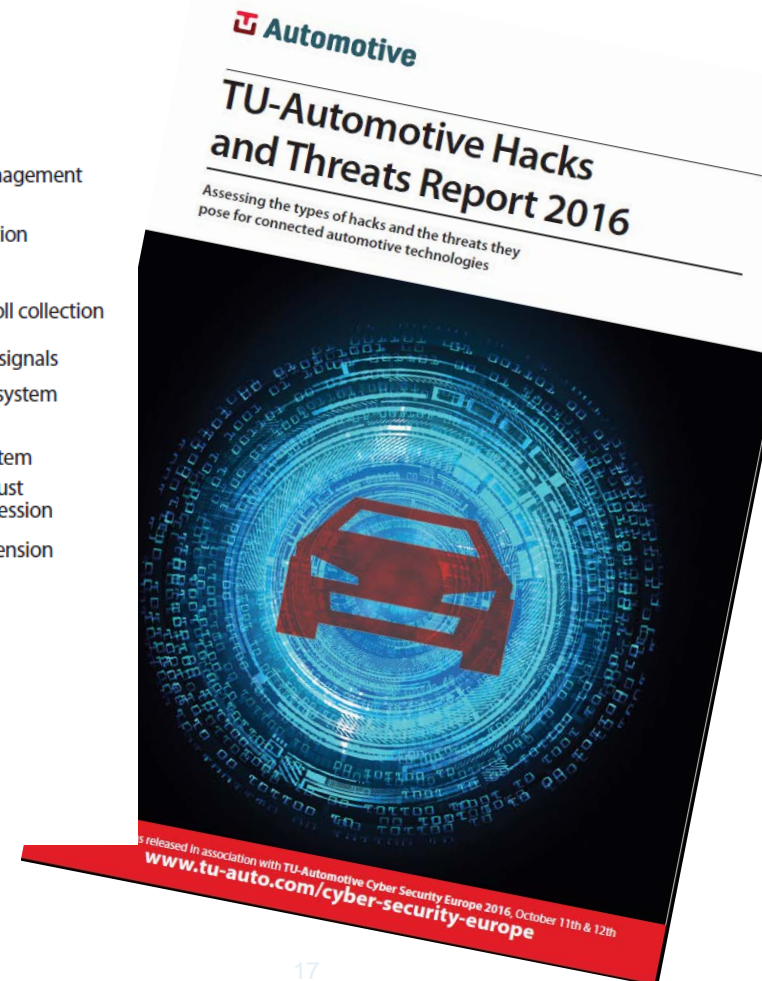
# TU Automotive Hacks and Threats Report 2016

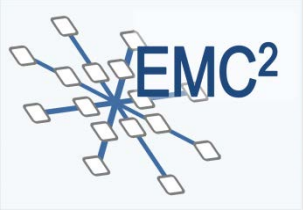
Assessment of the types of hacks and threats for connected automotive technologies (2016) [www.tu-auto.com/cyber-security-europe](http://www.tu-auto.com/cyber-security-europe)



© Nodal Industries 2015

## Increased # of Attack Surfaces





# Proposal to ISO TC22 SC32 WG08 (Jan. 2015)



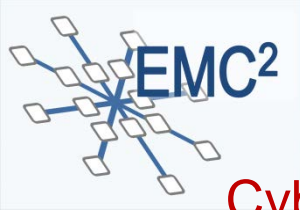
(led to a Cyber-Security & Safety Team for ISO 26262-2018)

- Cyber-security should be included as a risk factor to be considered during hazard and risk analysis → **autonomous vehicles, connected car**
- Appropriate security measures should be implemented, e.g. include recommendations for fitting security standards into ISO 26262 Ed. 2.0
- Include a requirement consolidation phase to resolve potential conflicts and coordinate safety and security requirements
- Validation of safety concept should include/consider security concept
- Security to be considered throughout the whole (safety) life cycle – recommendations to be included where appropriate

First results 2015/16, now in ISO 26262 DIS for 2018-version:

- One new mandatory requirement in Part 2 and some extensions/notes to consider cybersecurity in Part 2 (Management of functional safety) and in Part 4 (Product development at system level)
- A guideline for the Safety/Cybersecurity Interface (SCI) between both teams (details still ongoing)

**NEW**



# Goals of SAE J3061

## Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

- Define a recommended set of high-level guiding principles for cybersecurity for automotive cyber-physical systems, for series production vehicles
  - Define a framework for a automotive cybersecurity lifecycle
  - Give information about useful tools and methods for the design and validation of cyber-physical automotive systems
  - Define basic guiding principles on cybersecurity for automotive systems

### Particular additions in processes:

- Production and operation / service
  - Maintenance and repair activities
  - The operation phase also includes performing and maintaining the field monitoring process the incident response procedure
- Supporting processes (Establishment of communication channels!)

Foundation for further (standard development) activities in vehicle cybersecurity

**→ Huge overlap between SAE J3061 and ISO 26262 in terms of process steps, activities and required work products.**



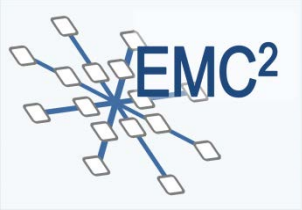
## ISO TC22: New Work Items starting (in one group)

- **“Road vehicles – Automotive Security Engineering”** (German DVA and DIN )
- **“Road vehicles – Vehicle Cybersecurity Engineering”**, SAE, based on the existing SAE Guideline J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems).

Both were accepted, but only one standard is envisaged, and the most important question is which approach to follow → **Joint ISO/SAE Group**

**NEW**

- German proposal tends towards an independent Cybersecurity Standard, not considering the safety impact as basis,
- SAE proposal takes up both: a safety-related part where both sides (safety and security) are taken into account following ISO 26262 life cycles, and a security related part, where issues like privacy and confidentiality without safety impact are handled.



# Standardization: Cloud and IoT



## **BRANDNEW:**

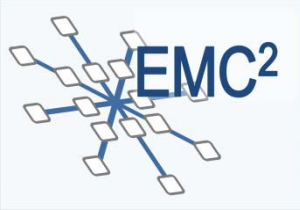
### **AIOTI: Alliance for Internet of Things Innovation**

**→ now AISBL Association (2016), in future becoming a cPPP?**

- IoT becomes a more and more intriguing issue.
- IoT landscape even more fragmented than Embedded Systems 10 years ago
- The recently founded AIOTI have worked in 11 (now 13) Working Groups on Recommendations for an IoT Research Program for the European Commission, a first IoT Calls were issued for this year.

Sources:

**IERC (European Research Cluster on the Internet of Things) 2015,**  
**AIOTI Alliance for the Internet of Things Initiative Reports, Nov. 2015, new**  
**WGs 2016**



# Standardization: Cloud and IoT



## BRANDNEW:

### AIOTI: Alliance for Internet of Things Innovation

WG 3 on “Standardization” has issued three documents:

- IoT LSP Standard Framework Concepts (LSP means “Large Scale Pilots”, an EC Large Projects’ Initiative)
- IoT High Level Architecture
- Semantic Interoperability (need for appropriate tools and semantic interoperability addressed)

IERC and AIOTI – **close cooperation with international standardization organizations**, including ETSI, ITU-T, CEN/ISO, CENELEC/IEC, IETF, IEEE, W3C, OASIS, oneM2M and OGC.

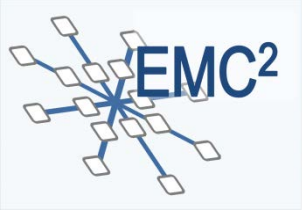
→ **in line with proposed ARTEMIS-IA – AIOTI Cooperation, new task for ARTEMIS-IA Standardization WG as mentioned before today; maybe another possibility to apply the IOS – ICF ideas in an fast evolving field**

## Alliance for Internet of Things Innovation

**Basis: Current Workinggroups = current topics of interest**

WG reports of all WG's (Except WG 10) completed

<b>WG 01</b>	IoT European Research Cluster											
<b>WG 02</b>	Innovation Ecosystems											
<b>WG 03</b>	IoT Standardisation											
<b>WG 04</b>	IoT Policy											
	SME Interests											
		<b>WG 05</b>	<b>WG 06</b>	<b>WG 07</b>	<b>WG 08</b>	<b>WG 09</b>	<b>WG 10</b>	<b>WG 11</b>	<b>WG 12</b>	<b>WG 13</b>		
		Smart Living Environment for Ageing Well	Smart Farming and Food Security	Wearables	Smart Cities	Smart Mobility	Smart Water Management	Smart Manufacturing	Smart Energy	Smart Buildings and Architecture		



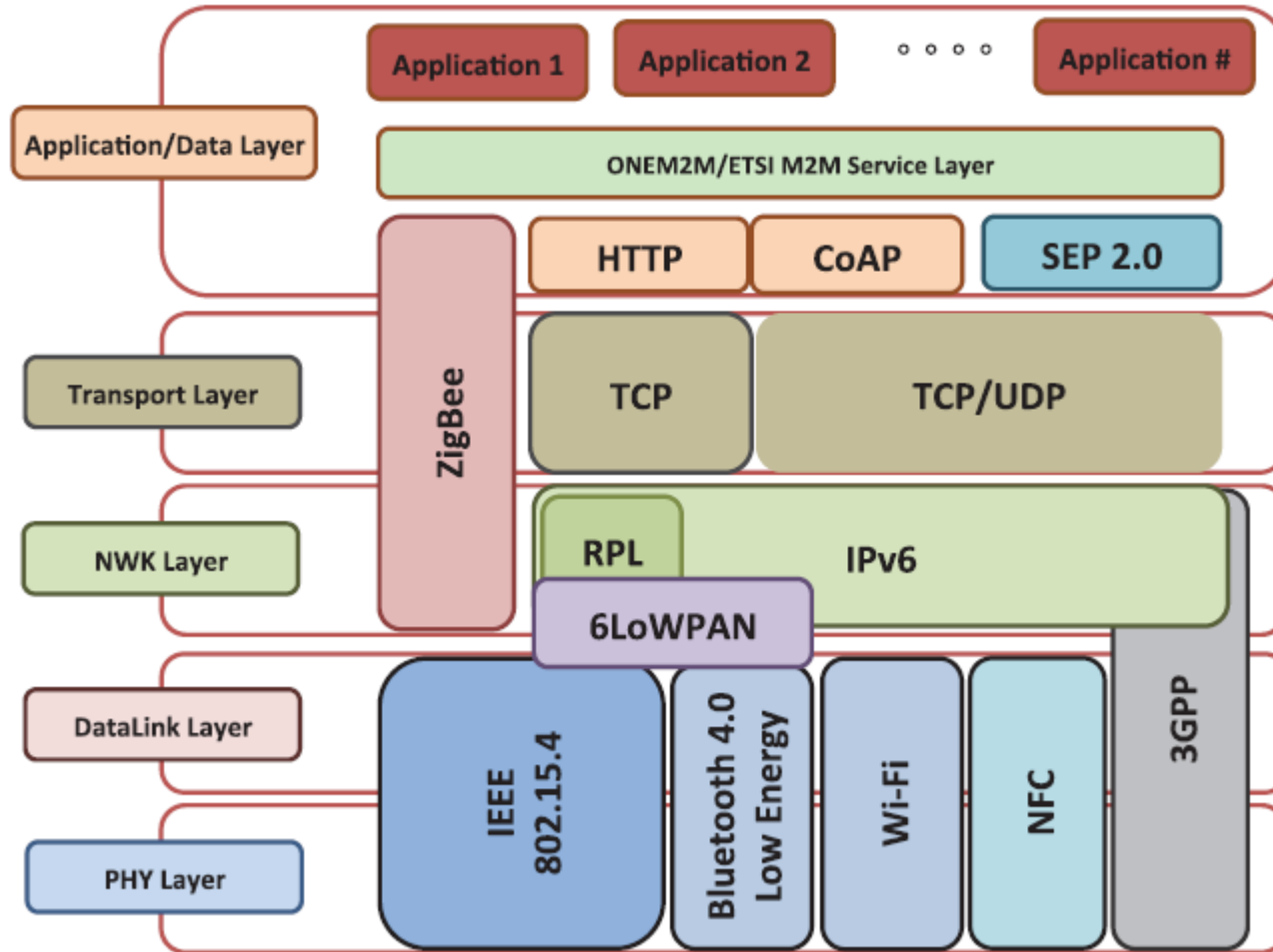
# ISO IoT Standardization Work

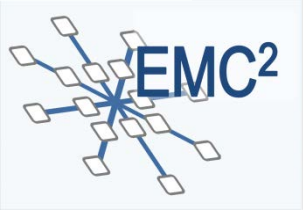


- **ISO/IEC CD 20924 - Information technology -- Internet of Things (IoT) -- Definition and vocabulary**
- **ISO/IEC WD 30141** Internet of Things Reference Architecture (IoT RA)
- **ISO/IEC FDIS 29341-30-2** Information technology -- UPnP Device Architecture -- Part 30-2: IoT management and control device control protocol -- IoT management and control deviceHide
- **ISO/IEC FDIS 29341-30-1** Information technology -- UPnP Device Architecture -- Part 30-1: IoT management and control device control protocol -- IoT management and control architecture overviewHide
- **ISO/IEC FDIS 29341-30-10:** IoT management and control device control protocol -- Data store service
- **ISO/IEC FDIS 29341-30-11:** IoT management and control device control protocol -- IoT management and control data model service
- **ISO/IEC FDIS 29341-30-12:** IoT management and control device control protocol -- IoT management and control transport generic service
- **ISO/IEC 29161** Information technology -- Data structure -- Unique identification for the Internet of Things
- **ISO/IEC AWI 18574 – 18577:** Internet of Things (IoT) in the supply chain

# IoT – Internet of Things

IoT Communications Standards environment:

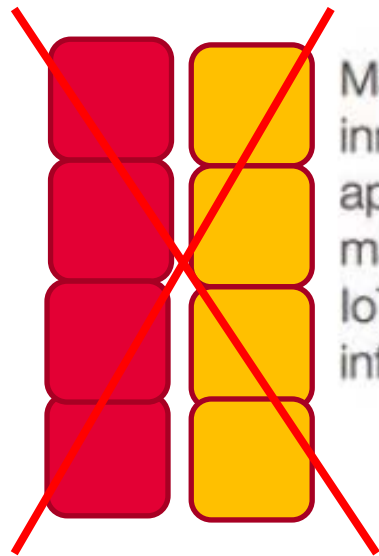




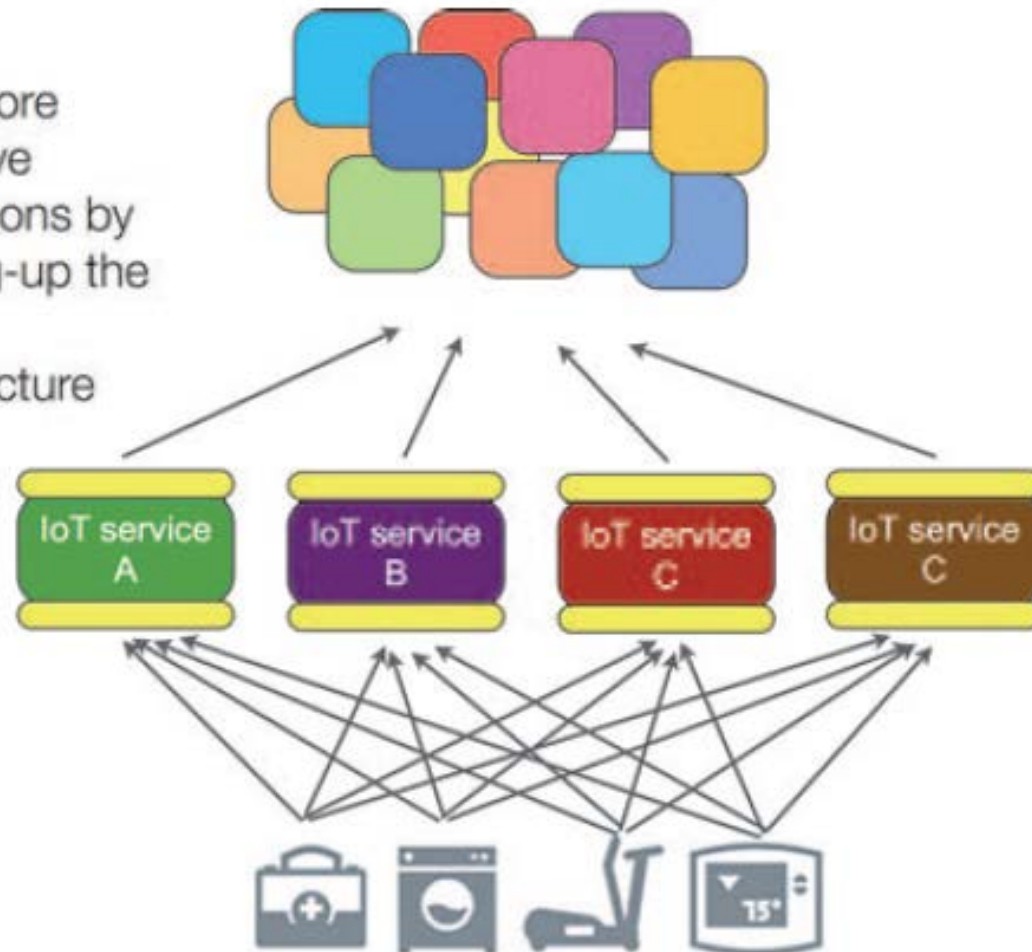
# IoT Internet of Things

## Multiple service stacks

- Horizontal, vertical and transversal communication and control
- Example: OGC sensor web for IoT Interoperability (Open Geospatial Consortium)



Many more innovative applications by mashing-up the IoT data infrastructure



# IoT – Internet of Things

How to bring IoT requirements to communication standards?

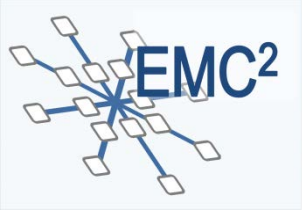
→ Pre-standardization Groups: IRTF-ISOC, ITU-T-Focus Group, IEEE-SA Industry Connection Program, ETSI – ISG → **No separate AIOTI Standards, utilizing existing organizations/groups**

**NEW**

Some results:

- FI-WARE now includes “Generic Enablers” for Future-Internet/IoT (OASIS eXtensible Access Control Markup Language XACML provided to the IoT domain)
- Cybersecurity, privacy, identification, traceability, anonymization, semantic interoperability, interoperability/coexistence testing, performance characterization and scalability, auto-configuration, discovery, self-configuration, service robustness and resilience → IERC central reference for EC IoT pre-standardization
- M2M Service Layer in IoT (integrated horizontal approach instead of vertical-only approach) (transport and application layer) ETSI-M2M
- Cross-Vertical M2M Layer Standardization (integrate different verticals) ETSI-M2M (**co-operation ETSI – AIOTI recently announced**)



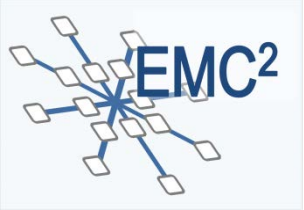


# Standardization: Industrial Internet of Things IIoT



**“NEW” Topic, promoters try to differentiate/separate:**

- Many competing standardization activities, e.g.
  - ISO/IEC JTC1, WG 10, Internet of Things; SWG 5
  - ISO/IEC JTC1, WG 7, Sensor networks
  - ISO, IEC: Many IoT relevant related standards in the communication area
  - IEEE: many IoT related standards and standards projects
  - Particular protocols, e.g. the open AllJoyn protocol, now supported by the AllSeen Alliance (Qualcomm, Cisco, Linux, Microsoft, ...)
  - Open Interconnect Consortium (Intel, Atmel, Dell, Samsung, WindRiver, ...)
  - Thread protocol (Google)
  - Particular protocols for e.g. home devices etc



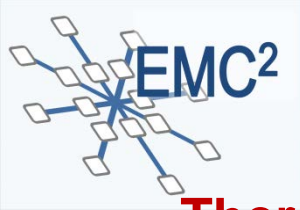
## **BRANDNEW: Standards for the Cloud**

- The Joint Technical Committee of ISO and IEC, JTC1, Subcommittee 30 (“Distributed Application Platforms and Services”) has started foundational work on Cloud Computing Standards. These standards
  - ISO IEC 17788 – Cloud computing – overview and vocabulary
  - ISO/IEC 17789 - Cloud computing - Reference architecture
- are recommended and supported by ITU-T, the International Telecommunication Union.
- In the mean-time , related standards like ISO/IEC 19831:2015 have been published (“Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based protocol”).
- Many other ISO IoT standards published (e.g. around UPnP)
- Particularly relevant for ARROWHEAD and EMC2 successor projects

## **BRANDNEW: Standards for the Cloud**

- Joint Technical Committee of ISO and IEC, JTC1, Subcommittee 30 (“Distributed Application Platforms and Services”): New standardization projects are another window of opportunity for research project partners, particularly when not just file services but more complex digital industrial services should be addressed in future:
  - Service level agreements,
  - Interoperability and portability,
  - Data and their flow across devices and cloud services,
  - Security issues
- Besides ISO/IEC, a number of standards and specifications from IETF, W3C and OASIS are relevant in the area of Cloud and Web Services.
- For common security requirements standardized protocols and specifications can be used, like for example SSL/TLS (RFC 5246), IPsec (RFC 4301), XML Signature and XML Encryption, SAML, XACML and others.

**NEW**



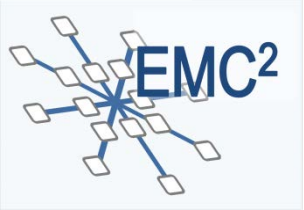
# Open Systems Dependability

IEC 62853/Ed1/CD © IEC:2015



**There is a standard evolving towards open, adaptive systems!**

- Open systems dependability is the ability of a system
  - operated for an extended period of time in a real-world environment to accommodate change in its objectives and environment,
  - to ensure that accountability in regard to the system is continually achieved, and
  - to provide the expected services to users without interruption. It systematizes and puts emphasis on post failure management.
- **Is about adaptive systems as well!**
- Standard provides four process views to achieve these goals:
  - Change Accommodation process view,
  - Accountability Achievement process view,
  - Failure Response process view and
  - Consensus Building process view.
- This International Standard requires a **dependability case** assuring these process views, and five assurance metacases:
  - Internal Consistency and External Consistency,
  - Validity, Adequacy and Confidence Assurance Metacases.



# SoA Standardization (Collaborative Automation, Local Clouds)



## Service Oriented Architecture: Service Interoperability

- Factory description system
- Deployment system
- Configuration system
- Event handler system
- Historian system
- Meta service registry system
- User registry system
- Quality of Service system

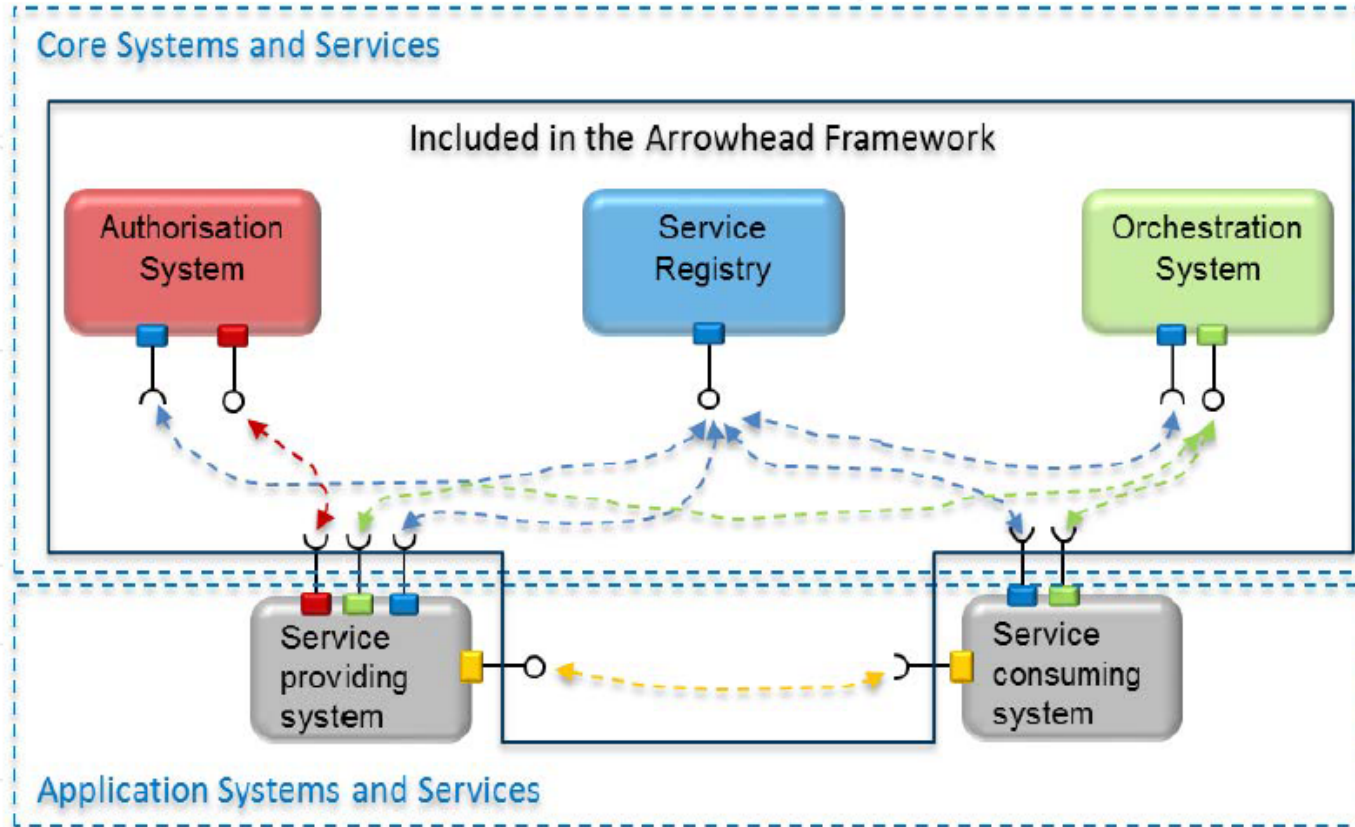
→ **Refer to ARROWHEAD, EMC<sup>2</sup>, ...**

→ **Concerns many Engineering Standards! ARROWHEAD Contributions**

- **Taken up by IETF, IPSO alliance**, COAP protocol and Application semantics
- Information Centric Networks, efficient IoT
- Information Security (other „path“ than ISO, IEC, ISA, ...) – MTTQ secure Server developed
- **W3C, EXI (Efficient XML Interchange) Standard accepted**

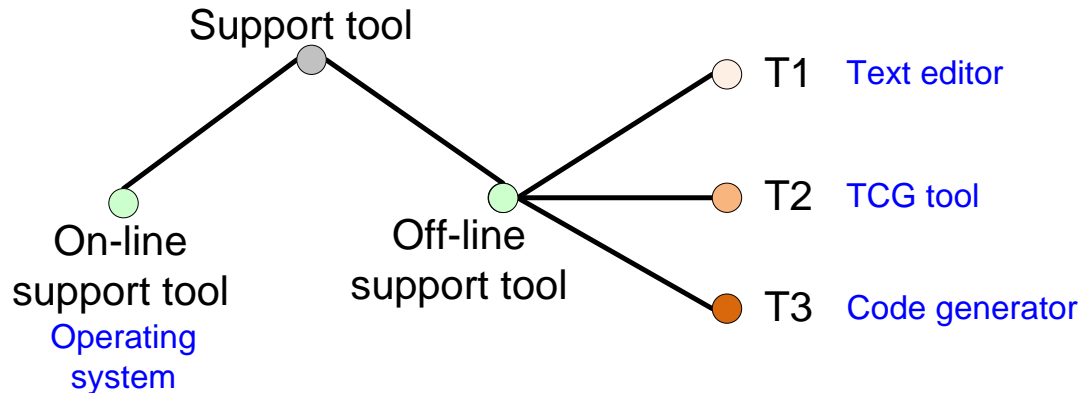
# SoA Standardization

Service Oriented Architecture based framework for integrating multi-vendor applications



# Tool Qualification/Tool Chains

## IEC 61508-3 (single) Tool Qualification



**Clause 7.4.4 in IEC 61508-3:** some general requirements for **off-line support tools** are:

- shall all be selected as a coherent part of the software development activities,
- shall be selected to be integrated to minimize the possibility of introducing human errors,
- selection and use shall be justified.

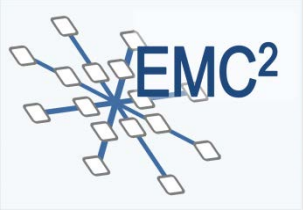
Support tools in classes T2 and T3 shall have

- a specification or product manual that defines the behaviour of the tool together with instructions and constraints on its use.
- to be assessed with the aim to determine the level of reliance that shall be placed on the tool, on potential failure mechanisms that may affect the executable software (T3 only).

Examples of how to achieve this:

- perform software HAZOP, restrict tool functionality, check tool output
- use diverse tools for the same purpose.

**Tool Chain issues insufficiently covered by Functional Safety Standards (SAFECOMP Paper 2012 by partner KTH) → Tool Interoperability!!**



# Tool Interoperability/Tool Chains

## ISO 26262 Tool Qualification



### Qualification requirements of software tools covered by **Clause 11 of Part 8**.

- General Requirements similar to IEC 61508 (documentation, version handling)
- A certain confidence is required in that these tools shall achieve:
  - the risk of systematic faults in the developed product due to malfunctions of the software tool leading to erroneous outputs is minimized
  - the (SW) development process is adequate with respect to compliance with ISO 26262, if activities or tasks required by ISO 26262 rely on the correct functioning of the tool.
- Two metrics for confidence, needs analysis of the tool and its role in the development chain:
- **TI (Tool Impact):** Can the malfunctioning tool and its corresponding output introduce or fail to detect errors in a safety-related item or element being developed (TI1 if no error/detection failure possible, supported by argument, else TI2)
- **TD (Tool error Detection):** confidence in preventing or detecting such errors in the output of the tool
  - a.) **TD1:** high confidence that malfunction/erroneous output will be prevented or detected
  - b.) **TD2** medium confidence
  - c.) **TD3** else

Qualification can be done independently from development, but confidence level has to be confirmed



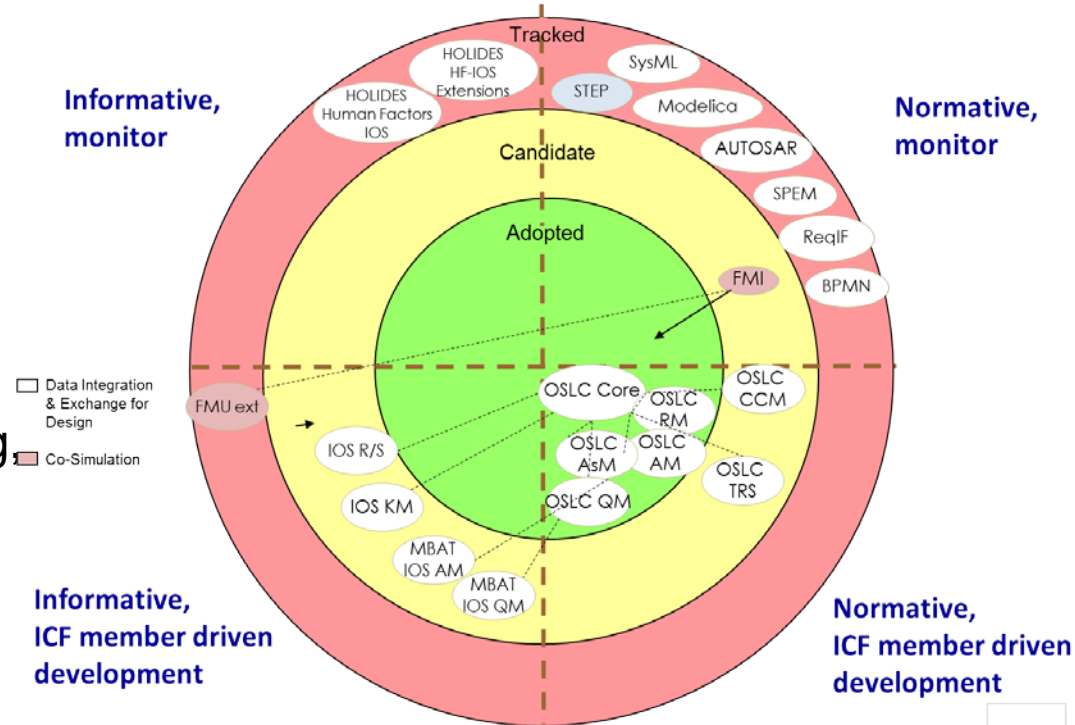
# The CP-SETIS – IOS Approach

## Interoperability leads to „Multi-Standards“

What is different, what is applicable?

Findings of CP-SETIS:

- IOS cannot be a single standard, specification or guideline
- IOS is rather a set of standards, guidelines and specifications
- It consists of items of different maturity level
- IOS defines a process of tracking, adoption and enhancement for standardization/ specification candidates

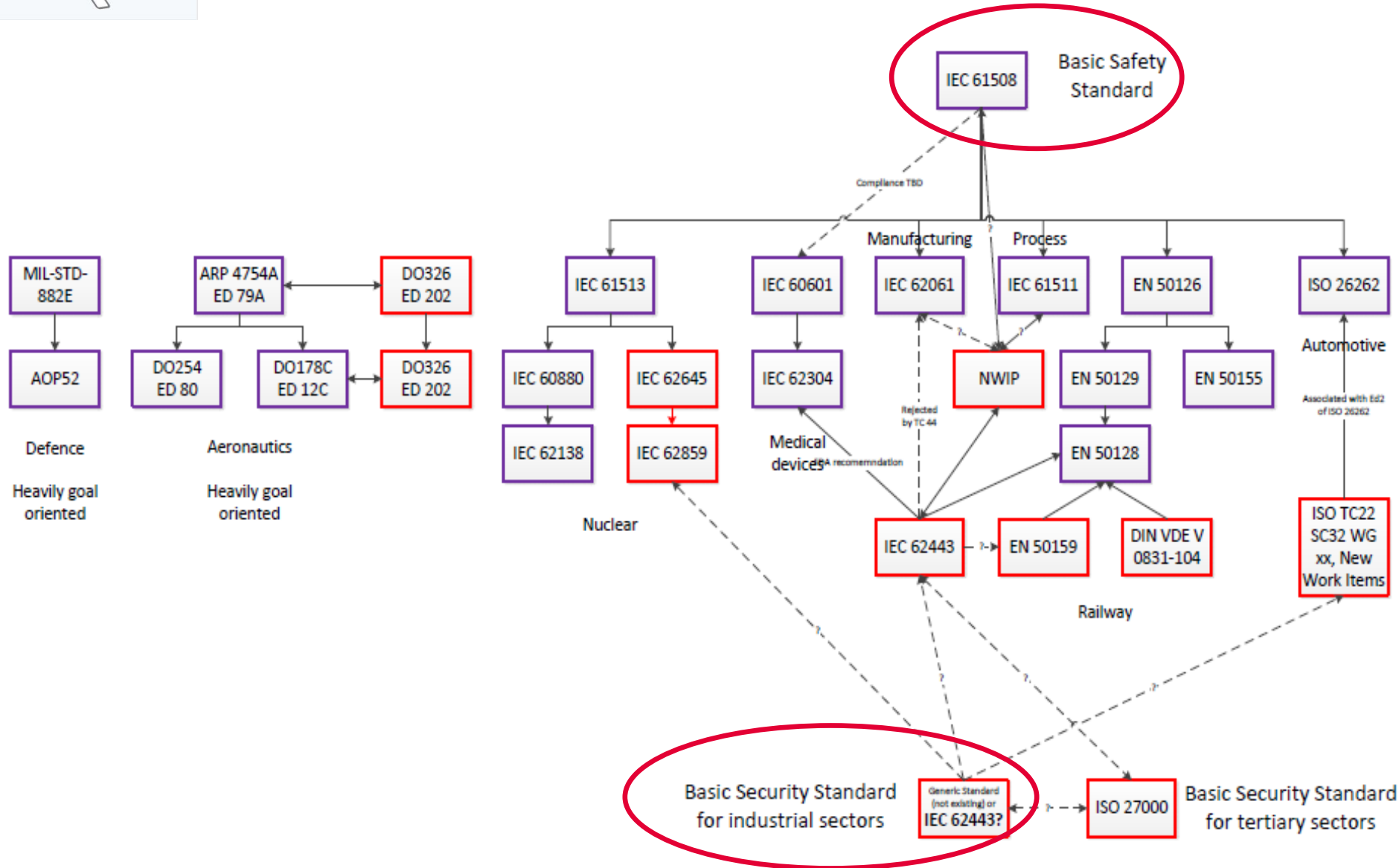


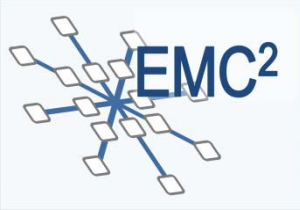
The proposed approach:

- Creation of the ICF (Interoperability Coordination Forum) (= stakeholders)
- Finding a suitable Sustainable Hosting Structure

**NEW: Can the „Multi-Standard“ Concept be generalized to resolve complex standardization issues where groups of consistent standards would be required?**

# Safety & Security Standards Framework (Multi-Standard? Example by Bertrand Rique)





# Multi-concern Issues: Multi-Standard? How to align all this?



**BRANDNEW:** IEC TC65 Ad Hoc Groups – Safety, Reliability, Cybersecurity, Smart Manufacturing, Human Factors, .... (Examples)

- **IEC TC65 AHG1 – now WG 20:** “Framework towards coordinating safety, security (in industrial automation): New Work Item started for a TS (“Industrial-process measurement, control and automation - Framework to bridge the requirements for safety and security”) – **IEC TS 63069**
- **IEC TC65 AHG2:** “Reliability of Automation Devices and Systems”, looking at the demand of reliability design, test, verification and operational life of (safety related) automation devices and systems as handled by IEC TC65.
- **IEC TC65 AHG3:** “Smart Manufacturing Framework and System Architecture” (Kick-off April 2016); will address the issues of highly interconnected industrial automation systems for smart manufacturing in a multi-concern manner (**RAMI4.0**).
- **Task Force “Standards Landscape” → JWG21 ISO TC184/IEC TC65 AHG3, Smart Manufacturing Reference Models**
- **IEC SC65E** (Devices and integration in enterprise systems) **AHG1 (started 2016)** “Smart manufacturing information models”. This subcommittee SC65E looks at enterprise management systems from top level down to devices.  
Main concern: **interoperability** of models and data exchanged, how managed by smart items in enterprise context (safety, security and dependability will play an important role)
- **IEC SC65A WG 17: Human factors – Functional Safety (IEC TR 62879)**

**NEW**

## „Human Factors & Functional Safety = Multi-Concern“

- Start of work on IEC TS 62879 Ed. 1 – Dr. C. Sandrom (UK) → left 2014
- **Motto: Don't forget the Human !!**
- Concept: to be written in a format that it could become easily integrated in a later IEC 61508 Edition (section structure etc.)

- Restart 2016 New convenor:  
Dr. Harald Schaub (IABG, DE)

- Consider cognitive and anthropomorphic factors

- **Whole Life Cycle Issue!**  
**From Concept to Operations, Maintenance, Disposal,**

- **Safety & Security?**

- **Usability**

- **Part of “Multi-Standard”**

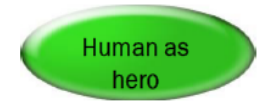
### Human Factors and IEC 61508

– Part 1: HF Process (Normative)

– Part 2: HF Guidance (Informative)

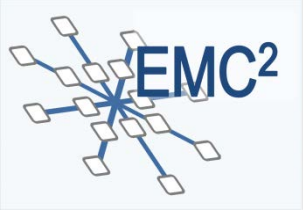


- Slips
- Lapses
- Mistakes
- Violations



- Adjustments
- Compensations
- Recoveries
- Improvisations

**Cybersecurity Threats = Human Factor?**



# Thank You for Your Kind Attention !

Contact:

[erwin.schoitsch@ait.ac.at](mailto:erwin.schoitsch@ait.ac.at)

[christoph.schmittner.fl@ait.ac.at](mailto:christoph.schmittner.fl@ait.ac.at)