ARTEMIS Technology Conference 2016

EMC^2 - Workshop

Madrid, October 06, 2016

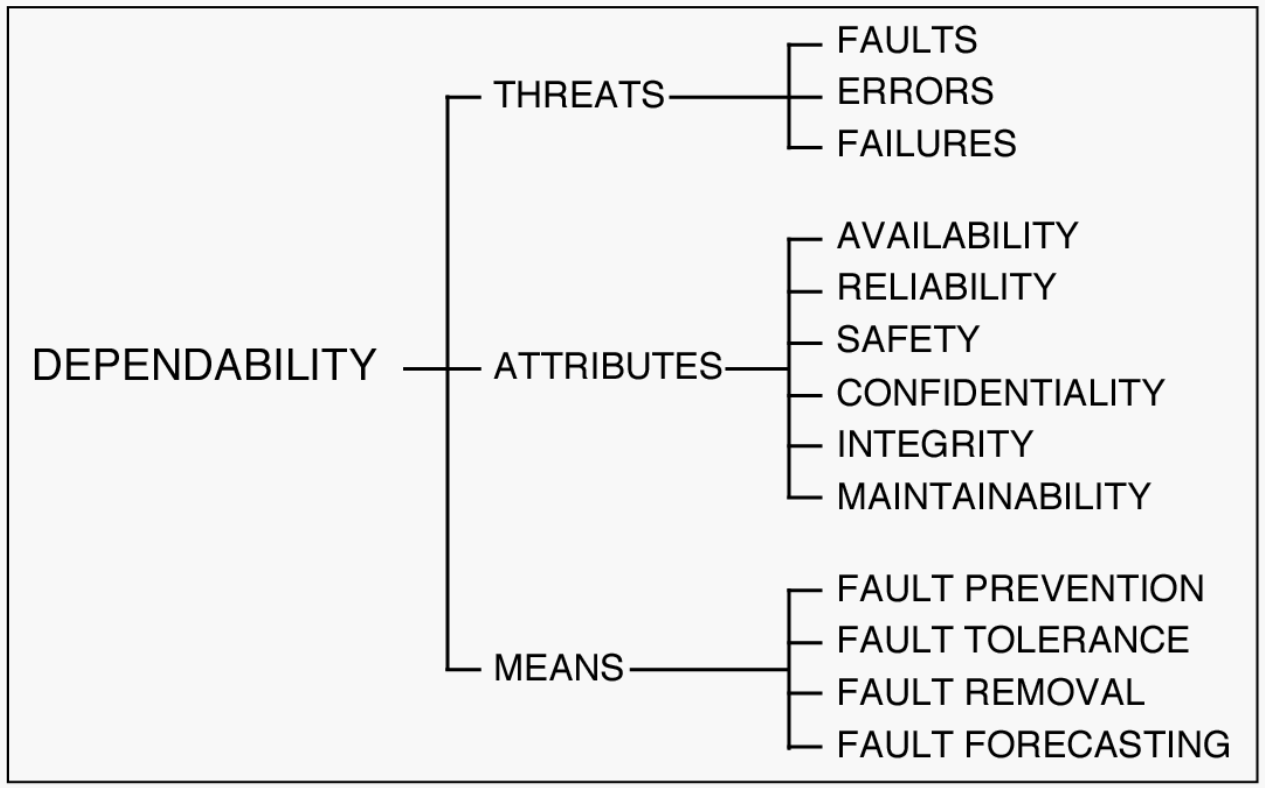
Ongoing Standardization Work: Safety & Security & others

Erwin Schoitsch
Erwin.schoitsch@ait.ac.at

Christoph Schmittner
Christoph.schmittner.fl@ait.ac.at

Dependability – a holistic umbrella term „multi-concern“

Dependability – Basic Concepts and Terminology (Dependability Tree) (J.-C. Laprie, A. Avizienis, H. Kopetz, Udo Voges, T. Anderson, et.al.)



DEPENDABILITY

- THREATS
  - FAULTS
  - ERRORS
  - FAILURES
- ATTRIBUTES
  - AVAILABILITY
  - RELIABILITY
  - SAFETY
  - CONFIDENTIALITY
  - INTEGRITY
  - MAINTAINABILITY
- MEANS
  - FAULT PREVENTION
  - FAULT TOLERANCE
  - FAULT REMOVAL
  - FAULT FORECASTING

Fault – error – failure – fault - …… in SoS

Security = CIA

Example from IEC TC 65: Families of Standards

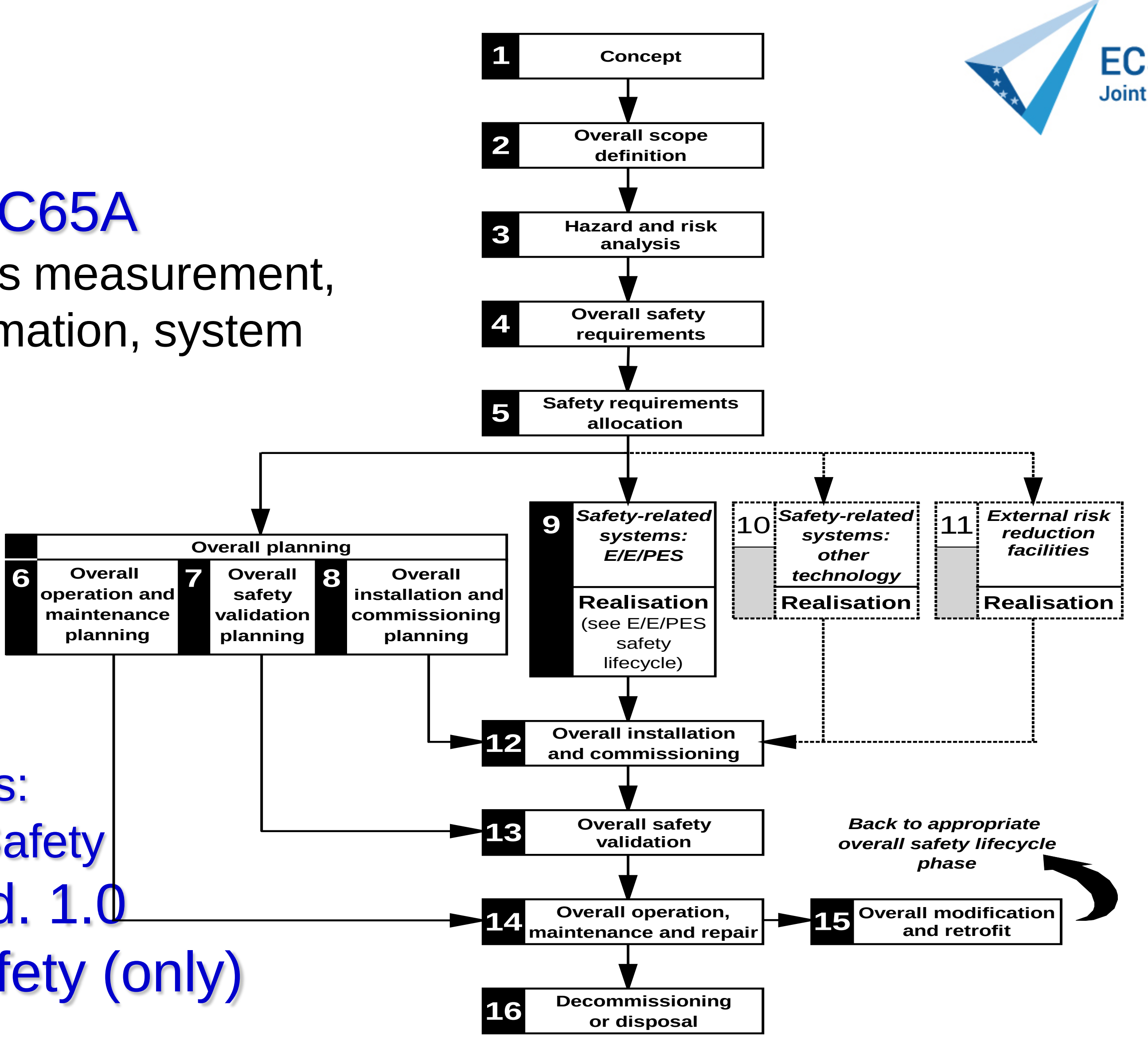
Consistent mapping from enterprise top level down to device

- 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 TC65 – SC65A

Industrial-process measurement, control and automation, system aspects


1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety-related systems: E/E/PES
Realisation (see E/E/PES safety lifecycle)
10 Safety-related systems: other technology
Realisation
11 External risk reduction facilities
Realisation
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal

Primary concerns: Functionality & Safety

IEC 61508, Ed. 1.0

Looking at Safety (only)

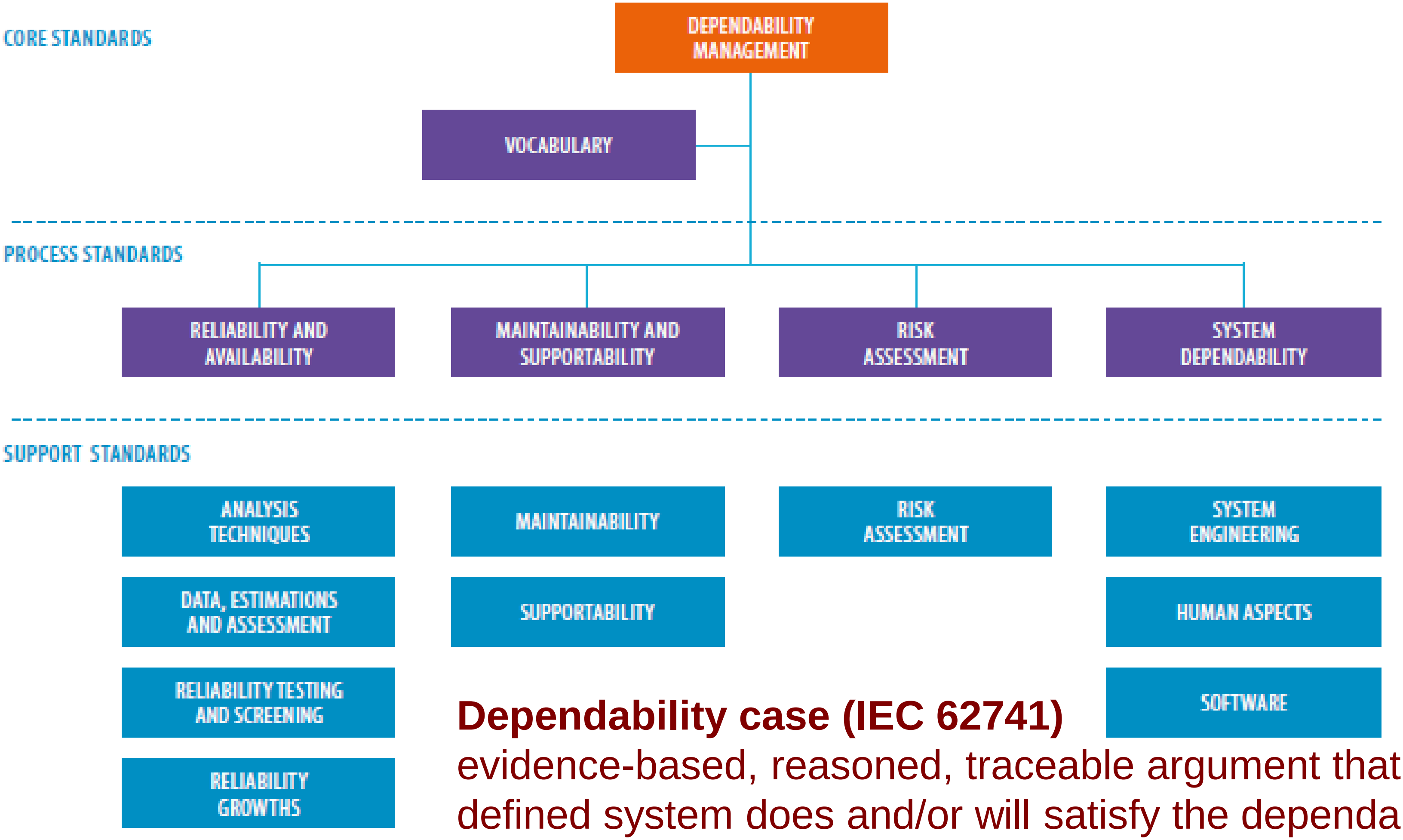
NOTE 1 Activities relating to ***verification***, ***management of functional safety*** and ***functional safety assessment*** are not shown for reasons of clarity but are relevent to all overall, E/E/PES and software safety lifecycle phases.

NOTE 2 The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 Parts 2 and 3 deal with box 9 (realisation) but they also deal, where onic (hardware and software) aspects of boxes 13, 14 and 15.

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)



Dependability case (IEC 62741)

evidence-based, reasoned, traceable argument that a defined system does and/or will satisfy the dependability requirements

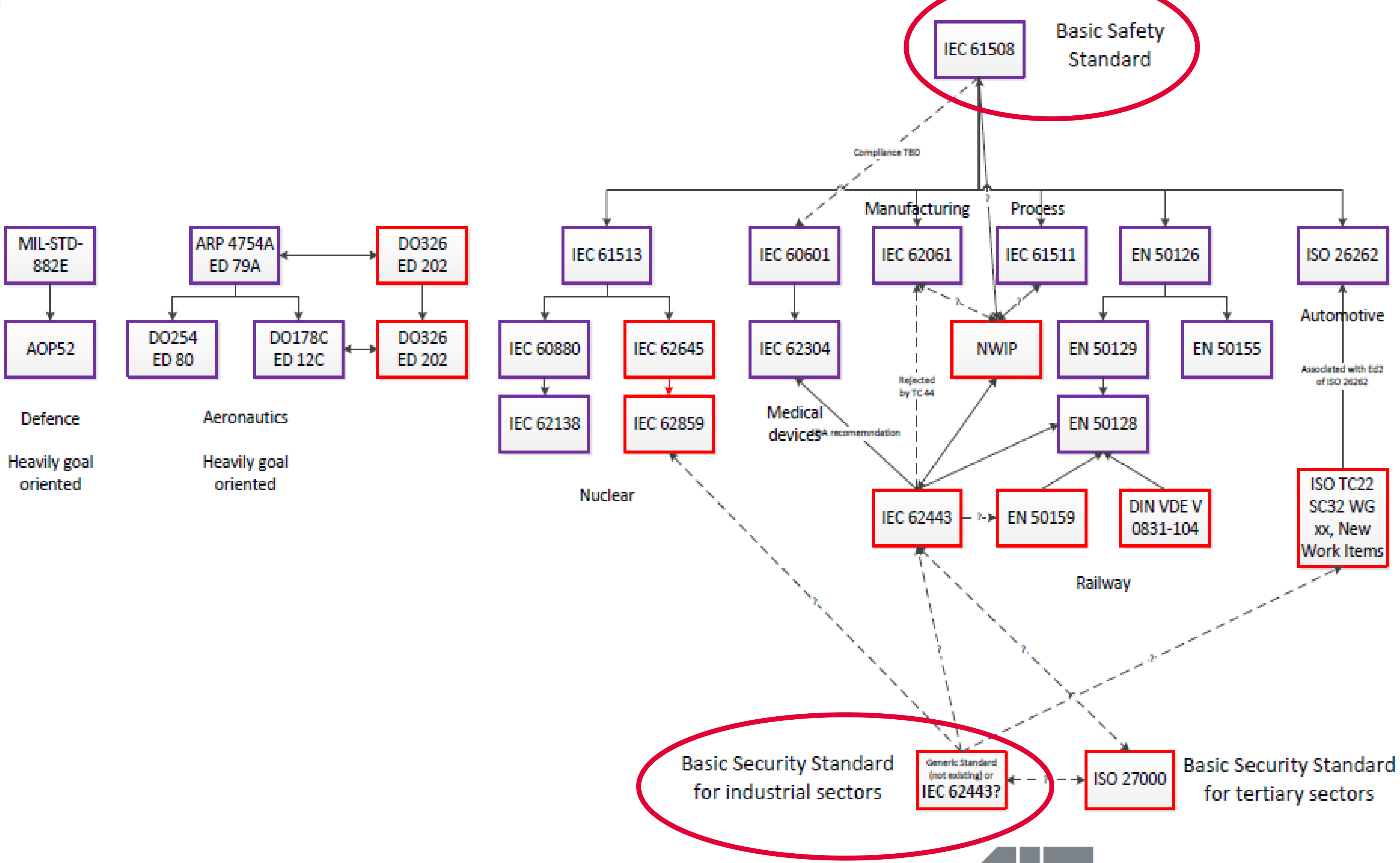
IEC 62443 status – in close cooperation with ISA 99

General	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 💡
Policies & Procedures	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 📄
System	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 📄	
Component	ISA-62443-4-1 Product development requirements 👥	ISA-62443-4-2 Technical security requirements for IACS components 👥		

Status Key

📄 Published	✏ In development	💡 Planned
🔍 Published (under review)	👥 Out for comment/vote	

Safety & Security Standards Framework (Bertrand Rique)



IEC 61508

Basic Safety Standard

Compliance TBD

Manufacturing

Process

MIL-STD-882E

AOP52

Defence

Heavily goal oriented

ARP 4754A ED 79A

DO326 ED 202

DO254 ED 80

DO178C ED 12C

DO326 ED 202

Aeronautics

Heavily goal oriented

IEC 61513

IEC 60880

IEC 62645

IEC 62138

IEC 62859

Nuclear

IEC 60601

IEC 62304

Medical devices

ISA recommendation

IEC 62061

Rejected by TC 44

IEC 61511

NWIP

EN 50126

EN 50129

EN 50155

EN 50128

IEC 62443

EN 50159

DIN VDE V 0831-104

Railway

ISO 26262

Automotive

Associated with Ed2 of ISO 26262

ISO TC22 SC32 WG xx, New Work Items

Basic Security Standard for industrial sectors

Generic Standard (not existing) or IEC 62443?

ISO 27000

Basic Security Standard for tertiary sectors

IEC TC65 WG10 (IEC 62443) and ISA 99 collaboration

- IEC TC65 and ISA99 collaborate on the development and publication of the 62443 standard
  - There are some differences between the IEC and ISA versions that must be addressed
  - Some parts originate in TC65 and others in ISA99
  - There is very weak coordination between parts (rely on common membership)
- Asynchronous development of parts creates significant differences in technical approach
- Only a few parts have reached the IS stage, some have reached the CDV stage, the rest are still a work in progress

ISA 99 IACS Security Standardization

Industrial Automation and Control Systems (IACS)

COMMON

- ISA-99.01.01: Terminology, Concepts and Models
- ISA-TR99.01.02: Master Glossary of Terms and Abbreviations
- ISA-99-01.03: System Security Compliance Metrics
- ISA-TR99-01.04: IACS Security Lifecycle and Use Case

SECURITY PROGRAMME

- ISA-99.02.01: Establishing an IACS Security Program
- ISA-99.02.02: Operating an IACS Security Program Impl
- ISA-TR99.02.03: Patch Management in the IACS Environment
- ISA-99.02.04: Certification of IACS Supplier security policies and practices

TECHNICAL - COMPONENTS

- ISA-99-04.01: Product Development Requirements
- ISA-99-04-02: Technical security requirements for IACS components

ISA founded ISCI – ISA Security Compliance Institute, for certification according to IEC 62443; defined an Embedded Device Security Assurance Scheme (2014).

Europ. IACS Components Cyber-Security Compliance and Certification Scheme (proposed by JRC ISPRA, ERNCIP, Industrial Control Systems and Smart Grids)

Safety & Cybersecurity in existing Standards and Committees

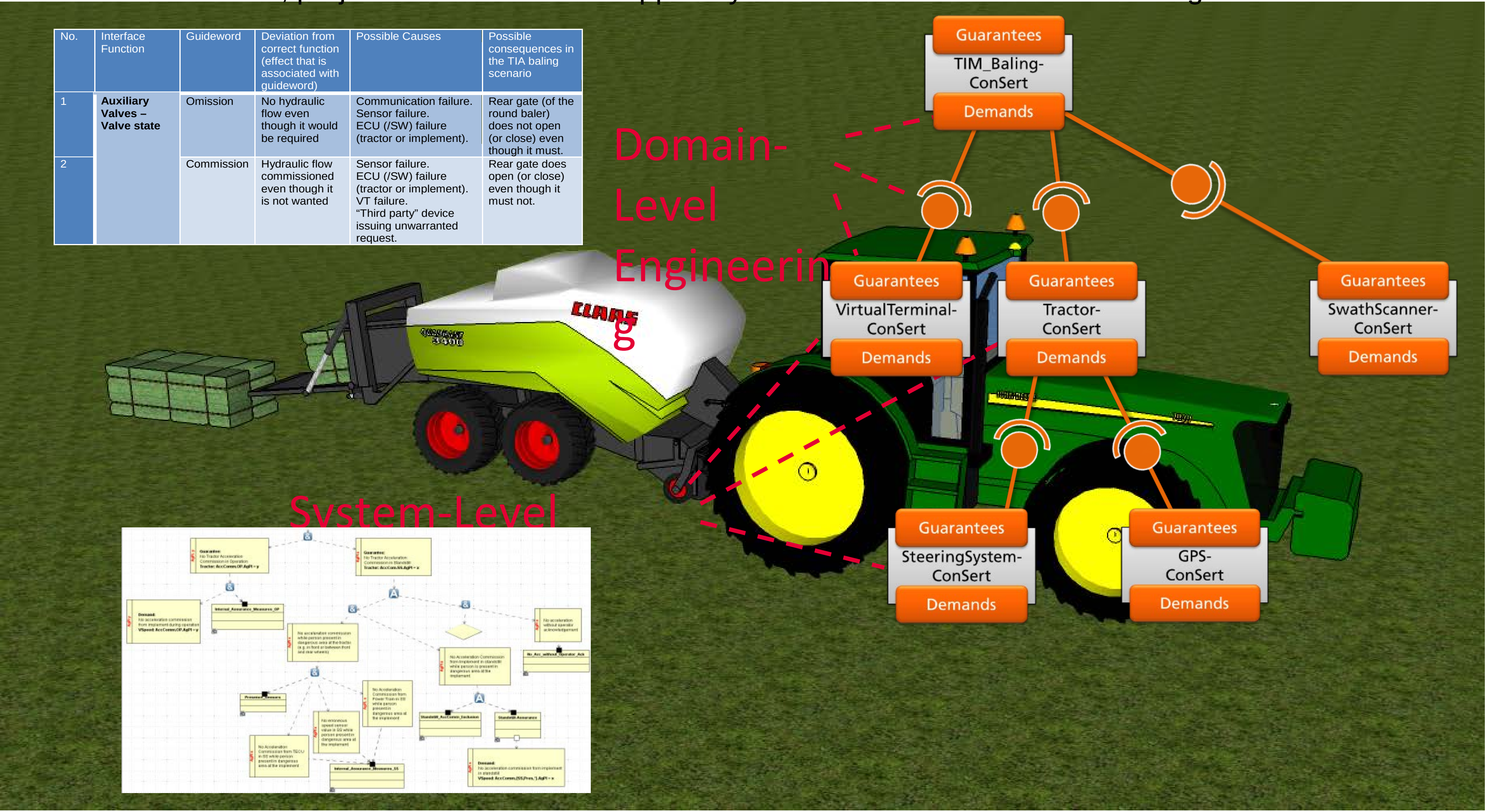
- **IEC 61508-3** Ed 3.0 preparation: Security aware safety guidelines – first proposals for IEC 61508-3, needs consideration in part 1 and 2 as well!!
- **ISO 26262**, Ed. 2.0: AIT proposal presented Jan. 2015 to consider security aware safety issues particularly because of "connected car" and "highly 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)
- **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**

EMC²: 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)

Adapting a System – all valid contracts (conserts=conditional contracts), subsequent incremental Certification at run-time – **also for security updates (Safety=never change, security=frequent updates)**

© Fraunhofer IESE, project EMC² - different support systems attached to same tractor engine



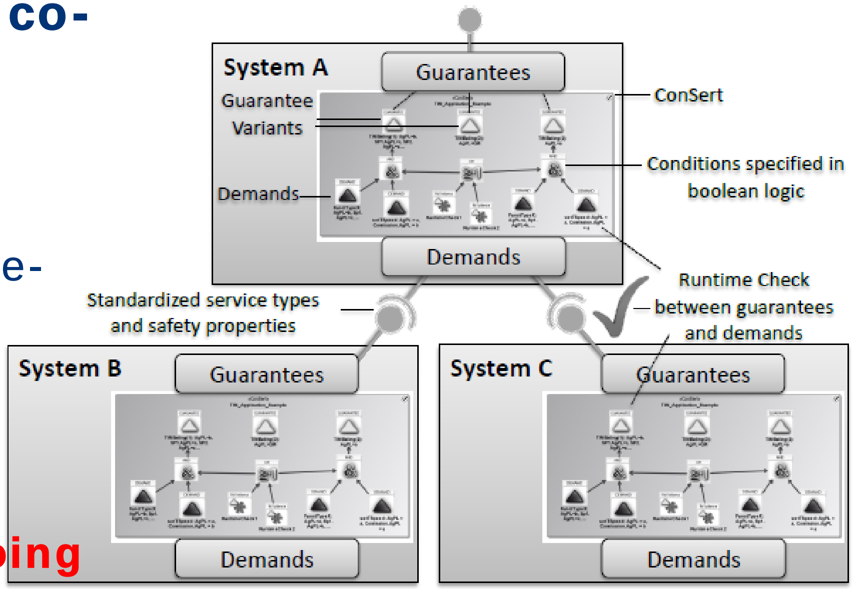
No.	Interface Function	Guideword	Deviation from correct function (effect that is associated with guideword)	Possible Causes	Possible consequences in the TIA baling scenario
1	**Auxiliary Valves – Valve state**	Omission	No hydraulic flow even though it would be required	Communication failure. Sensor failure. 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
Engineerin
g
Guarantees
TIM_Baling-ConSert
Demands
Guarantees
VirtualTerminal-ConSert
Demands
Guarantees
Tractor-ConSert
Demands
Guarantees
SwathScanner-ConSert
Demands
Guarantees
SteeringSystem-ConSert
Demands
Guarantees
GPS-ConSert
Demands
System-Level
Guarantee: No Tractor Acceleration Commission in Operation Tractor: AccComm.OP.AgPl = y
Guarantee: No Tractor Acceleration Commission in Standstill Tractor: AccComm.SS.AgPl = x
Demand: No acceleration commission from implement during operation VSpeed: AccComm.OP.AgPl = y
Internal_Assurance_Measures_OP
No acceleration commission while person present in dangerous area at the tractor (e.g. in front or between front and rear wheels)
No acceleration without operator acknowledgement
No_Acc_without_Operator_Ack
No Acceleration Commission from Implement in standstill while person is present in dangerous area at the implement
Presence_Sensors
No Acceleration Commission from Power Train in SS while person present in dangerous area at the implement
No erroneous speed sensor value in SS while person present in dangerous area at the implement
No Acceleration Commission from TECU in SS while person present in dangerous area at the implement
Internal_Assurance_Measures_SS
Standstill_AccComm_Exclusion
Standstill-Assurance
Demand: No acceleration commission from implement in standstill VSpeed: AccComm.(SS,Pres.*).AgPl = x

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
- ➢ **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**

IEC TC65 Multi-concern: How to align all this?

BRANDNEW: Ad Hoc Groups

- **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); this group will address the issues of highly interconnected industrial automation systems for smart manufacturing in a multi-concern manner.
- **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 (second meeting July 18-20 in Frankfurt, safety, security and dependability will play an important role)

Ongoing work – initial results

- **IEC TC65 AHG1 – report with recommendations to IEC TC65 Plenary in Dalian, 2015: „**recommendations about a framework toward coordinating standards of safety and security for industrial settings. This coordination considers both normal operating conditions and emergency situations. It will identify and assess the intersection between safety and security"; "The intent is not to develop new standards, but rather to profile and make recommendations to better co-ordinate the use of existing standards".

  → **Result: Start of a new WG20 developing a TS "Framework to bridge the requirements for safety and security" IEC TS 63069**
  Key chapters proposed (showing the direction):

  - □ Chapter 5: Basic recommendations for bridging safety and cyber security standards
  - □ Chapter 6: Recommendations for applying IEC 61508 and IEC62443 simultaneously

- ***Unfortunately:*** *Still re-discussion of scope (in detail), "Who are the stakeholders to address?", "What to bridge: IEC 61508 or just 61511 with IEC 62443?" (our intent: make a generic safety & security TS as template for domain specific ones, like IEC 61508 for domains in functional safety)*

Ongoing work – initial results

Motivation IEC TC65 AHG2:

- **It is difficult to evaluate the reliability of TC65 products because of the lack of related standards.**
- **General evaluation methods of TC56 can't accurately evaluate TC65 products, they are method-oriented, not product-oriented**
- **Therefore, we should develop reliability standards for measurement and control devices in TC65.**

IEC TC65 AHG2, meeting in Vienna **begin of June 2016:**
"Reliability of Automation Devices and Systems"

→ Major preliminary result (our intention): not to consider reliability as such and compete with IEC TC56 (e.g. not look at/calculate reliability of components) but rather to focus on the impact on systems built from such components and devices as industrial automation and control systems (as is the scope of TC65) → holistic approach, architecture, integration and interoperability aspects → closer to multi-concern!

IEC SC65A, WG 17 (was IEC AHG16) „Human Factors and Functional Safety“

Motivation: Don‘t forget the Humans!

- Safety of aircraft: over 90% of incidents in UK airspace during 1997 were caused by human factors; human failures are the dominant causal factor in many domains .
- General safety requirements in IEC 61508 related to Human Factors, but no detailed Human Factors guidance provided
- Survey undertaken by AHG 16, report issued for SC65A Plenary Sept. 2012
- Decision: SC65A WG 17 established to provide specific, detailed Human Factors processes and procedures for IEC61508 to address safety-related risks relating to Organizations, People, Procedures and Equipment and to address their impact upon Functional Safety.

Kegworth

Herald of Free Enterprise

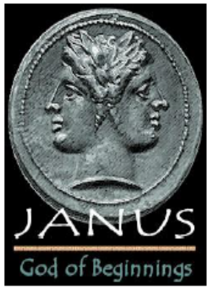
IEC TC65 SC65A WG 17 – IEC TS 62879 – Now Restart! „Human Factors and Functional Safety“

- *Start of work on IEC TS 62879 Ed. 1 – Human factors and functional safety (2013), conveynor Dr. C. Sandrom (UK)*
- *Concept: to be written in a format that it could become easily integrated in a later IEC 61508 Edition (section structure etc.)*
- *Sandrom left 2014 → Delay in schedule*
- *New convenor assigned: Dr. Harald Schaub (IABG, DE)*
- *Restart 2016 TWO DAYS AGO*
- *Consider cognitive and anthropomorphic factors*
- *Whole Life Cycle Issue! From Concept to Operations, Maintenance, Disposal,*
- *Safety & Security?*

Human Factors and IEC 61508
– Part 1: HF Process (Normative)
– Part 2: HF Guidance (Informative)

Human as hazard

- Slips
- Lapses
- Mistakes
- Violations



Human as hero

- Adjustments
- Compensations
- Recoveries
- Improvisations

Cybersecurity Threats = Human Factor?

Combined Safety & Security approaches: Railways

- EN 50129 does not define security threats and countermeasures explicitly, but requires addressing the prevention of unauthorized access in the safety case.
- **BUT:** Safety systems need to protect against operator errors, random failures and foreseeable misuse.
- So it could be expected that safety systems would fulfil SL1 of IEC 62443.
- IEC 62443 contains 41 requirements related to SL1, of which
  - □ the majority is explicitly covered by EN 50129 and EN 50159
  - □ some are usually fulfilled but not explicitly covered
  - □ a few are not in the scope of safety
- **DIN VDE V 0831-104:** includes the missing SL1 requirements in the safety system‘s requirements, and (in future) add these requirements in EN 50129 (German proposal)
- What about higher SLs? (SL 2 – 4 ?) – Open question (adapt IEC 62443?)

IEC 62859 Nuclear Power Plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity

5.2 Fundamental Principles

- **Cybersecurity** shall **not interfere** with the **safety objectives** of the plant and shall **protect their realisation**. It shall not compromise the efficiency of the diversity and defence-in depth features…
- **Cybersecurity requirements** impacting the overall I&C architecture shall be **addressed**…
- Implementation of **cybersecurity features** shall **not adversely impact** the required performance (including response time), effectiveness, reliability or operation **of functions** important to **safety**.
- The **failure modes and consequences** of cybersecurity features on the functions important to safety shall be **analyzed** and **taken into account**.
- Any **architectural property or characteristics** initially designed for safety reason (e.g., independence between systems), and later considered as a potential cybersecurity counter-measure … should be re-examined on purpose … to confirm its cybersecurity added-value

NEW Project: "Nuclear power plants - Instrumentation and control-systems – **Security controls**"

Gaps in ISO 26262 Functional Safety Standard

- ISO 26262 works on a single vehicle level
  - □ Hazards are identified at the vehicle level and not an systems of vehicle level
- ISO 26262 excludes any security threats as causes for failures and hazards
  - □ Although there are a few terms which could point to security they are aimed at reckless driver
- ISO 26262 includes controllability in the risk assessment, which cannot be applicable for automated vehicles
  - □ How can it be ensured that a driver can override all automated functions in all relevant situations and failure modes?
- Ignore security issues? Separate completely safety and security?

Focus Safety & Cybersecurity WHY?

- Chrysler Jeep: Manipulate safety critical elements in a vehicle via remote connectivity
- Corvette: Control brakes via insurance OBD dongle
- Tesla: Remote manipulation of instruments or drive systems
- VW: Disable Airbags via manipulated USB flash drive
- NISSAN LEAF electric cars hack vulnerability disclosed (Remote Access to charging, climate control, driving history - Vulnerable Service deactivated)
- German steel mill suffered "massive damage" following a cyber attack on the plant's network

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
- 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 CD 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)

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!)

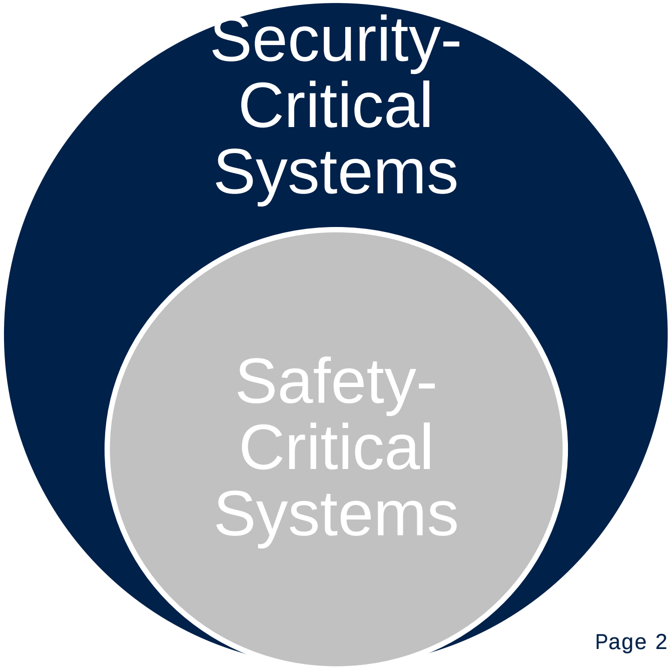
Foundation for further (standard development) activities in vehicle cybersecurity

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

Scope of Application for SAE J3061

- J3061 should be applied to all automotive systems that are responsible for functions that are ASIL (Automotive Safety Integrity Level) rated per ISO 26262, or that are responsible for functions associated with:
  - □ Propulsion, steering, braking, security, safety
- J3061 should be applied to all automotive systems that handle Personally Indentifiable Information (PII)

  (Privacy)
- In addition for systems which may be cybersecurity-critical an initial short assessment of threats and risks can be conducted



SAE J3061 – System Safety

- System Safety considers potential hazards to identify safety mechanisms that can be integrated into the design to address the causes of the potential hazards
  - Potential hazards and causes are more readily identified
  - Appropriate action to mitigate the potential consequences, or to eliminate the potential hazards all together can be taken
  - Causes of hazards based knowledge of system, components, and interactions
  - Focus on sub-systems

SAE J3061 – System Cybersecurity

- System cybersecurity considers potential threats posed by a malicious attacker whose goal is to cause harm, wreak havoc, gain financial benefits, or simply to gain notoriety
  - Cyber Security threats are more difficult to address than potential safety hazards
  - More difficult to try to anticipate the exact moves an attacker may take in order to add appropriate Security Controls to protect against attacker’s options.
  - Causes maybe unknown
  - Additional factors in risk assessment: attacker’s experience level, attacker’s access, attacker’s need for special equipment
  - Focus on sub-systems AND electrical architecture (i.e. possible access to safety-critical areas through non-safety-critical area, i.e. CD player)

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.:

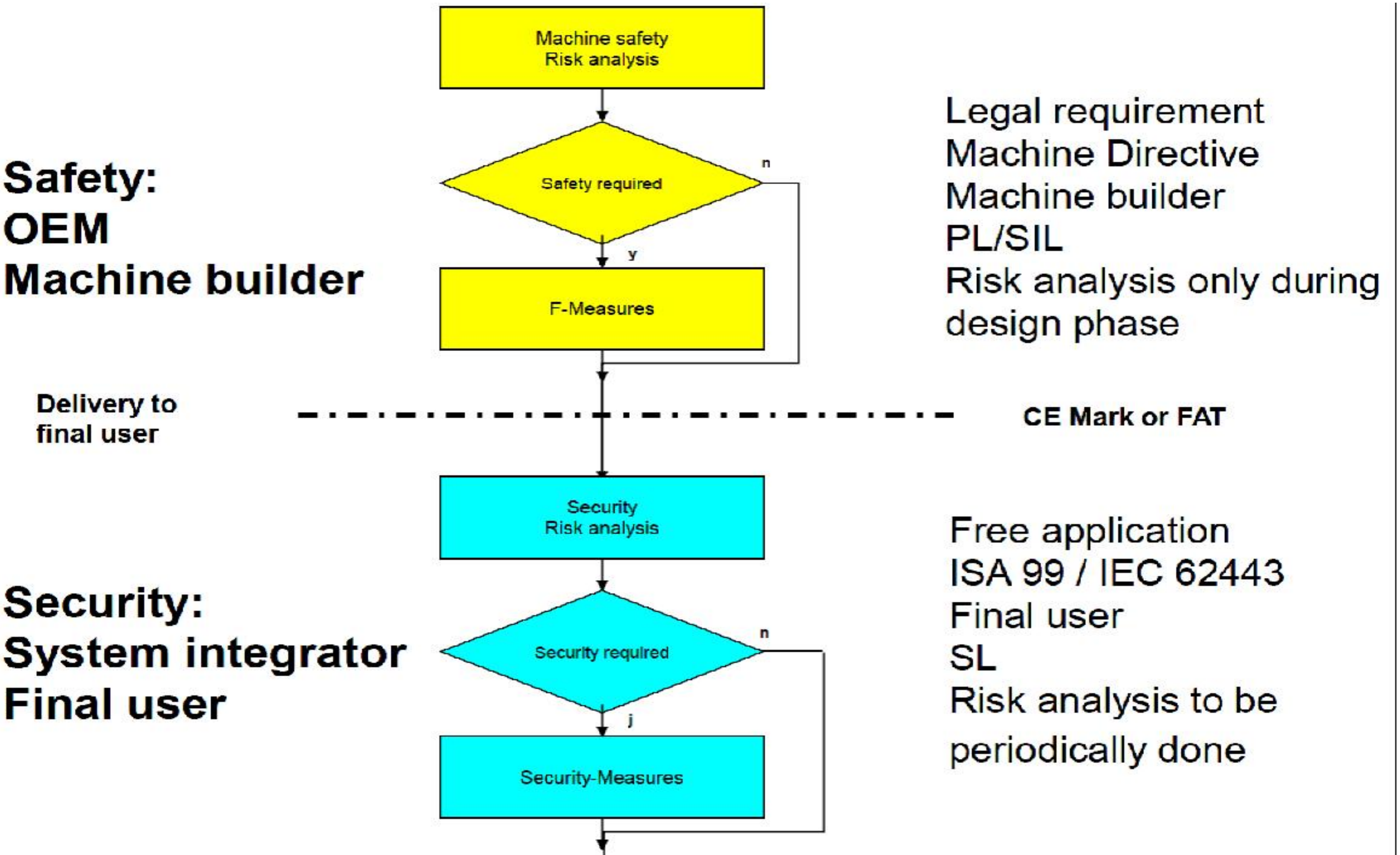
- German proposal tends towards an independent Cybersecurity Standard, not considering the safety impact as basis,
- SAE proposal takes up both: a safety-related part where both sides (safety and security) are taken into account following ISO 26262 life cycles, and a security related part, where issues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

The Austrian Committee commented:

While cybersecurity may require some extensions, especially in the maintenance and operations phase, it should, in our opinion, in general follow the ISO26262 lifecycle. Safety and Security is required for issues like advanced driver assistance systems with communication features.

While additional issues are also relevant for security, the primary goal are safe vehicles. The approach proposed in SAE J3061, to describe a combined process for safety and security critical systems and only use a stand-alone cybersecurity process for systems without safety relevance, should be adapted for the new standard.

IEC – TC 44, Safety of Machinery – first ideas: No holistic system approach? →ISA99 against separating requirements



Safety:
OEM
Machine builder

Legal requirement
Machine Directive
Machine builder
PL/SIL
Risk analysis only during design phase

FAT – Factory Acceptance Test

Security:
System integrator
Final user

Free application
ISA 99 / IEC 62443
Final user
SL
Risk analysis to be periodically done

NOW: Reasonable Restart (NP): „Security aspects related to functional safety of safety-related control (safe machine operation despite cybersecurity threats)"

New Issues: Cloud and IoT

- **BRANDNEW:**

Standards for the Cloud

- The Joint Technical Committee of ISO and IEC, JTC1, Subcommitte 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

New Issues: Cloud and IoT

- **BRANDNEW:**

Standards for the Cloud – evolving standardization projects

- New standardization projects on more complex digital industrial services:
  - 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.
- Addressing many 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.

Standardization: Cloud and IoT

- **BRANDNEW:**

AIOTI: Alliance for Internet of Things Innovation → becoming a cPPP

- IoT becomes a more and more intriguing issue.
- 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.
- 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

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

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

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

AIOTI (upcoming cPPP) with 13 WGs: Some results: Have influenced standards evolvement towards better IoT usability:

- FI-WARE now includes “Generic Enablers” for Future-Internet/IoT
- Cybersecurity, privacy, identification, traceability, anonymization, semantic interoperability, interoperability/coexistence testing, performance characterization and scalability, auto-configurisation, 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

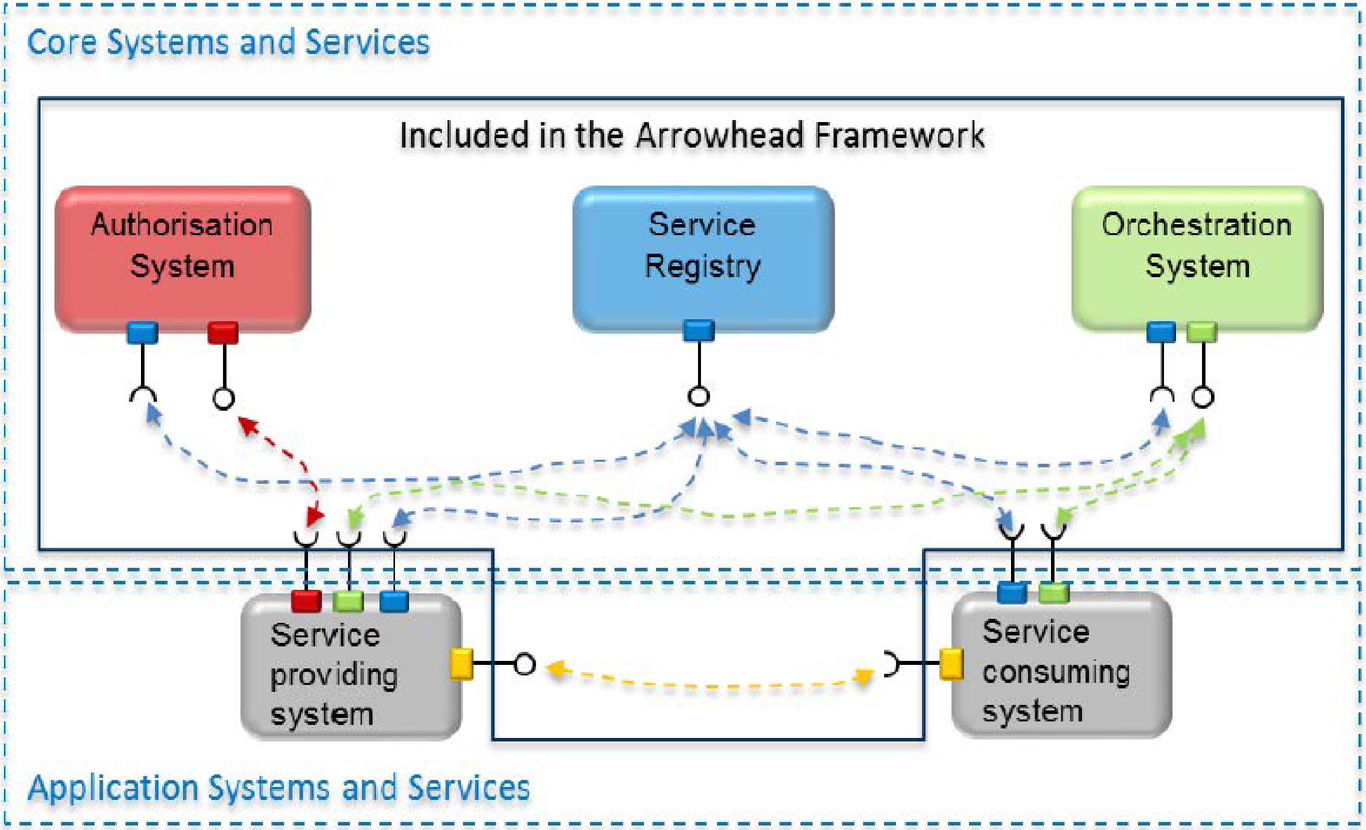
SoA Standardization (ARROWHEAD Contribution, Local Clouds)

- 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 EMC² WP1 presentation this morning!**

SoA Standardization

Service Oriented Architecture based framework for integrating multi-vendor applications



www.arrowhead.eu

ISO IoT Standards 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

Open Systems Dependability

IEC 62853/Ed1/CD © IEC:2015

NEW:There is a standard eveolving towards open, adaptive systems!

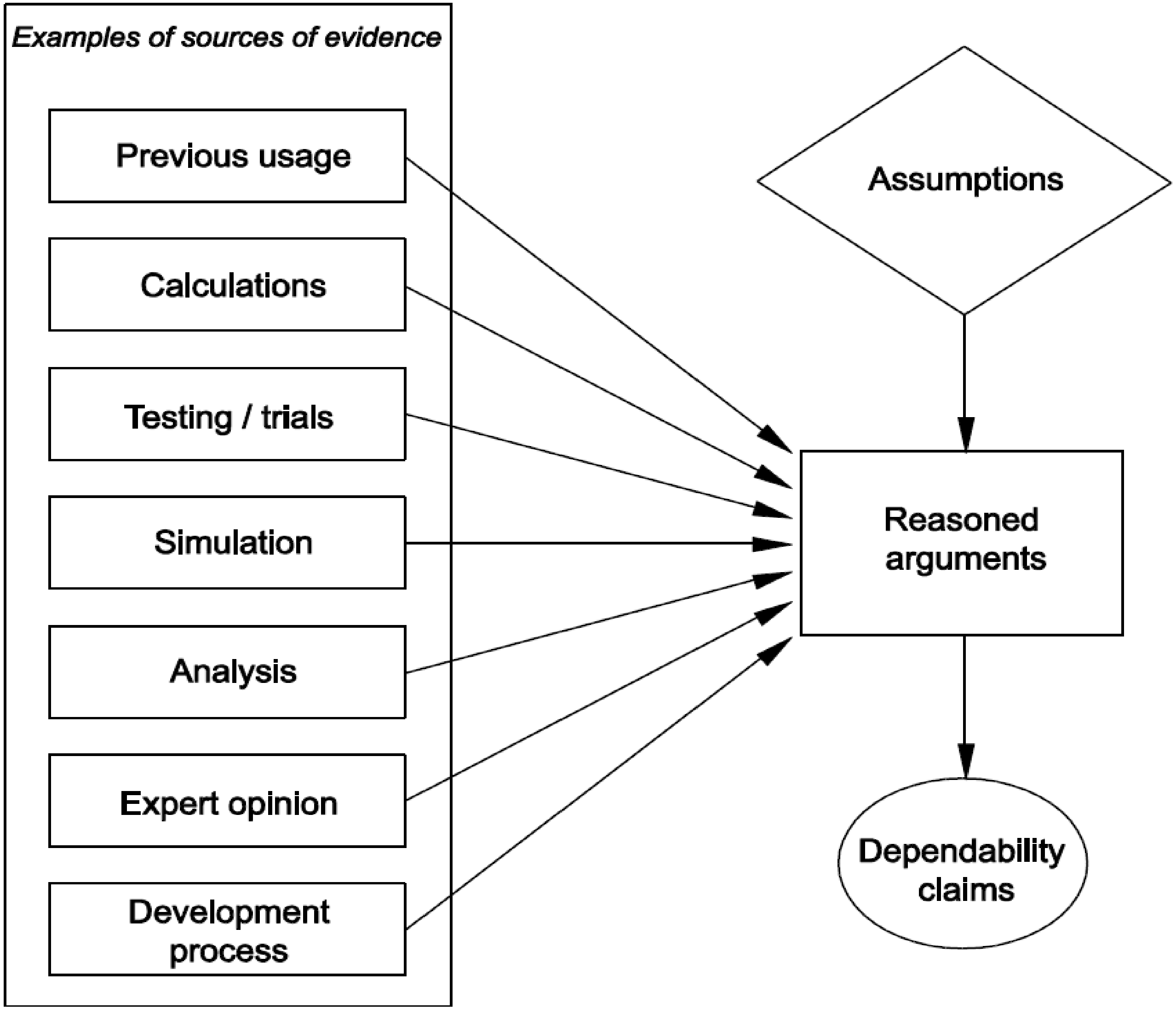
- Open systems dependability is the ability of a system
  - operated for an extended period of time in a real-world environment to accommodate change in its objectives and environment,
  - to ensure that accountability in regard to the system is continually achieved, and
  - to provide the expected services 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.

IEC 62741:2015 The Dependability Case

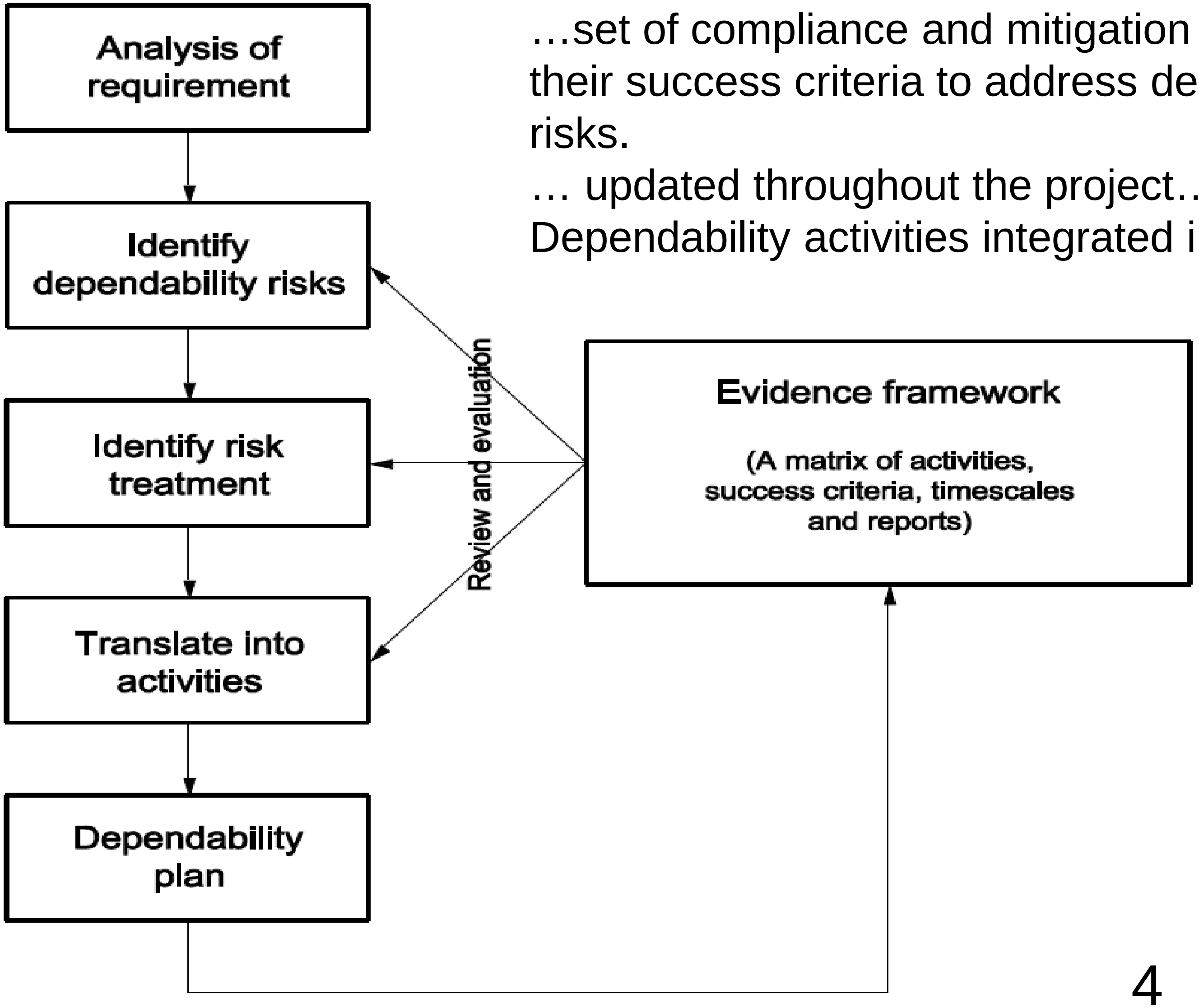
Guide to the demonstration of dependability requirements - The dependability case

- gives guidance on the content and application of a dependability case 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. The dependability case is 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 where they use the system 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: development of claims



Dependability Case: Develop Evidence Framework


Analysis of requirement
Identify dependability risks
Identify risk treatment
Translate into activities
Dependability plan
Review and evaluation
Evidence framework
(A matrix of activities, success criteria, timescales and reports)

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

… updated throughout the project…

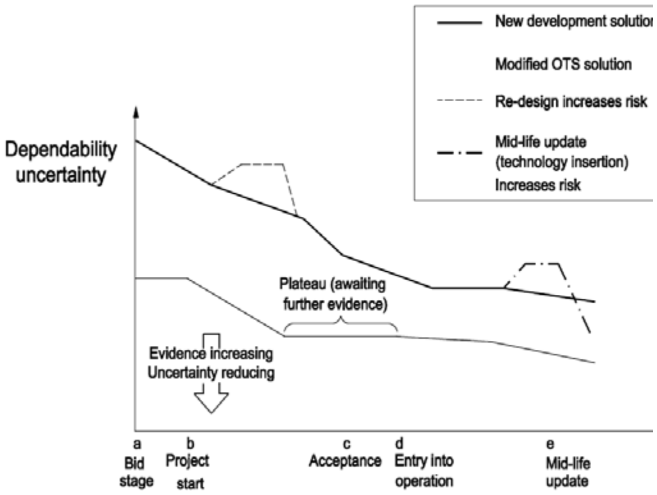
Dependability activities integrated in general PM

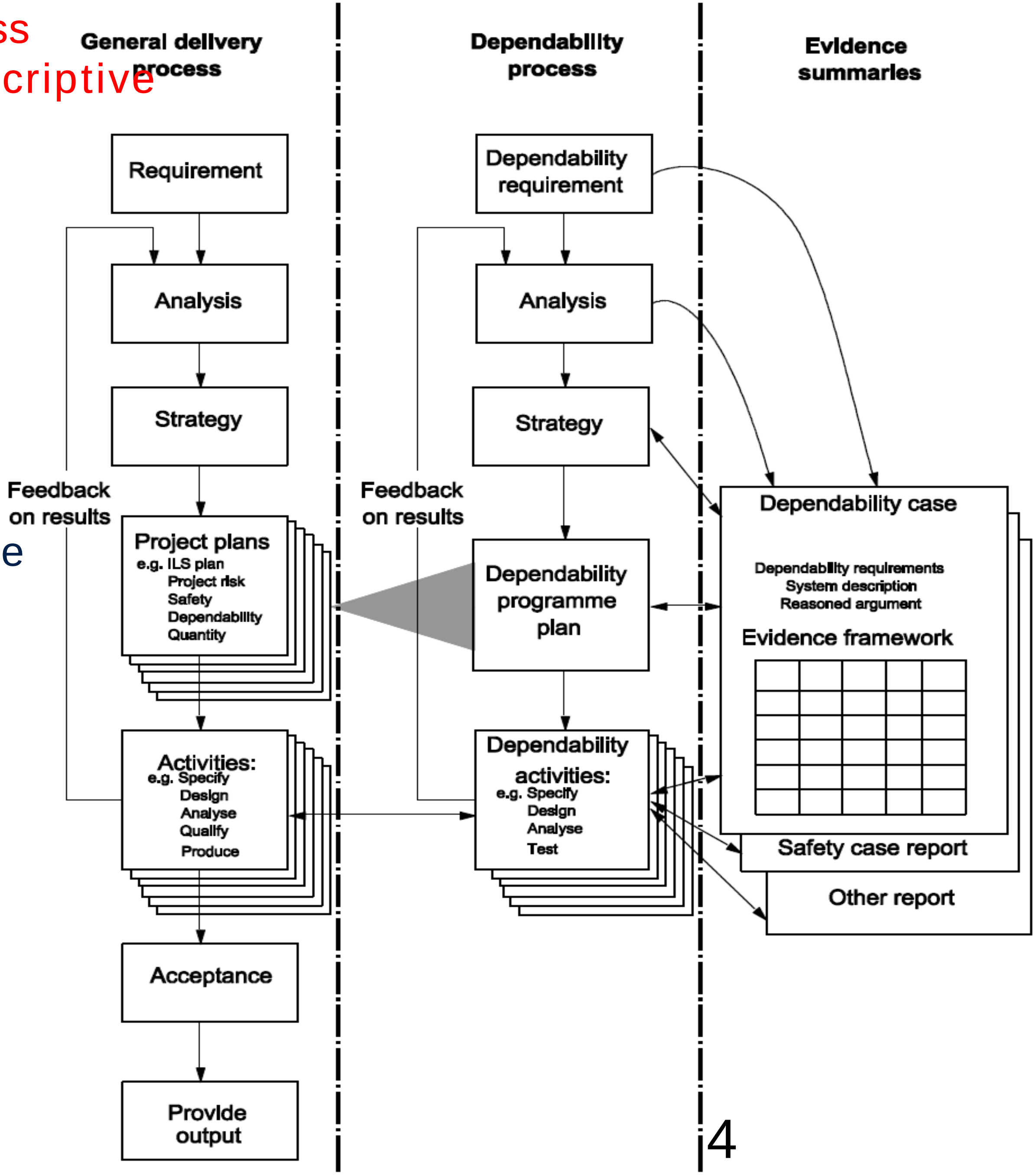
Defines a process rather than prescriptive requirements

Dependability Case

Dependability process, overall delivery process and evidence produced:

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





Thank You for Your Kind Attention !

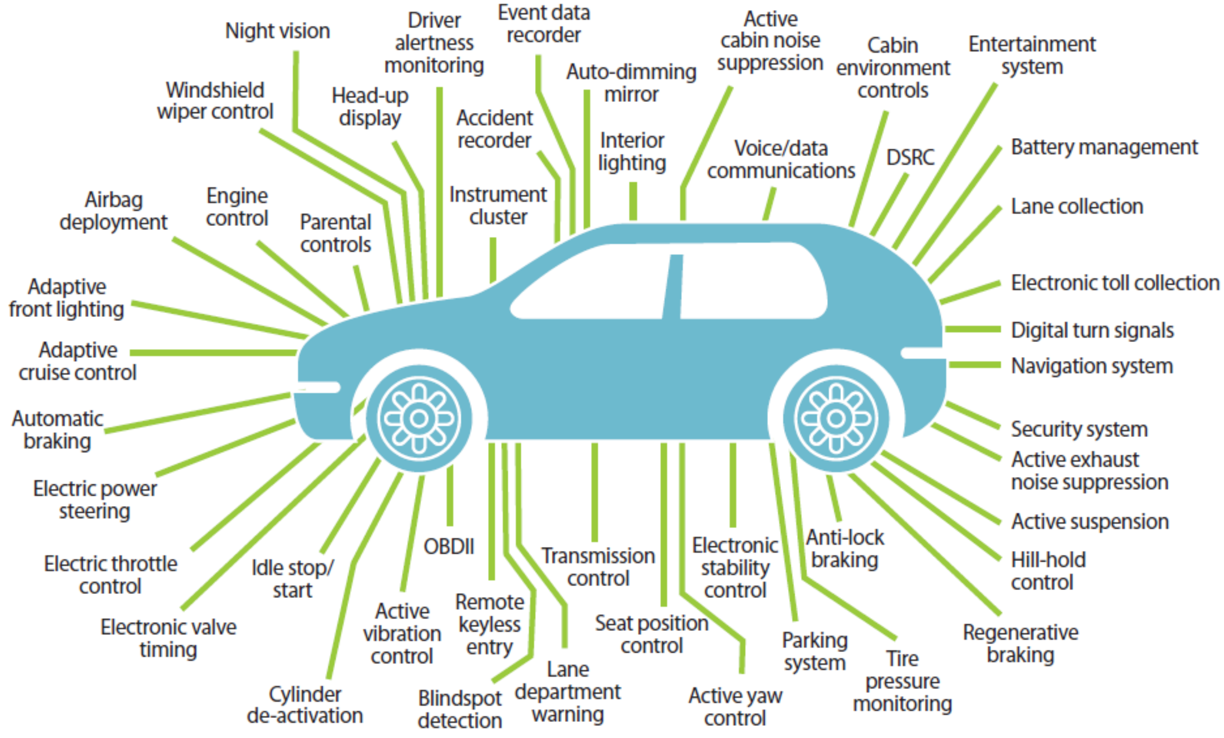
Contact: erwin.schoitsch@ait.ac.at
christoph.schmittner.fl@ait.ac.at

BACKUP SLIDES

Contact: erwin.schoitsch@ait.ac.at
christoph.schmittner.fl@ait.ac.at

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**



© Nodal Industries 2015

Automotive

TU-Automotive Hacks and Threats Report 2016

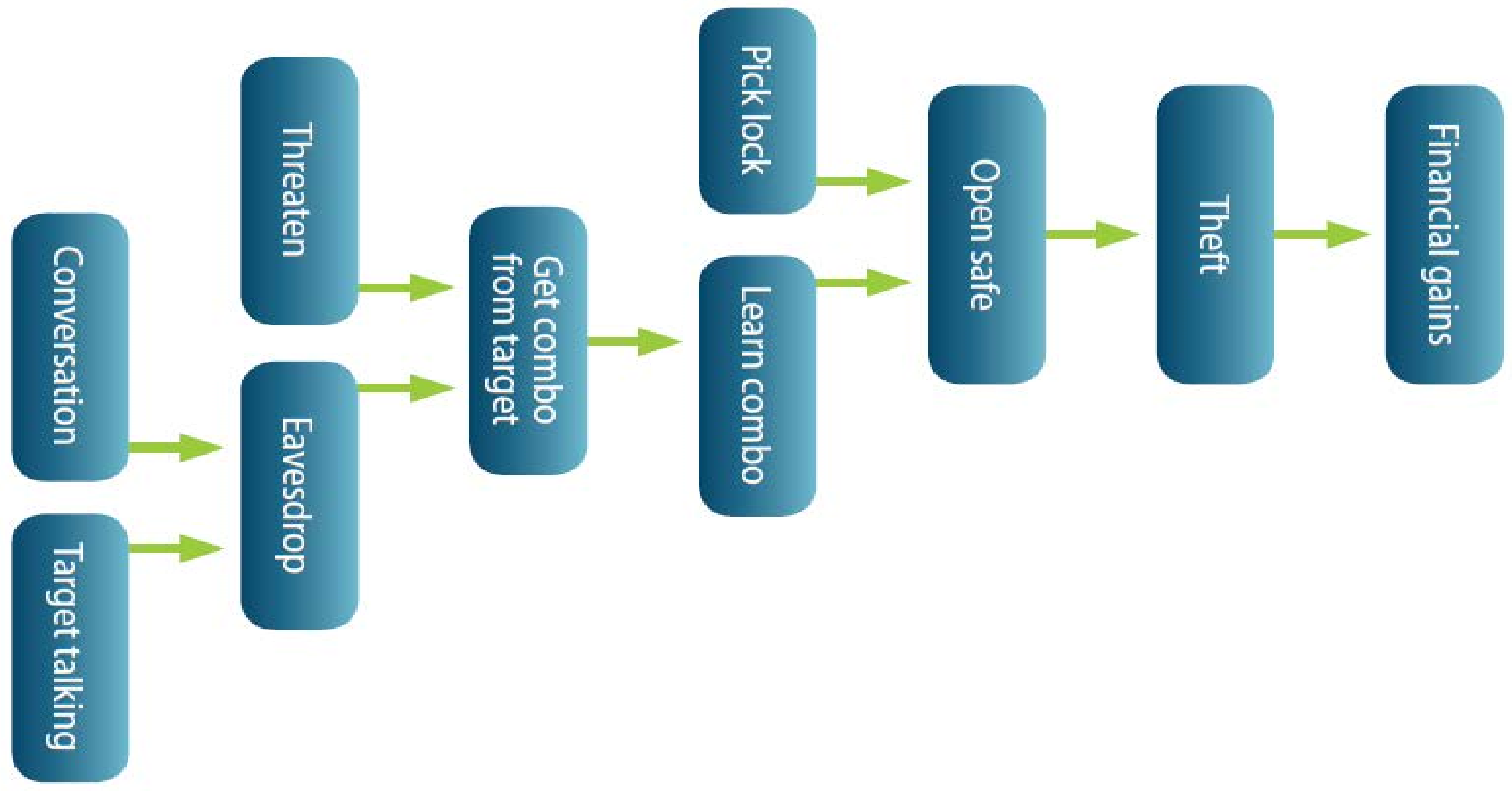
Assessing the types of hacks and the threats they pose for connected automotive technologies

s released in association with TU-Automotive Cyber Security Europe 2016, October 11th & 12th

www.tu-auto.com/cyber-security-europe

Increased # of Attack Surfaces

Tools: Attack Tree example: Safe cracking



Adapted from Schneier (1999)

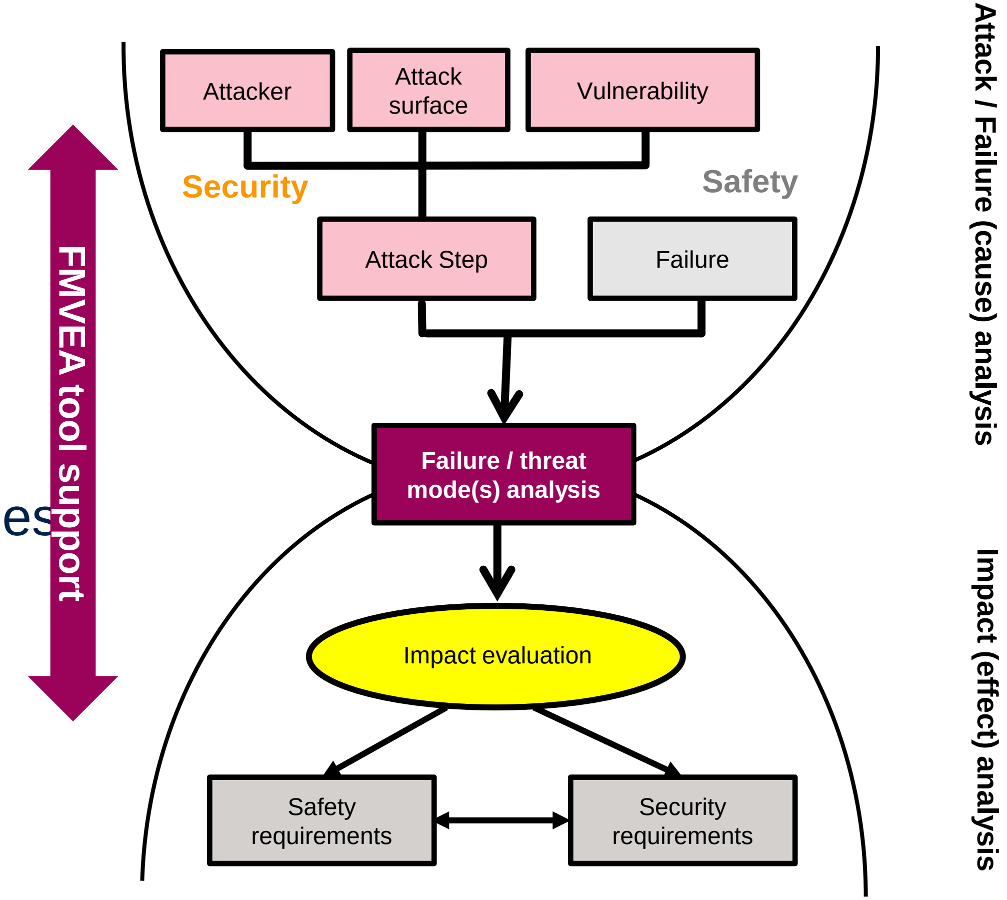
Tools: FMVEA Failure Mode, Vulnerability and Effects Analysis - Attack Likelihood (Safety: Probability driven, Security NOT)

- Current Approach: Rate the Likelihood based on the ease of attacking a system: **CARE-metric**

Parameter	**Values**			
Capabilities	Amateur (3)	Mechanic, Repair shop (2)	Hacker, Automotive expert (1)	Expert team from multiple domains (0)
Availability of Information	Information publicly available (3)	Information available for maintenance of for customer / operator (2)	Information available for production, OEM, system integrator (1)	Information available in company of ECU supplier (0)
Reachability	Always accessible via untrusted networks (3)	Accessible via private networks or part time accessible via untrusted networks(2)	Part time accessible via private networks or easily accessible via physical (1)	Only accessible via physical (0)
Required Equipment	Publically available standard IT devices / SW (3)	Publically available specialized IT devices / SW (2)	Tailor-made / proprietary IT devices / SW (1)	Multiple Tailor-made / proprietary IT devices / SW (0)

FMVEA - Overview

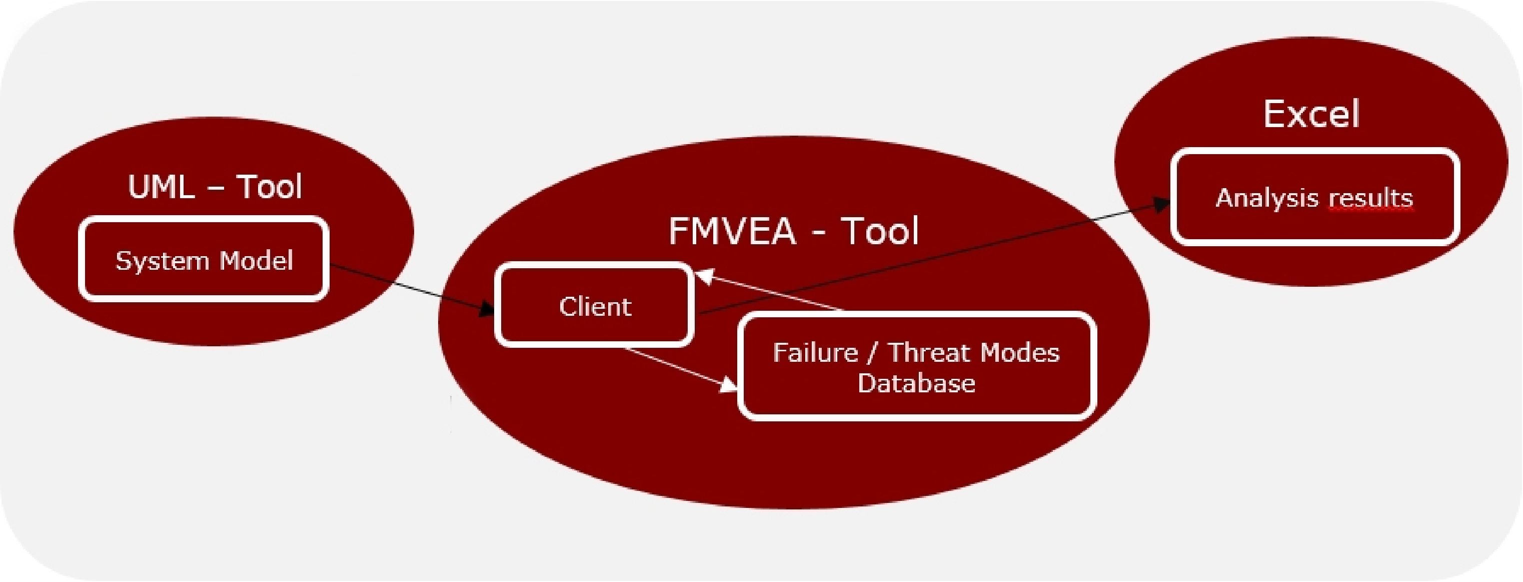
- Identify
  - □ Vulnerabilities
  - □ Attack surfaces
  - □ Potential Attackers
    - ⇒ Failure and Threat Modes
- Assess
  - □ Effects (Impact)
- Derive
  - □ Safety requirements
  - □ Security requirements



e.g. Resilience measures,
Incident response procedures,
System architectural measures,
Monitoring measures.

FMVEA – Tooling

- **Status:** First version of a tool for model-based analysis was developed
  - Analysis is generated based on a system model (currently modelled in DIA[1]) and a Failure / Threat Modes Database



[1] https://wiki.gnome.or/Apps/Dia/

Thank You for Your Kind Attention !

Contact: erwin.schoitsch@ait.ac.at
christoph.schmittner.fl@ait.ac.at