Standardization Challenges

ARROWHEAD: Service Interoperability Enabling Collaborative Automation for Production and Energy System Automation, Intelligent-Built Environment and Urban Infrastructure

EMC²: Platform for Embedded multi-core systems for mixed criticality applications in dynamic and changeable real-time environments

Erwin Schoitsch, AIT, Standardization Manager

March 11, 2015, Co-Summit Berlin, Germany

Advanced Research & Technology for Embedded Intelligence and Systems

Lengthy titles chosen deliberately to demonstrate complexity

Both projects: very large AIPP's
(78 resp. 100 partners, total budget 78 M€ resp. 90 M€)
Both projects:

- many domains,
- offering critical services
- on different levels,
- Cyber-physical Systems-of-Systems aspect,
- although different focus (enterprise/worldwide service collaboration
- vs. multi-core mixed criticality system implementation)

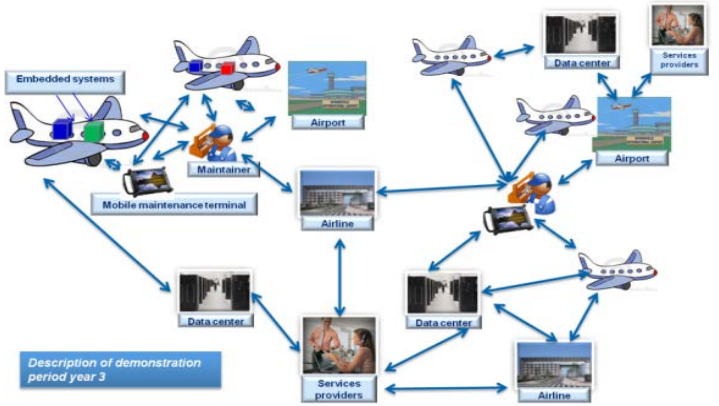
Huge Challenge concerning Standardization Activities' Management

- Following standards
- Influencing standards
- New approaches required, particularly concerning SoS-aspect

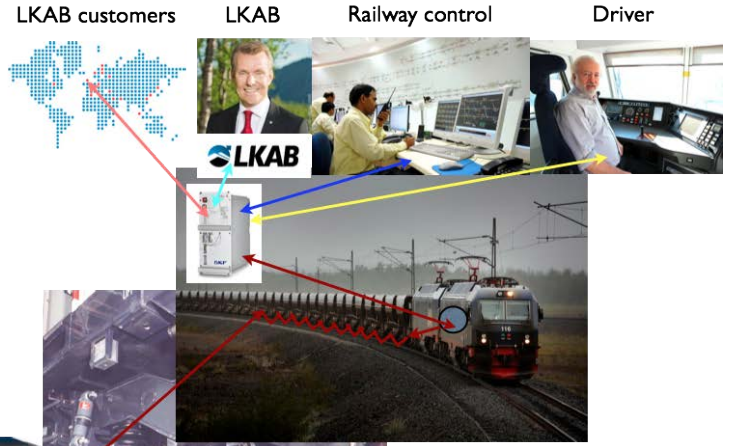
Project ARROWHEAD

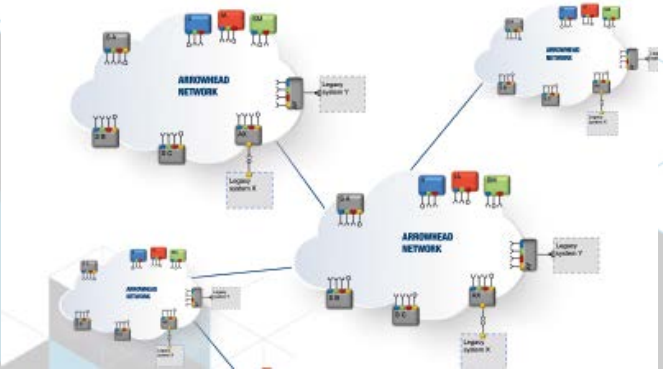
To be demonstrated in real world applications:

- The virtual market of energy
- Production efficiency e.g. manufacturing, mining, airlines, automotive, water, ...
- Energy system optimization
- Smart cities
- Electro-mobility
- From device to enterprise management in the collaborative automation cloud



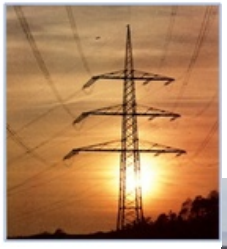
Stakeholders

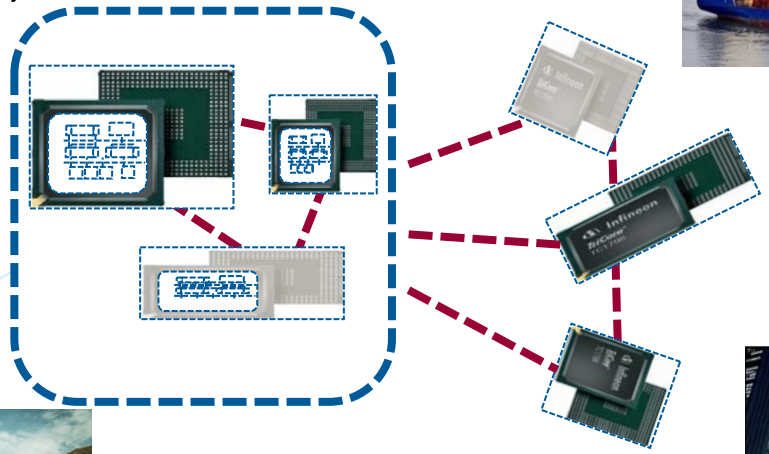




Project EMC²

- Applications: Automotive, Avionics, Space, Industrial Automation, Health care, Infrastructure, IoT Networks, Surveillance, …
- Technologies: From Requirements, HW, SW, Architecture, Development, V&V to Qualification/Certification
- Hardware Complexity
- Dynamic SoS Evolution



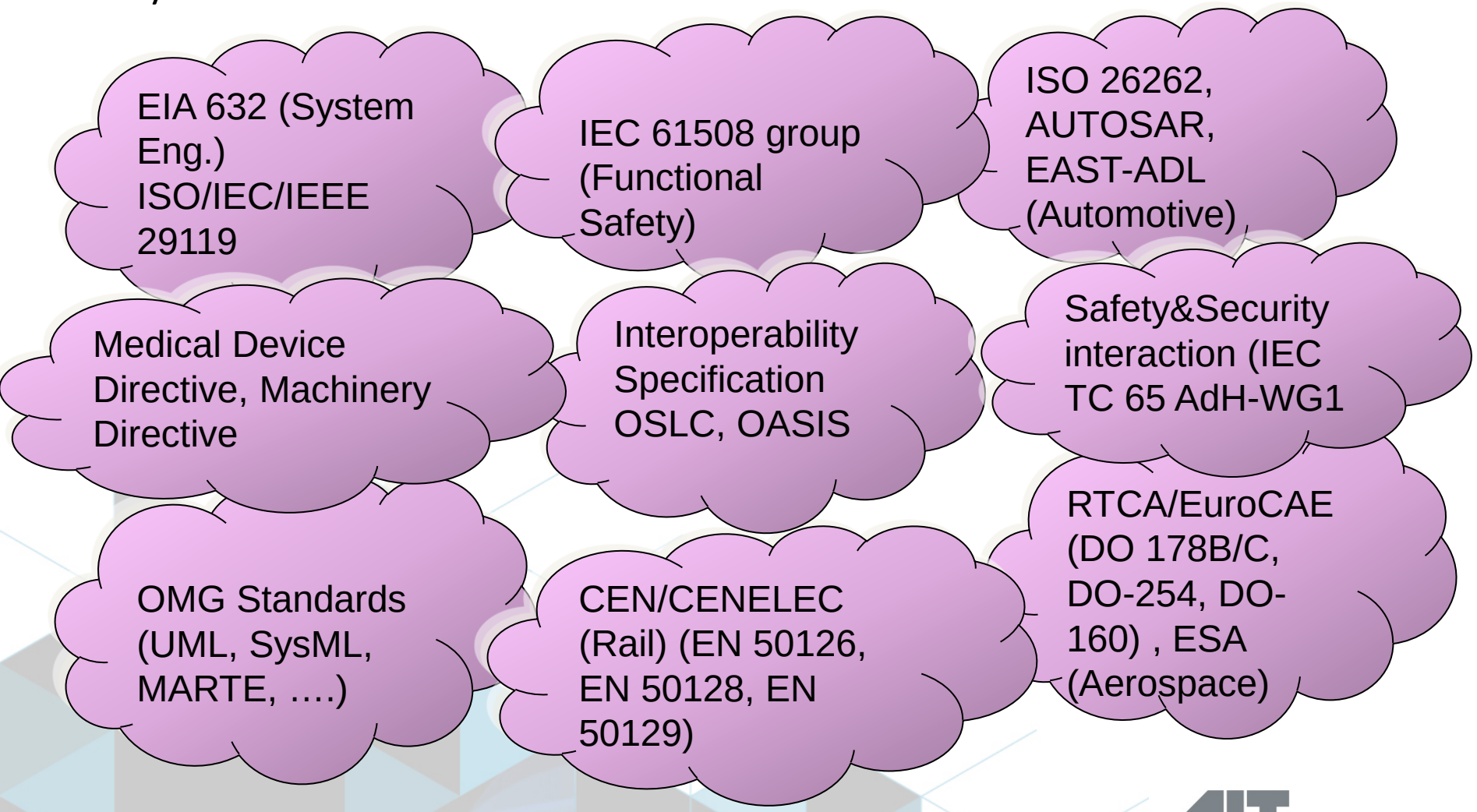








Standardization areas/issues What is different, what is common?

Many standardization areas…



Standardization Scene
(ARTEMIS Standardization Agenda)

< not all for both projects >

- **Standardization organizations:**
  - Overall: ISO, IEC, ETSI, CEN/CENELEC, ISA, IETF, OMG, SAE, RTCA/EUROCAE, …..
- **Application domains, e.g.**
  - Automotive industry, e.g. SAE, ASME, IEC, IEEE, ...
  - Mining, e.g. ISO, ISA,
  - Airlines, e.g. INCOSE, ARINC, ASD, ...
  - Energy production, e.g. IEC, ISA, ...
- **Technologies, e.g.**
  - Automation, e.g. IEC, OPC-foundation, OASIS, ISA, ...
  - Measurements, e.g., ISO, ISA, ...
  - Communication, e.g. IETF, IEEE, ETSI, ITU, PLC -Alliance, ISA,ISO, ...
  - SOA, e.g., OPC-Foundation, OASIS, IETF, ...
  - Service descriptions, e.g. W3C, IETF,

Standardization - Guideline

Interaction with standardization bodies/committees:

- Using/Following standards
- Monitoring standardization scene
- Influencing standardization (time frame normally longer than an ARTEMIS project) (successful examples: DECOS, MOGENTES, MBAT, SafeCer, ….??)
- New Approaches required, e.g. holistic dynamic Systems-of-Systems aspects

Therefore several subtasks, applicable to both projects:

1. Form a unified message to standardisation regarding service interoperability and integration → CP-SETIS, Artemis-IOS/CRTP approach
2. Decide on standardisation organisations and groups to address
3. Form strategies for pilot domain standardization related to the unified message and defined message for individual domain and standardization topics → Task of each WP/Sub-WP which addresses different domains
   - Technology specific standardisation
   - Application domain specific standardisation
4. Through partner activity push the messages to the targeted groups

Standardization Guideline as implemented in EMC²

This strong commitment is achieved by a twofold approach:

1. **Focused Standardization activities** in **all** WPs, particularly
   - WP5 (Tool Integration, Interoperability and Standardization: around UML OMG, OASIS OSLC etc., contributing to IOS (Interoperability Specification) and ARTEMIS CRTP),
   - WP6 (System Qualification and Certification: holistic approach to Quality, Safety & Security Assurance by Design and at Runtime; Trust Case, mainly addressing Functional Safety, Security and Dependability Standards around ISO, IEC, CEN/CENELEC and Do/RTCA and their further development)
2. **Co-ordination and Harmonization** of the various standardization activities (WP 13.5) addressed in the WPs, building on
   - previous experience in ARTEMIS projects, the Support Action ProSE (ARTEMIS Strategic Standardization Agenda) and
   - collaboration with the ARTEMIS Standardization WG, the Innovation Action CP-SETIS (Towards Cyber-physical Systems Engineering Tools Interoperability Standards

Standardization Guideline as implemented in EMC²

Standardization Areas of all WPs:

Backed up by partners' involvement, plans to support and extend selected standards.

- **WP1:** SOA protocols and service semantics (IRTF, IPSO, W3C)
- **WP2:** AUTOSAR Consortium, Accellera Systems Initiative (language C)
- **WP3:** AUTOSAR, IEC 61508, ISO 26262, RTCA/DO 178C
- **WP4:** various HW/emiconductor related standards, ED80/DO 254, VITA 51.x
- **WP5:** Interoperability Specification (IOS – OSLC, OASIS), CRTP (ARTEMIS collaborative Reference Technology Platform), ASAM etc.
- **WP6:** IEC 61508-familiy (IEC 61511, IEC 60601, IEC 62304), ISO 26262, EN 50126/28/29, RTCA/DO 178C, IEC 62443/ISA 99, Do 326A/ED 202A, DO355/ED 204, ECSS – Standards
- **WP7:** AUTOSAR, ISO 26262, ETSI (LDM); IEEE, ETSI and ISO communication standards
- **WP8:** Updates of ARP 4761, certification guidance material for EASA and FAA
- **WP9:** ECSS Standards, Satlab group (DVB-RCS), SOA group ISO(IEC JTC1/SC38 (DAPS Distr. Appl. Platforms and Services)
- **WP10:** EMC Standards (ISO, CEN/CENELEC)
- **WP11:** Industrial networks and Communication Standards (IEC, IEEE), safety&security co-engineering
- **WP12:** diverse cross-domain standardization areas (IEC, ISO, ETSI, OMG)

Standardization Guideline in ARROWHEAD

1. **Co-ordination and Harmonization** of the various standardization activities (WP 10.4), and, may be, motivation to address the standardization tasks within the technology and application WPs, building on
   - previous experience in ARTEMIS projects, the Support Action ProSE (ARTEMIS Strategic Standardization Agenda) and
   - collaboration with the ARTEMIS Standardization WG, the Innovation Action CP-SETIS (Towards Cyber-physical Systems Engineering Tools Interoperability)
   - **Assessment of relevant standardization scene and requirements over all partners and WPs started**
2. **Focused Standardization activities** in **all** WPs, particularly
   - Domain specific standards (which to follow, which need adaptations or interpretations)
   - holistic approach to Quality, Safety & Security Assurance by Design and at Runtime; Dependability/Trust Case building; collaboration in the cloud and interoperability of services addressed in the WP

Example from IEC: Families of Standards

Particularly for ARROWHEAD: consistent mapping from top level down to device

IEC TC65 (Industrial-process measurement, control and automation)

- **WG 10:** Security for industrial process measurement and control - Network and system security, with **IEC 62443** - Industrial communication networks - Network and system security, in close co-operation with ISA (Instrument Society of America, ISA 99 committee) – **industrial cyber-security**
- **SC 65A: 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, and functionality definition (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 (1));
  - 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

Standardization Examples Security

ISA99 Security for 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

Standardization Examples Security (2)

ISA99 Security for Industrial Automation and Control Systems (IACS)

TECHNICAL - SYSTEM

- ISA-TR99.03.01: Security Technologies for IACS
- ISA-99.03.02: Security Assurance Levels for Zones & Conduits
- ISA-99.03.03: System Security Requirements and Security Assurance Levels

WORKING GROUPS

- WG1: Technologies
- WG2: Security Program
- WG3: Terminology, Concepts and Models
- WG4: Technical Requirements
- WG6: Patch Management
- WG7: Safety & Security
- WG8: Communications & Outreach
- WG9: Wireless and Security
- WG11: ISA99-ISA67 JWG on cyber security for nuclear plants

Standardization Outlook : What is common for both projects?

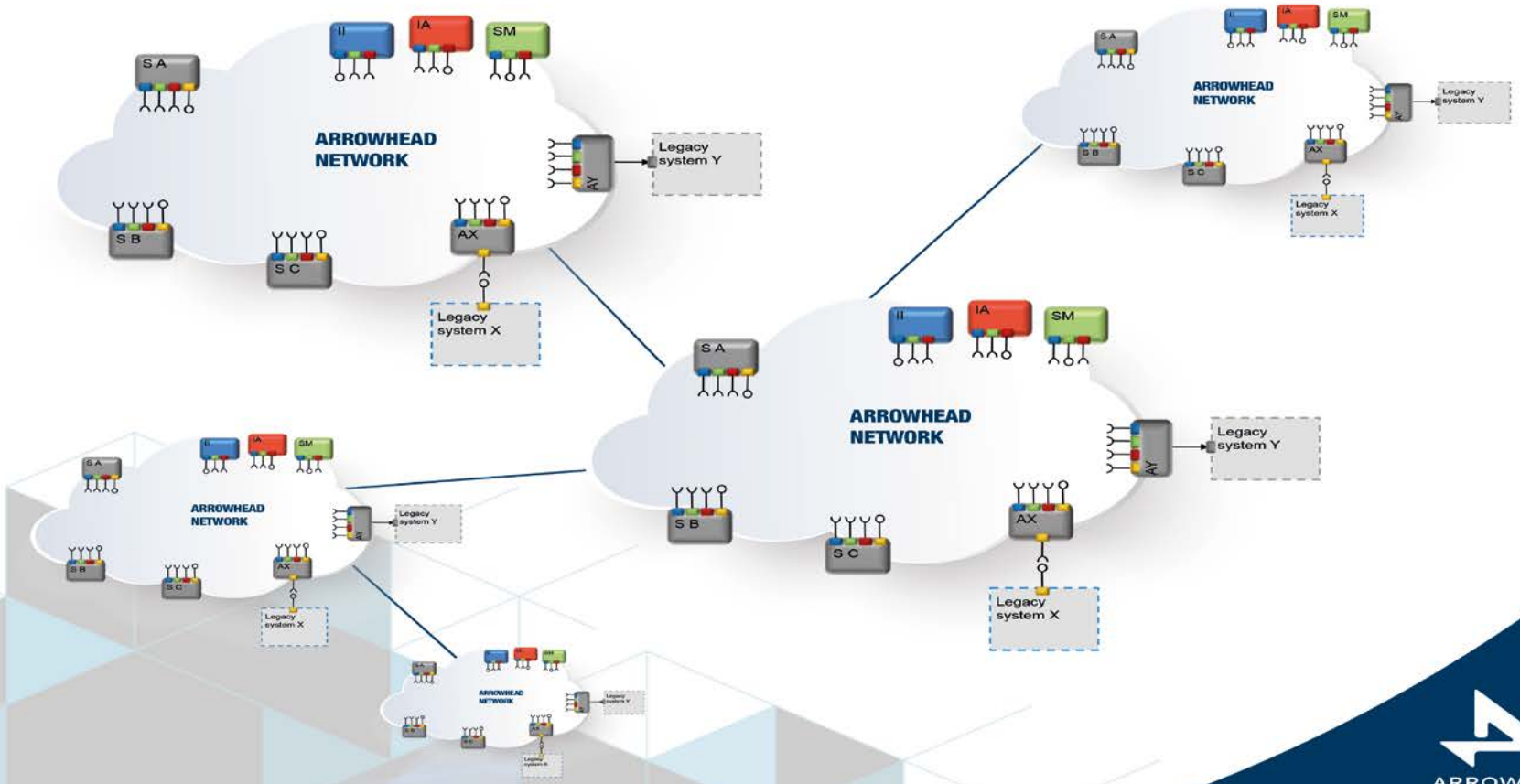
- Recent developments led to increasing awareness that **“security aware safety”** is absolutely necessary in highly automated Systems-of-Systems, particularly if dynamic SoS properties, wireless communication and collaboration in the cloud are involved → to build on **integration, co-engineering and co-certfication/qualification**
- IEC TC65 started an Ad-hoc Group **“Framework towards coordination of Safety and Security** (in industrial automation)”
- Looking at IEC 61508, IEC 61511, TC 44 (Safety of machinery, electro-technical aspects), ISA 99, ISA 100, EN 50126/28/29, IEC 62859 Nuclear Power Plants and EN 50159, DO 326A/ED 202A, DO 255/ED 204), ISO 26262 where similar approaches started or are proposed
- **Safety & Security Co-Engineering**: Consequences for methods, techniques and tools: extend them to include security-aware-issues in V&V, RHA, Workflow of certification/ qualification process – Security particularly requires incremental and life-time (run-time) approach

Recent Safety & Security Standardization activities

- **IEC TC65 AHG1 (Ad-hoc Group 1):** Framework towards coordination of safety & security in industrial automation (started end of Oct. 2014)
- **IEC 61508-3** Ed 3.0 preparation: Security aware safety guidelines (Nov. 2014)
- **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”
- **EN 50129, EN 50159** (Railway): activities particularly in Germany (DKE)
- **ISA 84, ISA 99 and ISA 100** (process industry, industrial process control and communication), IEC 62243 (industrial automation, network and communication security)
- **IEC 62589** (Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity)
- **IEC TC44** – Safety of machinery, electro-technical aspects (first considerations)
- **Do 326A/ED 202A:** Airworthiness Security Process Specification, Do 355A/ED 204A Information Security Guidance for continuing Airworthiness

Particular issues in ARROWHEAD and EMC²

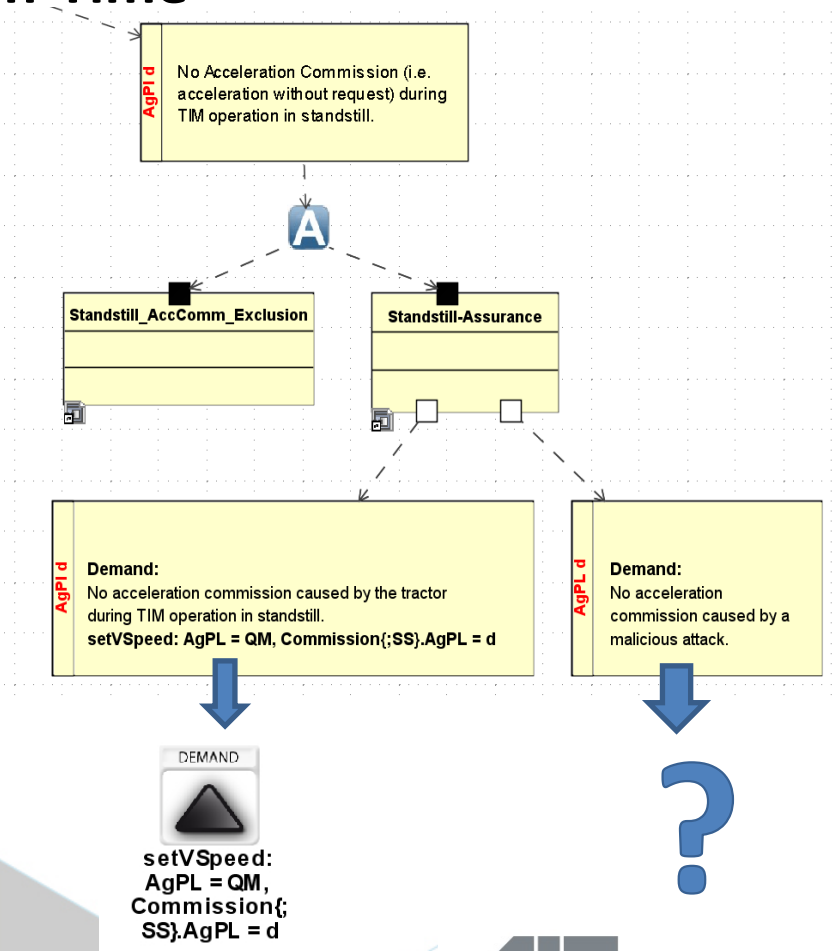
- **ARROWHEAD: Safety, Security and QoS (Performance) in the collaborative Cloud**

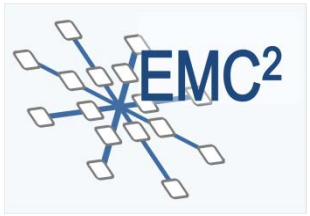


Particular issues in ARROWHEAD and EMC²

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

- **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**





Thank you for your kind attention!

Erwin Schoitsch <erwin.schoitsch@ait.ac.at>

Advanced Research & Technology for Embedded Intelligence and Systems

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Safety & Security

- Back-up Slides

Combined Safety & Security approaches: Railways (from J. Braband, H.-H. Bock)

- EN 50129 does not define security threats and countermeasures explicitly, but requires addressing the prevention of unauthorized access in the safety case.
- From a conceptual point of view hazard and threat analysis are quite similar
- However methodology and target measures are different e. g. SIL and SL
- Quantification of IT Security Risks for Safety is considered impossible as the likelihood of an attack can not be estimated („Likelihood trap“). Thus security threats will be treated like systematic errors in safety.
- IEC 62443 used as reference for security issues

Combined Safety & Security approaches: Railways

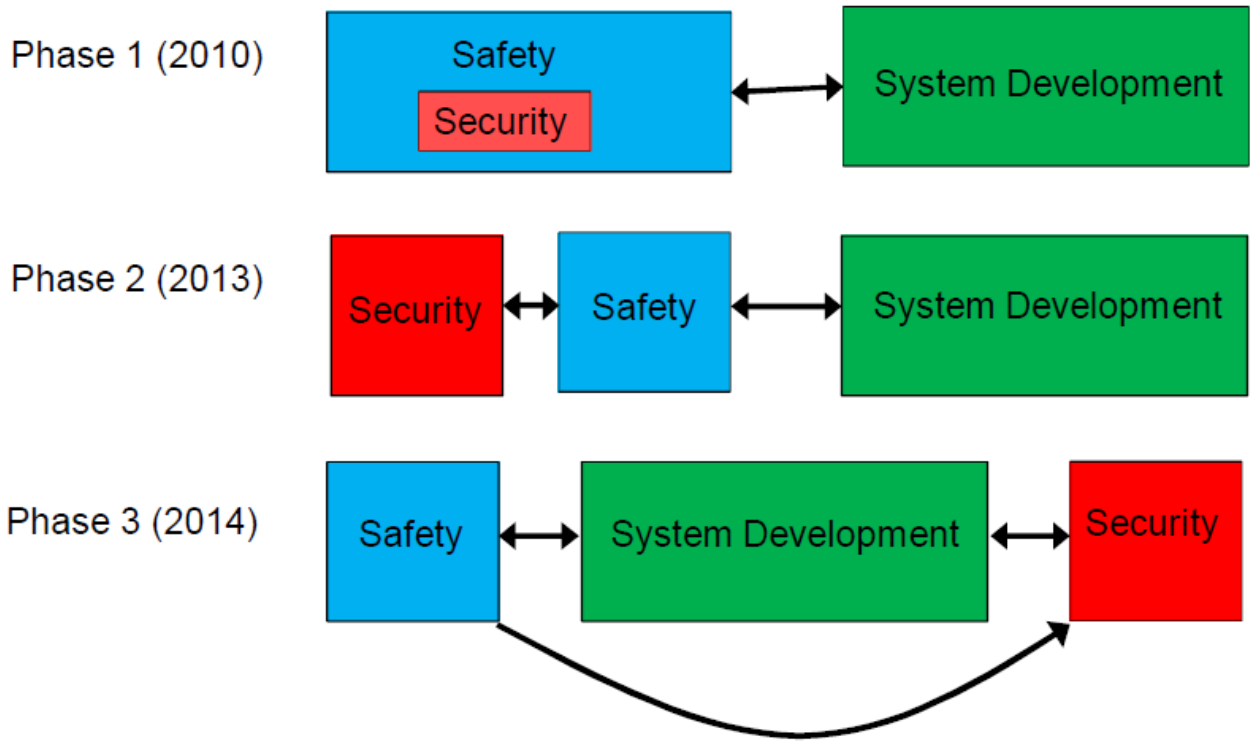
- **Comparison with Safety**
- Safety systems need to protect against operator errors, random failures and foreseeable misuse.
- So it could be expected that safety systems would fulfil SL1 of IEC 62443 (“casual or unintended”).
- IEC 62443 contains 41 requirements related to SL1, of which
  - the majority 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
- It is recommended to include the missing SL1 requirements in the safety system‘s requirements, and (in future) add these requirements in EN 50129.

Combined Safety & Security approaches: Railways

- **What about higher SLs? (SL: qualitative measure)**
  - SL1: casual or unintended
  - SL 2: simple means: low resources, generic skills and low motivation
  - SL 3: sophisticated means: moderate resources, IACS-specific skills and moderate motivation
  - SL 4: sophisticated means: extended resources, IACS-specific skills and high motivation
- Adaptation of IEC 62443 to specific railway requirements?
- Priority to safety engineering, complemented by security engineering (security engineering focusing on safety relevant issues, rigour of measures/techniques (EAL, SL) according to risks and SILs)
- How to achieve holistic approach? Security certification embedded in safety-certification, components may be qualified independently and then an incremental component based approach taken (projects SafeCer etc.)

Combined Safety & Security approaches: What happens in other domains?

Example: Aircraft Standards – interesting development over evolving standards



(our IEC 61508 approach) - Safety first preferred by authorities

Combined Safety & Security approaches: What happens in other domains?

From presentation of Jeff Joyce at ISSE 2014 WS (SAFECOMP) in Sept.:
„Integration of Security and Airworthiness in the Context of Certification and Standardization“

Document	Title		Publication date
DO-326A / ED-202A	**Airworthiness Security Process Specification**	The process document proposes guidance to assess security risk, design security protection and ensure effectiveness of these protections **The What part**	August 2014
DO-YY3*	**Airworthiness Security Methods and Considerations**	This document provides considerations and methods to support the process and the activities described in DO-326A. **The How part**	Expected September 2014
DO-355 / ED-204	**Information Security Guidance for Continuing Airworthiness**	This document proposes guidance to develop Instructions for Continued Airworthiness (ICA) and guidance for the operation and maintenance of aircraft and for organizations and personnel involved in these tasks .	June 2014

RTCA SC-216, Aeronautical Systems Security, Collaborative work with EUROCAE WG-72

*No EUROCAE counterpart at the moment

Instrumentation and control systems - Requirements for coord. safety and cybersecurity

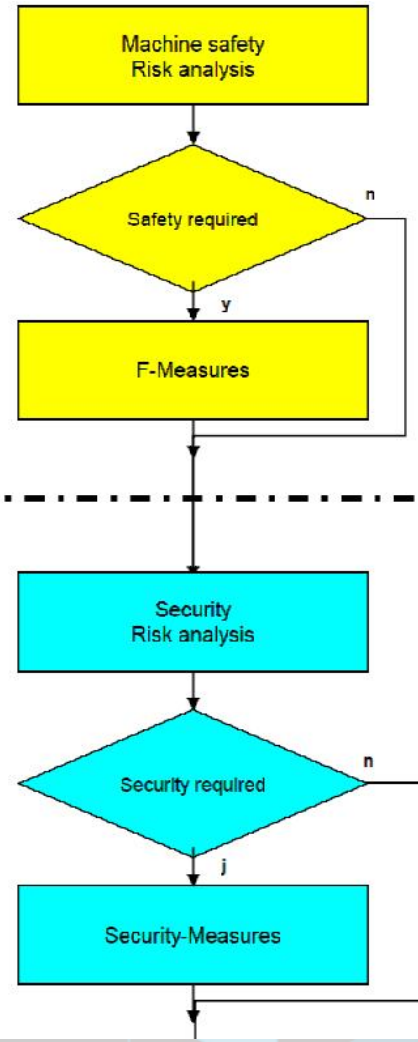
5.2 Fundamental Principles

- **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 **analysed** 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

IEC – TC 44, Safety of Machinery

Reqirements separation? No holistic system approach!
→ISA99 against

Safety:
OEM
Machine builder



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

CE Mark or FAT

Security:
System integrator
Final user

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

FAT – Factory Acceptance Test

Combined Safety & Security approaches: What happens in other domains?

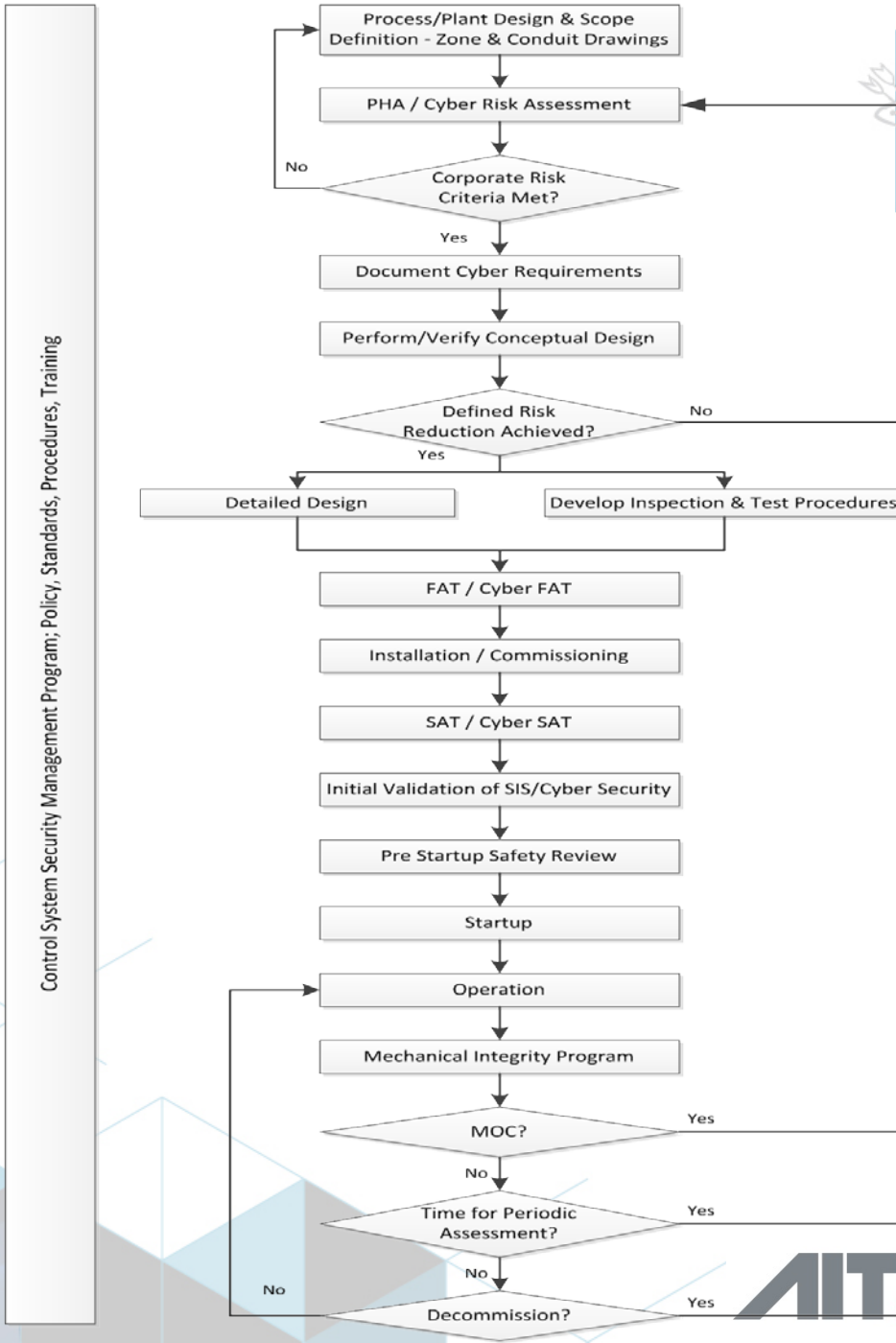
For IEC 61511 (SIS),

ISA TR 840009

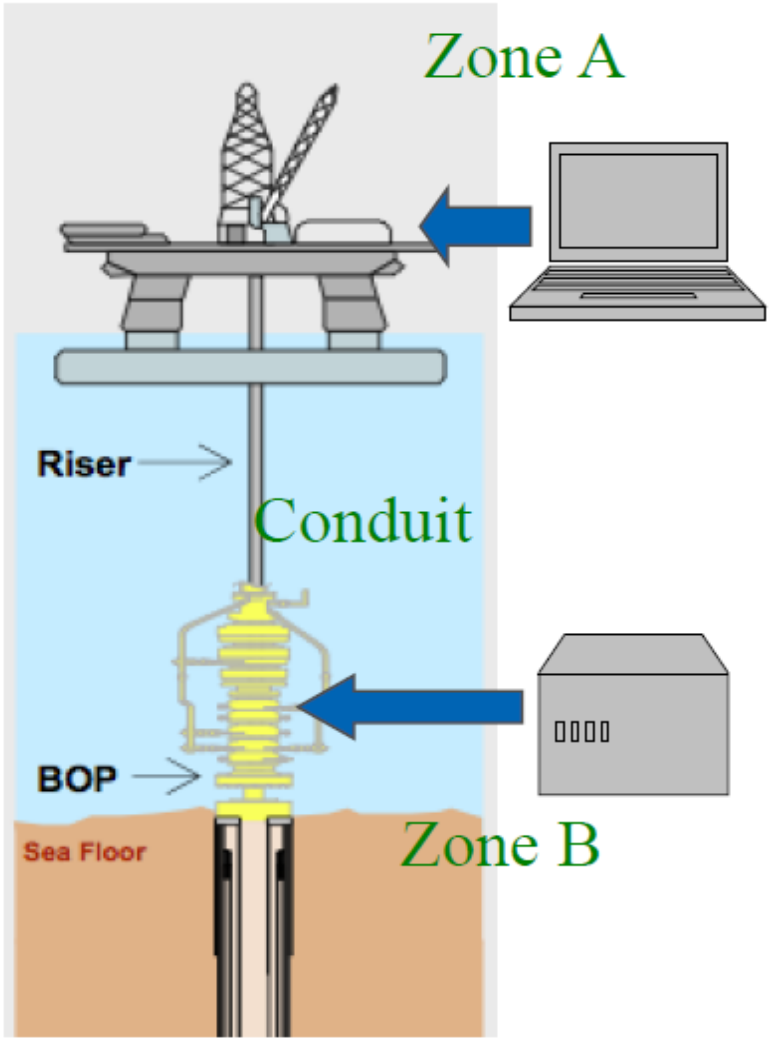
(from drafts and meeting notes, nothing final or agreed):

Cyber-Security Life Cycle integrated with Process Safety Management

FAT Factory Acceptance Testing
SAT Site Acceptance Test



Example Ingo Rolle, DKE: SIL vs. SL → complementing each other



Findings:

IT security is a continuously carried out process, organizational measures are more important than in functional safety (because of moving target).

Most functional safety standards don't contain a hazard model – IT security does. Functional safety is a complementary property to other safety properties.

Safety functions are defined according to the application. The foundational requirements are common.

The Security levels are valid for a certain zone. The safety function with the assigned SIL extends through the conduit.

We found out for zone A:

no SIL, but tool requirements and high SLs for certain FRs (Foundational Requirements: access, data, resources).

for zone B: high SIL and low SLs.

In a non safety-relevant application we may arrive at high SLs and no SIL (e.g. data acquisition system)

IEC – the way forward: History

- May 2013: TC65/AG14(Advisory Group) @ Beijing
  Koji DEMACHI (KD), Yokogawa, Japan) presented “Safety concerns in Industrial Automation”
- TC65AG recommends that an ad hoc group be established to examine and chart the relationships between the safety (functional safety and safety) and security standards, and the relationship between them and the system approach. (65/559/INF Advice 5)
- April 2014: TC65 plenary @ Hamburg < I was present, discussion >
  TC65 agreed to form an ad-hoc group to provide a framework toward coordinating Safety and Security in an Industrial setting (Resolution # 10)
- July 2014: Call for experts (65/569/DC)
- Sep 2014: Compiled comments from NCs (65/574/INF)
- 33 experts from 13 countries registered;
- 20 present at the kick-off meeting end of Oct. 2014
- Next kick-off meeting: June 29 – July 2, 2015, VIENNA

IEC – the way forward

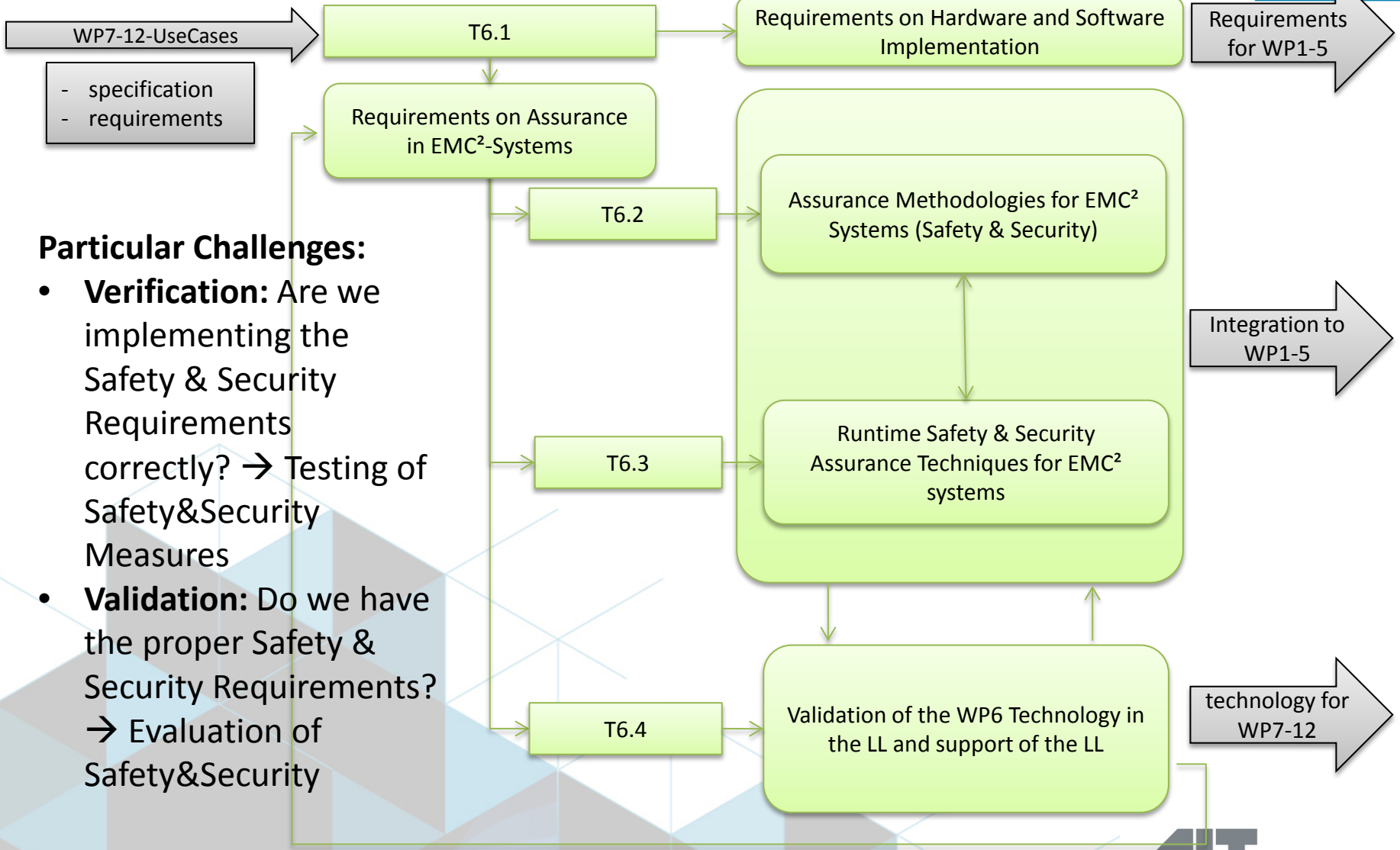
Objective stated in 65/569/DC (draft for comments)

- **The objective of the ad-hoc group is to investigate directions in coordinating safety and security standards, both under normal resources conditions as well as in emergency situations, and to provide recommendations and a new work item proposal.**
- **1. To provide recommendations**
- **2. To provide NP, if it is necessary and feasible**

In general, an AHG investigates an issue and provides recommendations. Recommendations are forwarded to the AG (Advisory Group) and can be

- **a new work item project (NP)**
- **or a new WG**
- **or recommendations how existing or upcoming standards should take into account the issue investigated (e.g. there are ISO/IEC standards how to include safety in standards, or security in standards)**
- **or that the work should be transferred to an existing group to take care of it**
- **Liaisons etc. …..**

EMC² WP 6: System qualification and certification



Particular Challenges:

- **Verification:** Are we implementing the Safety & Security Requirements correctly? → Testing of Safety&Security Measures
- **Validation:** Do we have the proper Safety & Security Requirements? → Evaluation of Safety&Security

SESAMO: Artemis 295354

SESAMO

Security and Safety Modelling

- Starting date: May 1st 2012
- Duration: 36 months
- Total costs: 12.013 k€
- EU contribution: 1.968 k€
- Total planned effort: 1.114 p/m
- 7 Work packages, 31 deliverables

Reducing the cost of building

safe and secure products

Why SESAMO?

- SESAMO addresses:
  - … the root problems arising with the convergence of safety and security in embedded real-time (and therefore time-critical) systems …
  - … subtly and poorly understood interactions between functional safety and security mechanisms …
  - … the absence of a rigorous theoretical and practical understand of safety and security feature interaction …