



7th International Symposium Programmable Electronic Systems in Safety Related Applications
Köln/Cologne
TÜV Nord, TÜV Rheinland, EWICS TC7

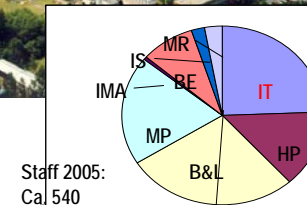
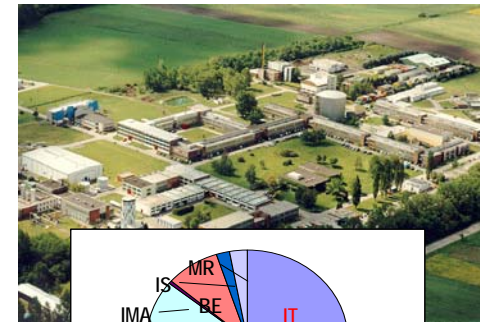
“Dependable Embedded Systems – a Challenge for a holistic Safety and Security Design”

3.- 4. May 2006

Erwin Schoitsch, ARC Seibersdorf research



Seibersdorf Research: Largest enterprise of ARC – Austrian Research Centers
Austria's largest independent, contract-oriented research organisation (14 sites, 800 staff)



Staff 2005:
Ca. 540

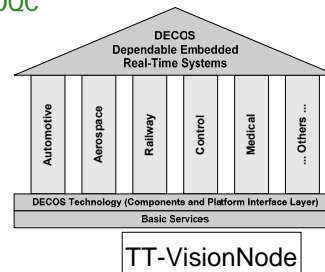


- Information Technologies
- Health Physics
- Biogenetics, Natural Resources
- Life Sciences
- Materials & Production Engineering
- Integrated Microsystems Austria
- Biomedical Engineering
- Intelligent Infrastructures and Space Applications
- Media Research Studios Salzburg



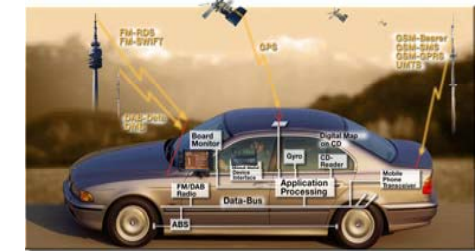
IT - Dependable Embedded Systems Group

- Co-ordinator of EU Integrated Projects **DECOS**, **SECOQC**
- TT-VisionNode (SensorNode) & SD4SC
 - ♦ Integration of Image Processing and Dependable Controls, Smart Cameras and Sensors
- Accredited V&V Lab (EN ISO/IEC 17025)
- Research Topics
 - ♦ Methodology & tools for dependable embedded components and systems
 - ♦ Model based V & V of components & systems
 - ♦ Host-target testing with Hardware-in-the-loop (HIL) / Software-in-the-loop (SIL)
 - ♦ RAMSS/Hazard analyses for component based systems
 - ♦ European Projects and Networks on Dependability and Software Process Management (ENCRESS, AMSD, ISA-EuNet, SPIRE, OLOS, ACRuDA, ESPITI, DECOS, COOPERS...)



Embedded Systems' Application: Human Centered, Vision-Driven – Safety and/or Security Driven

- **Automotive:** Accident free Driving
- **Avionics:** Safe Sky for Europe
- **Medical:** Robot Surgeon
- **Communications:** Seamless Connectivity
- **E-Life:** Ubiquitous Computing, environment awareness
- *personalised (user centered, dynamically adapted to user preferences),*
- *dependable (time dynamics, timely responsiveness, secure),*
- *context-awareness (person, object, location, time),*
- *natural interaction*



Industrial Vision:
„Aerospace Safety at Automotive Cost“

Industrial Need: From Supply Chain to Design Chain





Trends in Medical Systems - Component Healthcare System

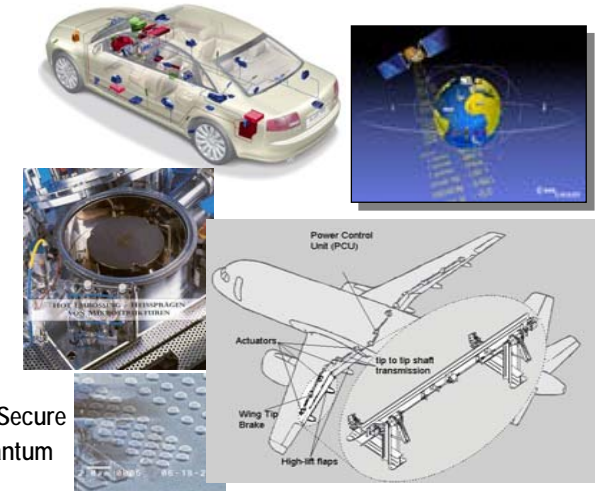


DECOS Dependable Embedded Components and Systems

DECOS Technology: Platform for an *Integrated Architecture* for dependable embedded real-time systems:

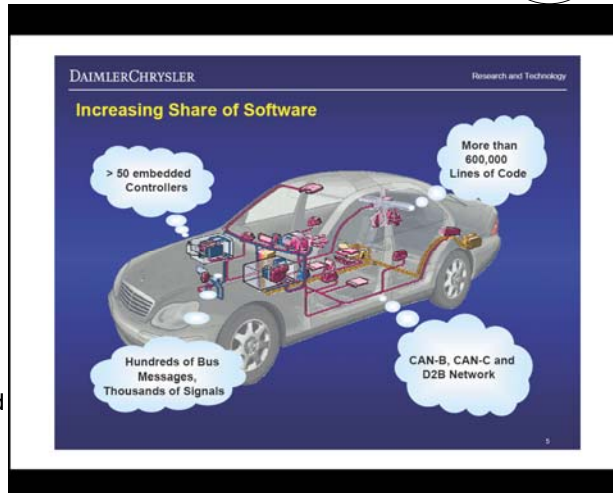
- Automotive
- Aerospace
- Railway
- Industrial Control
- Space
- Medical Systems
- Robotics/Autonomous Systems

SECOQC: Global Network for Secure Communication based on Quantum Cryptography



Why Integrated Architectures – Automotive Example:

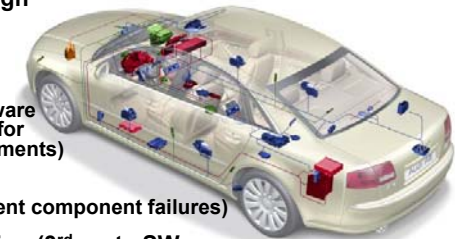
- From mechanics to electronics and software – 80 ECUs, one per function and per supplier?
- Increase of electronics from 25% to >40%
- Innovations 80 – 90% based on electronics and software
- 55% of car failures caused by electronics, cabling/connectors and software (GI conference Oct. 2003 – DC postponed “X-by-wire”) – Liability !!!



DECOS Motivation (Safety first!)

Facilitate the systematic design & deployment of “integrated” electronic subsystems in embedded systems through:

- Electronic Hardware Cost Reduction (fewer ECU’s, cables, connectors)
- Enhanced Dependability by Design (clear partitioning of safety-critical and non safety-critical subsystems by design)
- Reduced Development Costs (modular certification, reuse of software components, structured integration for communication & computational elements)
- Diagnosis and Maintenance (diagnosis of transient and intermittent component failures)
- Intellectual Property (IP) Protection (3rd party SW as “black box”)





DECOS Basics Safety first!

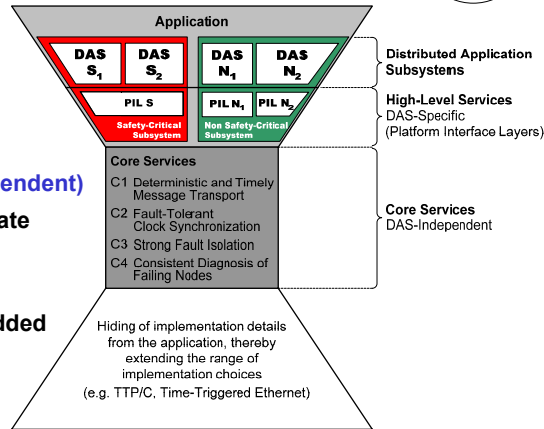
Objective:

Development of fundamental
(domain and technology independent)

enabling technologies to facilitate
paradigm shift from

federated to **integrated** design

of dependable real-time embedded
systems

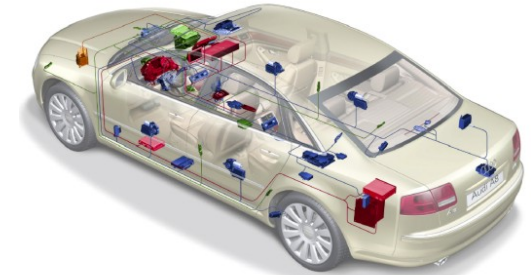
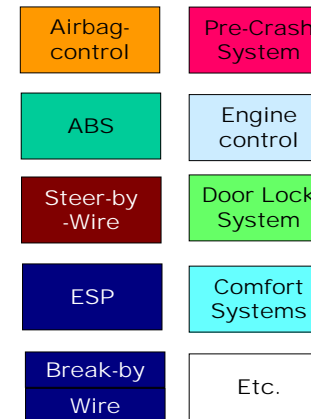


Project Facts

Start: July 1st, 2004, Duration: 3 Years, Budget: 14.3 Mio €, EU Funding: 9 Mio €



Allocation of Distributed Subsystems of different criticality



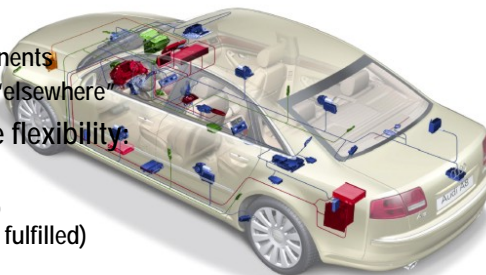
Allocation of Distributed Subsystems (2)

Currently, task seems trivial:

- Software is developed for manufacturer-specific components
- No choice to locate software "elsewhere"

Integrated Systems increase flexibility:

- Uniform hardware nodes
- Software may run on any chip (provided that *constraints* are fulfilled)



Basic Requirement for Integrated Architecture:

No interference between „jobs“ in

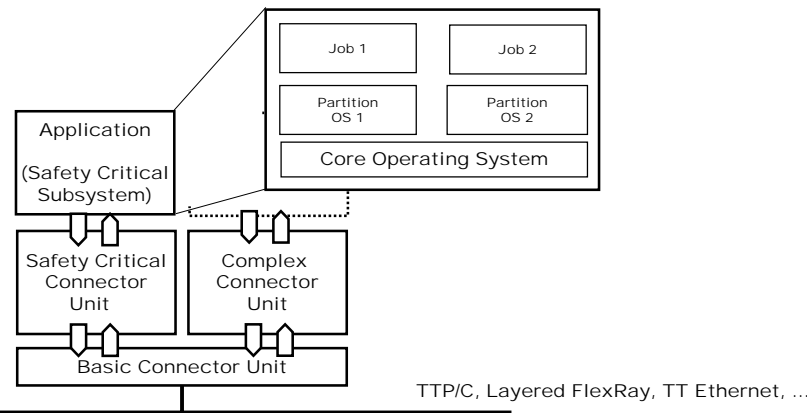
- Time (predictable/fixed allocation of time slots to nodes)
- Space (encapsulated execution environment, virtual communication links and gateways, partitioned OS)
- between FCUs (nodes), safety critical and non-safety-critical components

Then: Job Allocation within DECOS nodes

- Tasks can be allocated to any node as long as *constraints* are fulfilled (resource, dependability, performance, ...)
- Dependable configurability, composability, even of mixed-criticality applications
- Allocation/Scheduling is part of development methodology
 - MDA: Platform Independent Model vs. Platform Specific Model



Node of DECOS Architecture (FCU, component)



DECOS will provide

- ◆ encapsulated execution environment,
- ◆ virtual communication links and gateways (jobs to behave as if physically separated),
- ◆ fault tolerance layer (functional, value and time domain),
- ◆ partitioned OS in HW, software controlled (diagnosis, fault tolerance)
(supports SW-IPR protection by transparent "black box" integration)
- ◆ diagnostic services (identifying faulty components, intermittent and transient faults and Heisenbugs by job heuristics)
- ◆ And a Generic Test Bench to facilitate validation and certification of DECOS-based applications in a modular, component based manner (component-based modular safety case).
- ◆ And a prototype tool chain for development as well as prototype components



That's good for: on-board embedded systems, protected environment

Three groups of trends: "Das Auto denkt mit"

- Advanced comfort, "personalized car"
 - e.g. Car Body Electronics (adaptive equipment: seats, superposed adjustable steering wheel, (no) pedals, ...)
 - Noise suppression, adaptive air conditioning, configurable cockpit,
 - Navigation, communication, information, new types of displays
- Safety enhancement (*EU eSafety on the Road ... minus 50% accidents !*)
 - Vehicle Dynamics (ABS, ASR, ABC, ESP (Electronic Stability Program), AAS (Active Additional Steering), Adaptive Cruise Control (ACC), Road Tire friction Control, ...) *Safety - critical controls !*
 - Advanced Warning- and Control Systems (pedestrian protection, crash avoidance, track control, lane support, ...), Advanced Driver Assistance (ADAS) *Safety - critical controls !*
 - Driver Monitoring, Predictive Driver Assistance, Emergency call system
- Optimized resource usage
 - Power Train (Integrated Engine Control, Engine/Energy Optimization, Transmission Control) *Safety - critical controls !*
 - Fully integrated Electrical Energy Management



But not sufficient for:

- Extending autonomous on-board functions with interactive and co-operative systems:
- Roadside embedded systems and interaction (intersection, speed control, emergency call systems)
 - Local connectivity: vehicle - to -vehicle (long term) - highway throughput optimization, advanced adaptive cruise control
 - Global Connectivity: Satellite, traffic navigation and control
- Ultimate Goal: Autonomous Driving, "Platooning" of vehicles
- Liability, Legal and Standardization Issues !!

Linking to global infrastructures: Link to "Ambient Intelligence"
Security Issues: Design, Development, Integration, IPRs, Supply Chain; Connectivity during Operations & Maintenance!! (Call-back, Upgrades off-line/on-line, Repair, Manufacturer's Statistics ("Know more than police")?)
Unfortunately: Safety and Security Community do not co-operate!



Safety & Security: a joint issue in Embedded Systems?

*In a protected, controlled, closed environment:
Safety remains major issue*

In an open environment with

- *Access points (at least: maintenance!!)*
- *Wireless interaction,*
- *Mobility*
- *Co-operating systems*

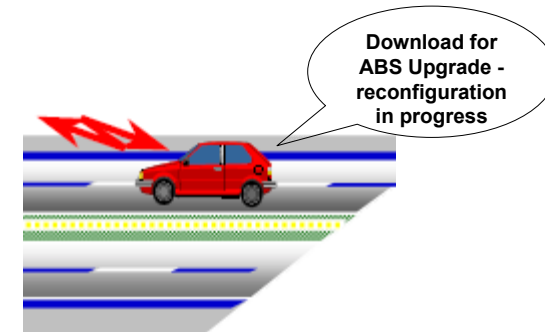
Security becomes a safety-relevant issue!!!

Example. Automotive Visions



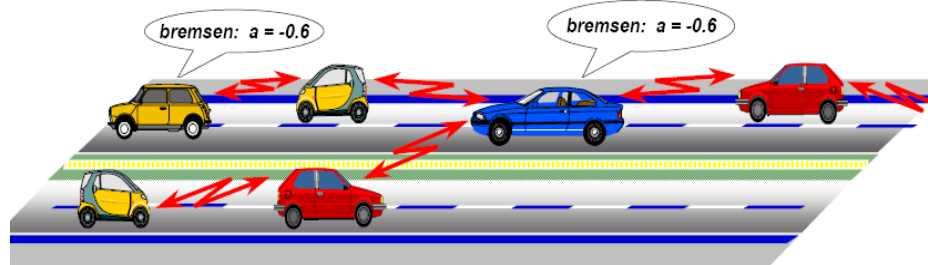
e.g. Maintenance:

Imagine: Field Update of Control Software on the Highway ...



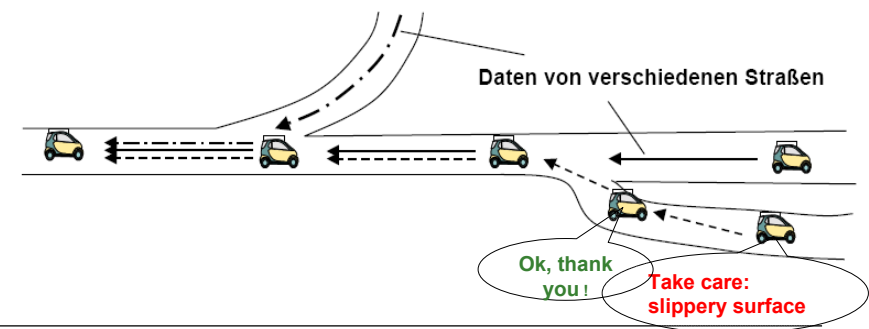
Automotive Visions

Platooning car "trains" – large scale electronic coupling
– high throughput, lower risks (?)



Trends in Automotive

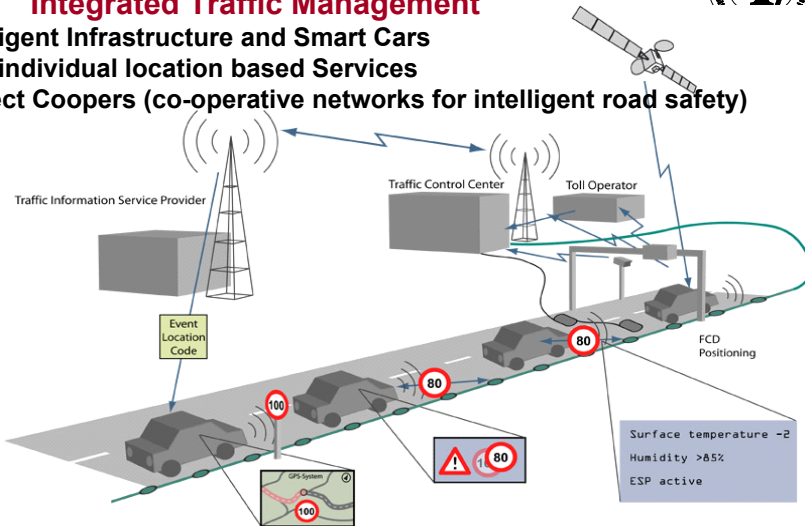
Localized "Floating Car Data",
"To look around the corner", "Upstream Warning"





Integrated Traffic Management

Intelligent Infrastructure and Smart Cars
plus individual location based Services
Project Coopers (co-operative networks for intelligent road safety)



Automotive Visions: Examples eSafety on the road (EU)

Platooning – project “Chauffeur 2”
(Chauffeur Assistant)(small scale electronic coupling)



Safety & Security – joint issues ?

Characteristics of all visionary Scenarios:

Regional/Global Connectivity and Integration, remote Maintenance and Control, many access points → *SECURITY has Safety Impact, and vv*
BUT: Different approaches, standards, not the holistic view, e.g. in IEC 61508 „Functional Safety of electrical/electronic/programmable electronic safety-related systems” - safety only !!

Maintenance Phase of IEC 61508 – JTT4 – Security Aspects (or SC65C, WG13, Digital Communications, Cyber security ?) NEW IEC 62443 !?(Ind. Control) vs. „Other World”: Security Standards (ISO 17799, ISO 15408) (ref. NIST)
Independent work on „Security Profiles” for Avionics (CAA), Industrial Automation (Process Control Security Requirements Forum PCSRF)

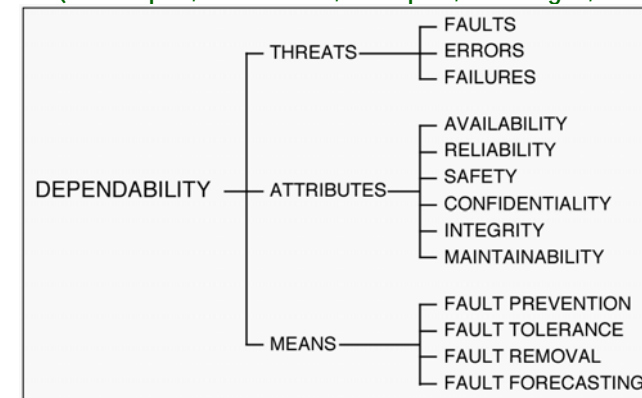
To span the gap: JRC project of EWICS TC7

Study of the Applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the needs of safety critical systems (March 2003)



Safety & Security – joint issues ?

Dependability – Holistic System Concept (*Trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers*).
(J.-C. Laprie, A. Avizienis, H. Kopetz, Udo Voges, T. Anderson, et.al.)



Fault – error – failure – fault – in SoS

Security: „CIA“

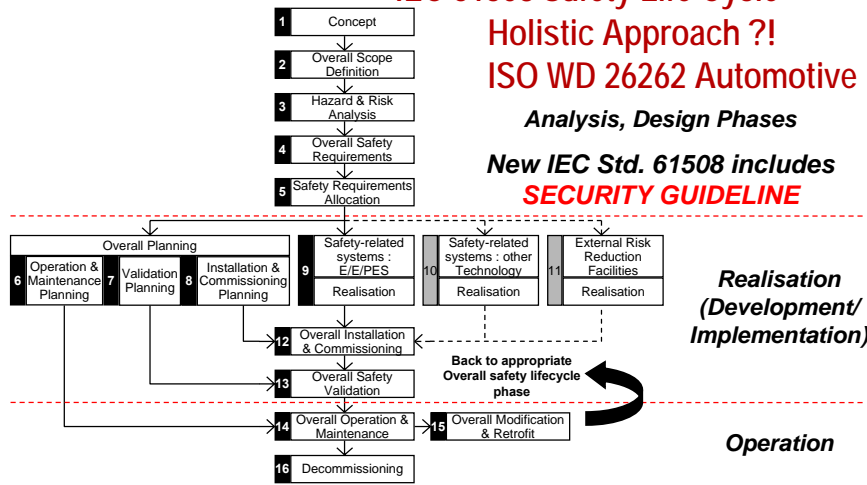
Impact and Trade-offs



IEC 61508 Safety Life Cycle Holistic Approach ?! ISO WD 26262 Automotive

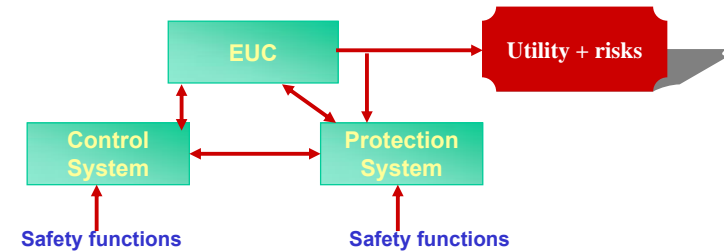
Analysis, Design Phases

New IEC Std. 61508 includes
SECURITY GUIDELINE



Safety View APPLICATION OF IEC 61508

There is equipment under control (EUC) which, with its control system, poses a threat to its surroundings



- Safety functions are performed by E/E/PE systems
- Steps need to be taken to understand the risks involved and reduce them to a tolerable level

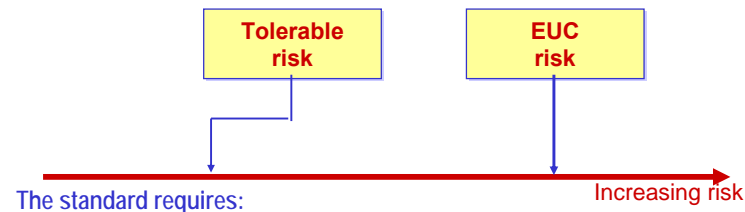
Security: Surrounding a threat to the system – "vulnerability"-Focus



IEC 61508 – Principles: Safety or Joint View ?

IEC 61508: How to meet the goal - Risk as low as reasonably possible, at least at a tolerable level !! < Security Impact on Safety – Safety Impact on Security>

1 - Understanding the Risk

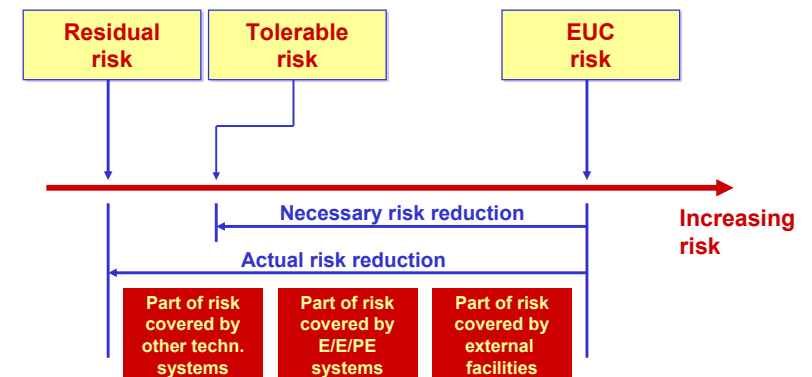


The standard requires:

- ♦ Assessment of the risks posed by the EUC
- ♦ Decision on what level of risk is tolerable
- ♦ Decision on what risks should be reduced
- ♦ Determination of how to go about reducing the risks



IEC 61508 - MEETING THE GOAL "RISK ALARP" (2) – Safety AND Security Risks, JOINT VIEW ?!



- Risk may be reduced by more than one safety-related system – and Security?
- This standard gives guidance on E/E/PE systems



IEC 61508 - MEETING THE GOAL "RISK ALARP"

- Safety View only ?

3 - Principles Involved

- The safety lifecycle is a model for identifying the activities appropriate to safety-related systems
- A risk based approach means not merely following a procedure and assuming that "safety" will result, but:
Identifying the risks and reducing them appropriately
- Safety integrity levels (SILs) provide targets for risk reduction
(Security: EAL-Evaluation Assurance Level ? Correlation to SILs ?)
- The safety requirements specification defines the safety requirements necessary for risk education
- Carrying out safety planning ensures a methodical and auditable approach



SAFETY LIFECYCLE PHASES

3 Hazard and risk analysis – DO SAFETY and SECURITY together!

To identify the hazards of the EUC in all modes of operation, the event sequences leading to the hazards, and the EUC risks associated with the hazards

- ⇒ What hazards does the system pose?
- ⇒ What are their possible causes and consequences?
- ⇒ What is the likelihood of their occurrence?
- ⇒ What are the risks associated with each of the hazards?
- ⇒ By how much do we need to reduce the risks



HAZARD AND RISK ANALYSIS

- Hazard identification <Safety and Security>
 - Define hazards and hazardous of EUC and EUC control system for all reasonably foreseeable circumstances
 - Fault conditions
 - Reasonably foreseeable misuse
 - Human factors (not sufficient to confirm that normal operation is safe)
- Hazard analysis <Safety and Security>
 - Determine the event sequences leading to each hazardous event
 - Identify the causes of hazards and assess the consequences of hazardous event
- Risk analysis <Safety and Security>
 - Determine the risks associated with the hazardous events

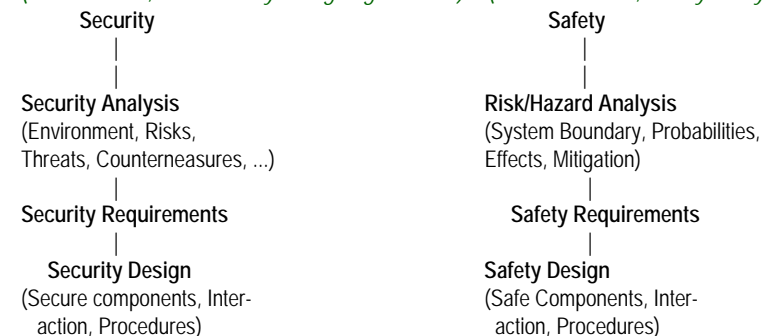


EWICS TC7 Safety AND Security Life Cycle

Proposed IT – Overall Safety AND Security Life Cycle - Integration
(equivalent to the Safety Reference Model, IEC 61508, Part 1)

System Requirements – Unified Approach

(ref. A. Bialas, ICT Security Designing Process) (ref. T. Cichocki, Safety Analysis Method)





EWICS TC7 – IT Safety&Security Life Cycle

Activities may differ very much between Safety and Security depending on requirements; traditional trade offs between safety and security as between safety and reliability, e.g. during Decommissioning and Disposal:

Security: Secure management of data (unretrievable destroyed or secure archivation of preserved integrity);

Safety: Safe management of shut down or continued (degraded) operation

Unified Approach: Consider both aspects and interactions during system analysis and design!
(Francesca Saglietti, ECN, European CIIP Newsletter)



Standards and certification:

With X-by-Wire: „Automotive market is now entering the world of safety critical systems“... “Liability, supply-chain structures will require certifications and V&V („automotive industry will have to set up standards for system validation“)“... “Emphasis on the added value of software in distributed embedded systems architecture” – (topic addressed directly by DECOS).

Didier Blondin, AXLOG Ingenierie, Business Development Manager, „Would certification become mandatory in automotive engineering?“, 2nd European congress ERTS, 2004. (Future visionary applications will require SIL4) (and Security in context of Safety?)

IEC 61508 applying to the vehicle	SIL4	SIL3	SIL2	SIL1	na
Steer-by-wire		○			
Dashboard				○	
Engine management system			○		
Navigation					○
Brake-by-wire		○			
Body controller				○	
Diagnostic					○
Entertainment system					○



Standards and certification: IEC TC56 WG 10 – NEW IEC 62443-“Security for Industrial Process Measurement and Control – Network and System Security” << still problem: NO holistic view >> (Others: SC65C, WG13, Fieldbus Security Profiles IEC 61784-4)

Table v1: SRLs and related verification requirements (proposal)

SRL	Security functions and related Evaluation Assurance Levels according to ISO/IEC 14508	Hardware, software or ASICS and related Safety Integrity Levels according to ISO/IEC 61508
Low	EAL 3 + ?	SIL 1
reduced	EAL 4	SIL 2
Full	EAL 5	SIL 3



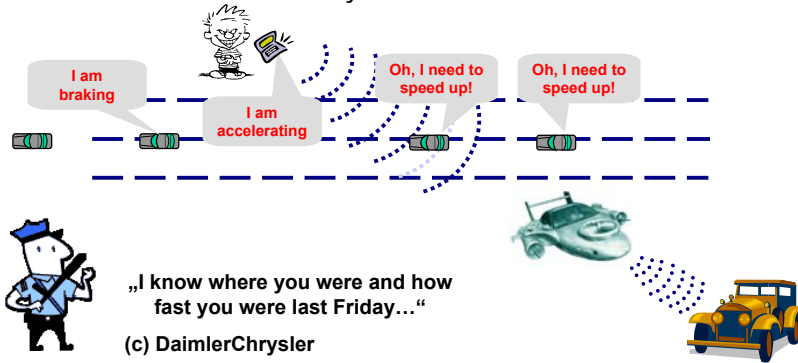
Table v2: Verification and validation problems and related standards (all three)

Problem	Dealt with in IEC 62443	Dealt with in ISO/IEC 14508/3	Dealt with in IEC61508
Industrial security requirements	Yes		
Detailed requirements for the security	Yes		
Development of software	No	11	Part 3
Guidance documents	Partly	12	Part 2, 3
Life-cycle support	No	13, as required for security issues	Part 2, 3; safety-related
Security target evaluation	No	14	
Tests	No	15	Part 3
Vulnerability analysis	Partly	16	
Verification of correct functioning of HW	No		Part 2
Verification of functioning of ASICS	No		Part 2



Back to Automotive Example: additionally required Security Design for (1) Safety and (2) Privacy

- Fake safety messages could cause severe damage
- Information of vehicle's communication could be used against its driver/owner
- Vehicles could outlive their security solutions



USA (FCC): reserved 5,9 GHz bandwidth 75MHz; IEEE 802.11p (WAVE WG)



Security Design

- Trust: Vehicles shall trust safety messages they receive over the air
 - ♦ Message was created by valid sender (i.e. not a hacker with a laptop)
 - ♦ Message content was not tampered with in transit
- Anonymity: Safety communication shall not ease tracking or identification
 - ♦ Automotive companies want to design products that protect their customers and increase their sense of safety
 - ♦ If the privacy of the consumer is violated, the technology will not succeed
- Resiliency: Security design must support efficient maintenance and update
 - ♦ Compromising a handful of DSRC radios should not compromise the entire system
- Efficiency: Safety messages should be self-contained and the receiver should be able to verify their authenticity in real time without prior or further communication
 - ♦ Automotive Safety is a time-critical
 - ♦ There is no time to „phone home“ to a central authority to verify the message
 - ♦ Nor time for checking among vehicles to establish trust first

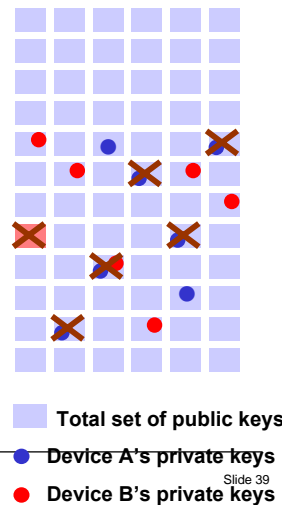


Possible Solution: Public Key Mgmt. Block Approach

- All devices have the same set of public keys
- Each device has a unique subset of corresponding private keys
- If a device is compromised, the leaked private keys are banned by authority, devices use other keys

Requirements met:

- Trust: is provided via verification of the signature with a known and trusted public key
- Anonymity: each key is shared among many vehicles, but it is obviously not perfect
- Resiliency: the system can tolerate a limited number of compromises by revoking the leaked key set(s)
- Efficiency: requirement is met, perhaps with the exception of key revocation



BACK to DECOS: Dependability Experiment: Vulnerability of DECOS systems and components

- Dependability is an umbrella term covering aspects of
 - ♦ Safety
 - ♦ Reliability
 - ♦ Availability
 - ♦ Maintainability
 - ♦ Security (Confidentiality, Integrity, Authenticity,...)
- A Safety Case covers traditional safety issues, based on probabilities and unintentionally inserted faults (main focus of DECOS)
- Security includes intentional malicious interaction
- A Trust case includes both, especially the safety impact of security breaches during design, development, operation and maintenance and of configuration

Activities are twofold:

- Vulnerability Analysis of DECOS components and systems (RAMSS)
- Experiment on a selected trust case based on the analysis (Digital Signatures etc.)



- [1] Process Control Security Requirements Forum (PCSRF) – Security Capabilities Profile for Industrial Control Systems (June 13, 2003; Aug. 8, 2003)
- [2] PCSRF – Security Profile Specifications (SPS) (Aug. 26, 2002) (Applying CC)
- [3] Joe Falco, Keith Stouffer, Albert Wavering, GFrederic Proctor, Intelligent Systems Division, NIST, USA: “IT Security for Industrial Control Systems”
- [4] C.L. Beaver, D.R. Gallup, W.D. NeuMann, M.D. Torgerson: Key management for SCADA (Scandia National Laboratories), March 2002 (Security Aspects and requirements of the Supervisory Control and data Acquisition System, for the Electric Power Grid)
- [5] CAA: Report on the development of security requirements for CAA safety related SW
- [6] IEC SC65C/307/NP: New Work Item on Communications Profiles for Safety and Security
- [7] SSE-CMM – System Security Engineering Capability Maturity Model (June 15, 2003) (in line with ISO 15504-2 (SPICE) and CMM-I (following maturity level concept for security engineering instead of software development) (not safety application – specific)
- [8] EWICS TC7 – Study of the Applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the needs of safety critical systems (March 2003)
- [9] A. Pfitzmann: Why Safety and Security should and will merge. SAFECOMP 2004, Potsdam, Proceedings, Springer LNCS 3219 (Sept. 2004)
- [10] R. G. Herrtwich, Automotive Telematics – Road safety vs. IT-Security? SAFECOMP 2004, Potsdam, Proceedings, Springer LNCS 3219 (Sept. 2004), ITSC05, Vienna, Sept. 13, 2005
- [11] E. Schoitsch, “Design for Safety and Security”, in: Springer NATO Science Series, Cyberspace Security and Defense: Research Issues, Vol. 196, 2005.



Thank You For Your Kind Attention

Reference:

E. Schoitsch, “Design for Safety and Security”, in: Springer NATO Science Series, Cyberspace Security and Defense: Research Issues, Vol. 196, 2005.

DES-Roadmaps: <https://rami.jrc.it/roadmaps/amsd>

DECOS project: <http://www.decos.at>

ARC-sr, IT: www.smart-systems.at

Email: erwin.schoitsch@arcs.ac.at