"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."

SAFURE

Safety and Security – Towards a Combined Approach for Mixed-Critical Cyber-Physical Systems

André Osterhues, ESCRYPT GmbH

HiPEAC
SAFURE Workshop
22th January 2018
Manchester, UK

SAFety and secURity by dEsign for interconnected mixed-critical cyber-physical systems

Agenda: Safety & Security

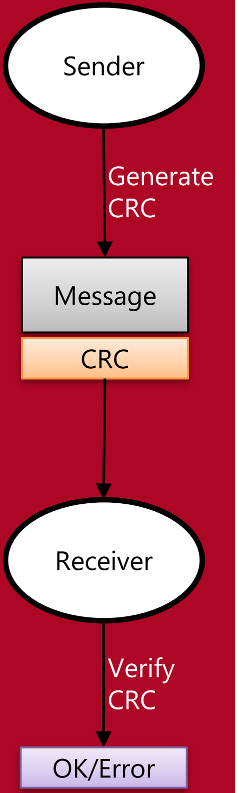
- Definition
- Synergies and conflicts
- Combined analysis
- Safety + security by design in development

Definition

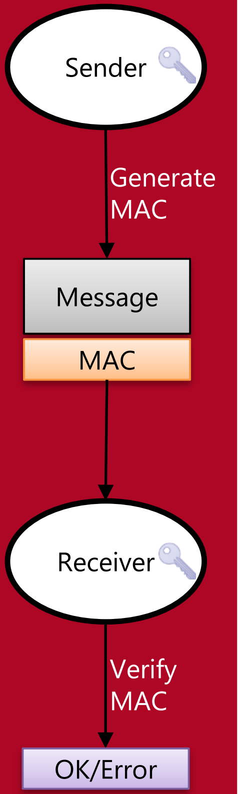
- Safety:
  - Random hardware faults
  - Systematic failures during design
    - Design failures
    - Software bugs

- Security:
  - Intentional manipulation by attackers
    - Vulnerabilities in hardware/software systems
    - Security is determined by weakest link in the system

Example 1: Data Integrity



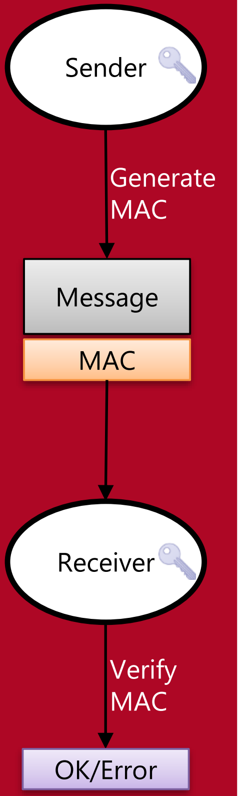
- Safety: Cyclic Redundancy Check (CRC)
  - Detect randomly distributed errors
  - Uses additional redundant data generated by binary polynomial division
  - Polynomial usually optimized at single bit errors
  - Easy to implement in SW and HW
  - Widely used in communication (e.g. CAN bus protocol)



Example 1: Data Integrity

- Security: Message Authentication Code (MAC)
  - Fixed-length keyed code representing a message
  - Uses cryptographic primitives (Hashes or block ciphers)
  - Generation and verification uses secret key
  - Infeasible for attacker to create a valid MAC without knowing the secret key
  - MAC value can be truncated
  - Error detection probability $2^{-len(MAC)}$

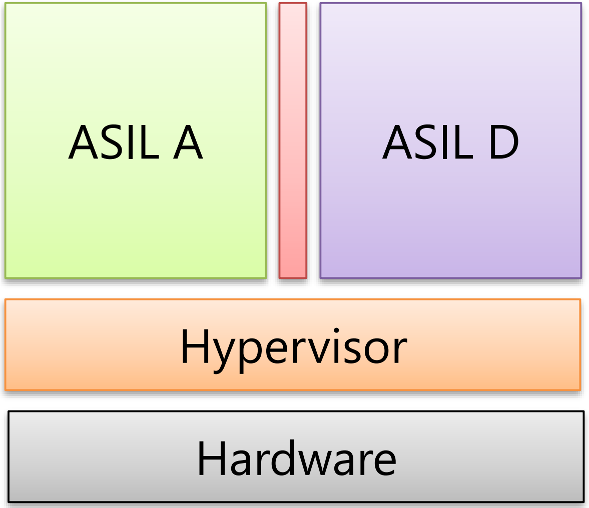
Example 1: Data Integrity



- Safety + Security:
  - CRCs can be replaced by (truncated) MACs in many systems
  - Better integrity protection (multi-bit errors are detected)
  - Authenticity: MAC calculation requires secret key
  - However: Additional complexity
    - MAC calculation more complex than CRC
    - Truncated MAC (64-128 bits) larger than CRC (16-32 bits)
    - Key Management

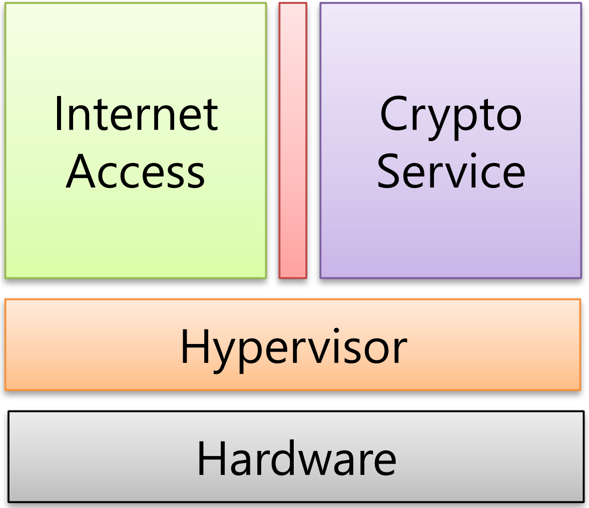
Example 2: Virtualization for CPS

- Virtualization as a Safety Measure:
  - Minimize hazards and risks
  - Separation of different criticality levels
    (e.g. ASIL A vs. ASIL D)
  - Freedom in interference



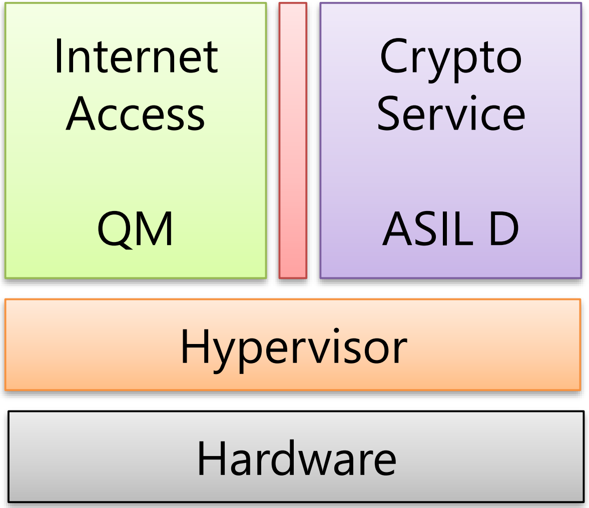
Example 2: Virtualization for CPS

- Virtualization as a Security Measure:
  - Strong separation of security-critical from non-critical services
  - Security attack on one VM (e.g. Internet Access) does not affect other VMs
  - Small trusted code base (hypervisor and crypto service)



Example 2: Virtualization for CPS

- Virtualization as Security and Security Measure:
  - Separation of different criticality levels
  - Strong separation of security-critical from non-critical services



Further Synergies

- Analysis
  - Safety: Hazard Analysis & Risk Assessment
  - Security: Security Risks Analysis
- Availability
  - Safety: Reliability, Robustness
  - Security: Absence of Denial-of-Service attacks
- Event of damage:
  - Safety: Producer’s liability
  - Security: Liability (attack on safety function), Reputation

Conflicts: Power Window

- Safety:
  - Protection against injury
  - Behavior on obstacle detection (normal car):
    - Prevent hazard
    - Stop and move window down a bit
- Security:
  - Protection against manipulation
  - Behavior on obstacle detection (high-security car):
    - Prevent access
    - Close window

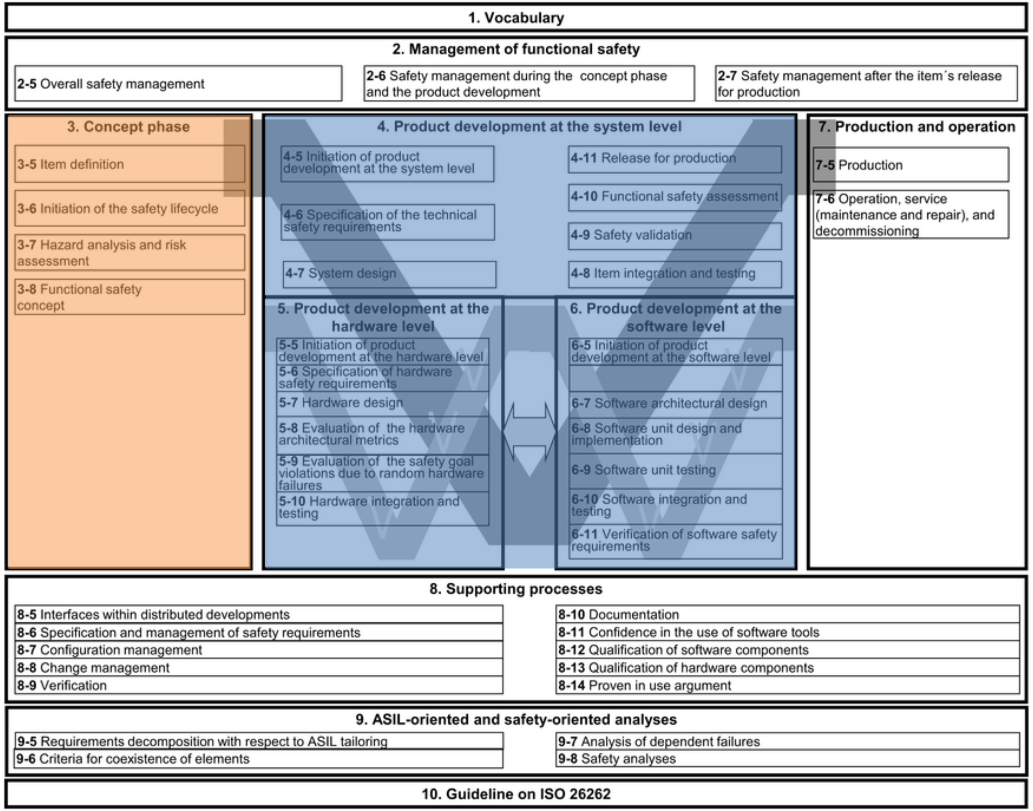
Source: Hyundai

Further Conflicts

- Safety:
  - (Hard) Real-time requirem

- Security:
  - Crypto algorithms take itional time
  -

Development Process



1. Vocabulary

2. Management of functional safety
- 2-5 Overall safety management
- 2-6 Safety management during the concept phase and the product development
- 2-7 Safety management after the item´s release for production

3. Concept phase
- 3-5 Item definition
- 3-6 Initiation of the safety lifecycle
- 3-7 Hazard analysis and risk assessment
- 3-8 Functional safety concept

4. Product development at the system level
- 4-5 Initiation of product development at the system level
- 4-6 Specification of the technical safety requirements
- 4-7 System design
- 4-8 Item integration and testing
- 4-9 Safety validation
- 4-10 Functional safety assessment
- 4-11 Release for production

5. Product development at the hardware level
- 5-5 Initiation of product development at the hardware level
- 5-6 Specification of hardware safety requirements
- 5-7 Hardware design
- 5-8 Evaluation of the hardware architectural metrics
- 5-9 Evaluation of the safety goal violations due to random hardware failures
- 5-10 Hardware integration and testing

6. Product development at the software level
- 6-5 Initiation of product development at the software level
- 6-7 Software architectural design
- 6-8 Software unit design and implementation
- 6-9 Software unit testing
- 6-10 Software integration and testing
- 6-11 Verification of software safety requirements

7. Production and operation
- 7-5 Production
- 7-6 Operation, service (maintenance and repair), and decommissioning

8. Supporting processes
- 8-5 Interfaces within distributed developments
- 8-6 Specification and management of safety requirements
- 8-7 Configuration management
- 8-8 Change management
- 8-9 Verification
- 8-10 Documentation
- 8-11 Confidence in the use of software tools
- 8-12 Qualification of software components
- 8-13 Qualification of hardware components
- 8-14 Proven in use argument

9. ASIL-oriented and safety-oriented analyses
- 9-5 Requirements decomposition with respect to ASIL tailoring
- 9-6 Criteria for coexistence of elements
- 9-7 Analysis of dependent failures
- 9-8 Safety analyses

10. Guideline on ISO 26262

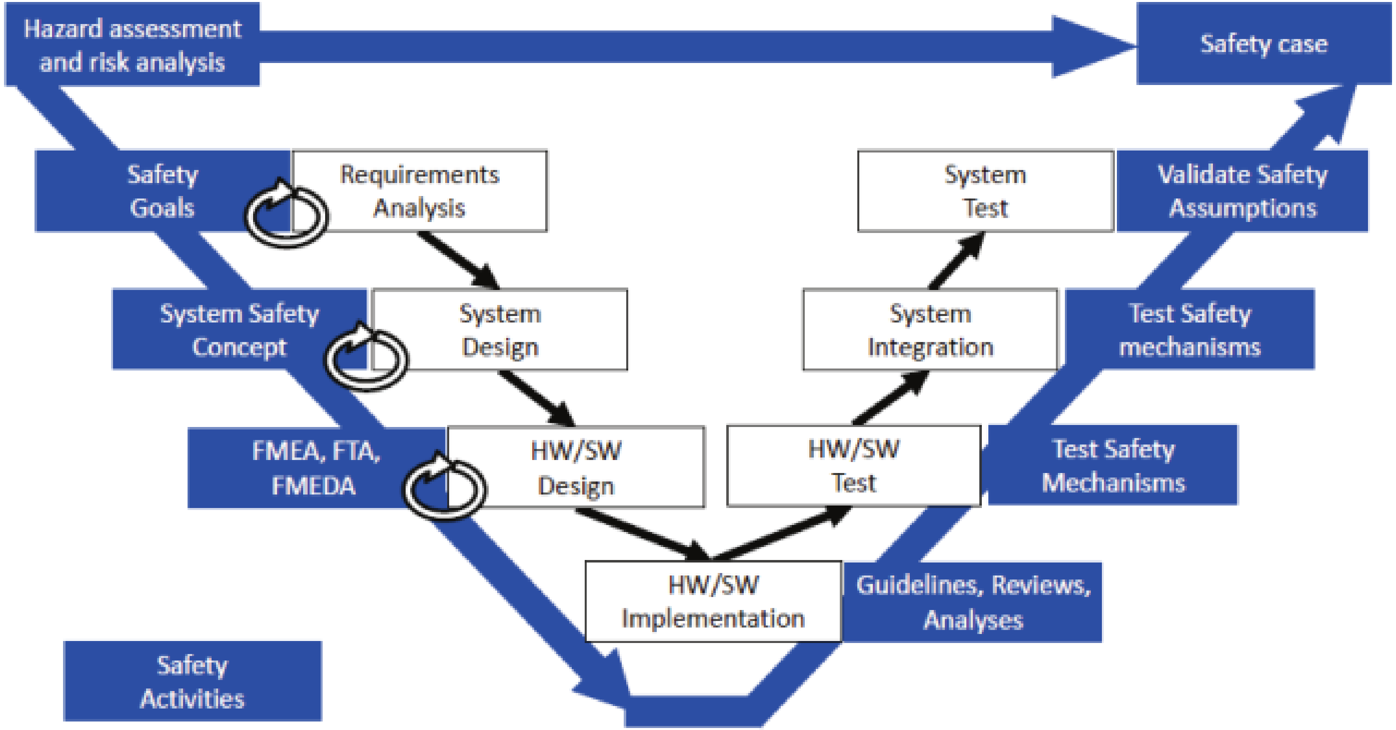
Source: ISO 26262: „Road Vehicles – Functional Safety"

Concept Phase

- Safety:
  - Analysis at design/implementation
    - Hazard analysis
    - FMEA, FTA, FMEDA
  - Included in development process
  - Stable, established, standardized

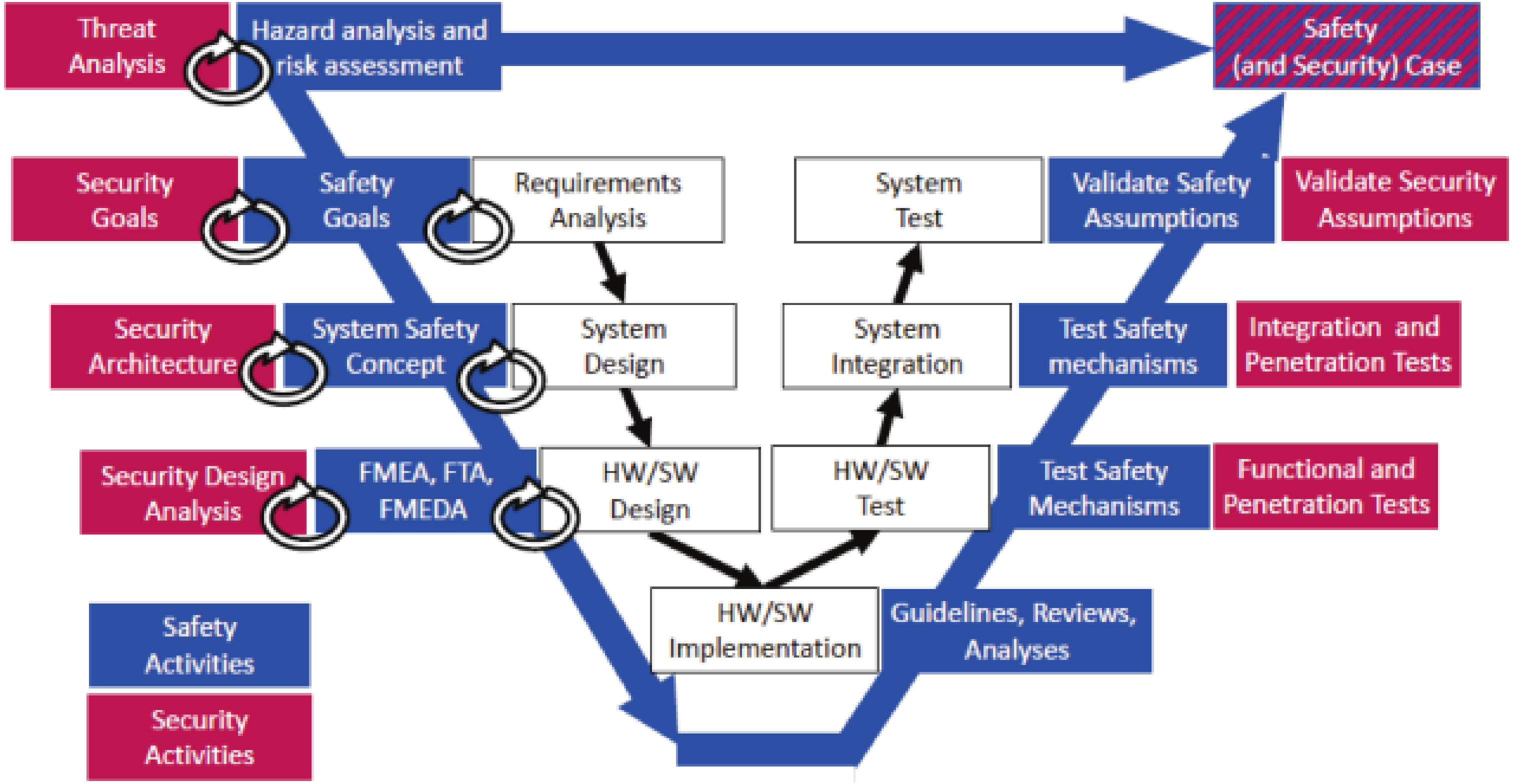
- Security:
  - Security and Risk Analysis
    - Threat and damage analysis
  - Countermeasures
    - Cryptography, HSMs, side-channel elimination
  - Moving target
    - New vulnerabilities and attacks
  - Relatively new, standards not fully established

Safety Process



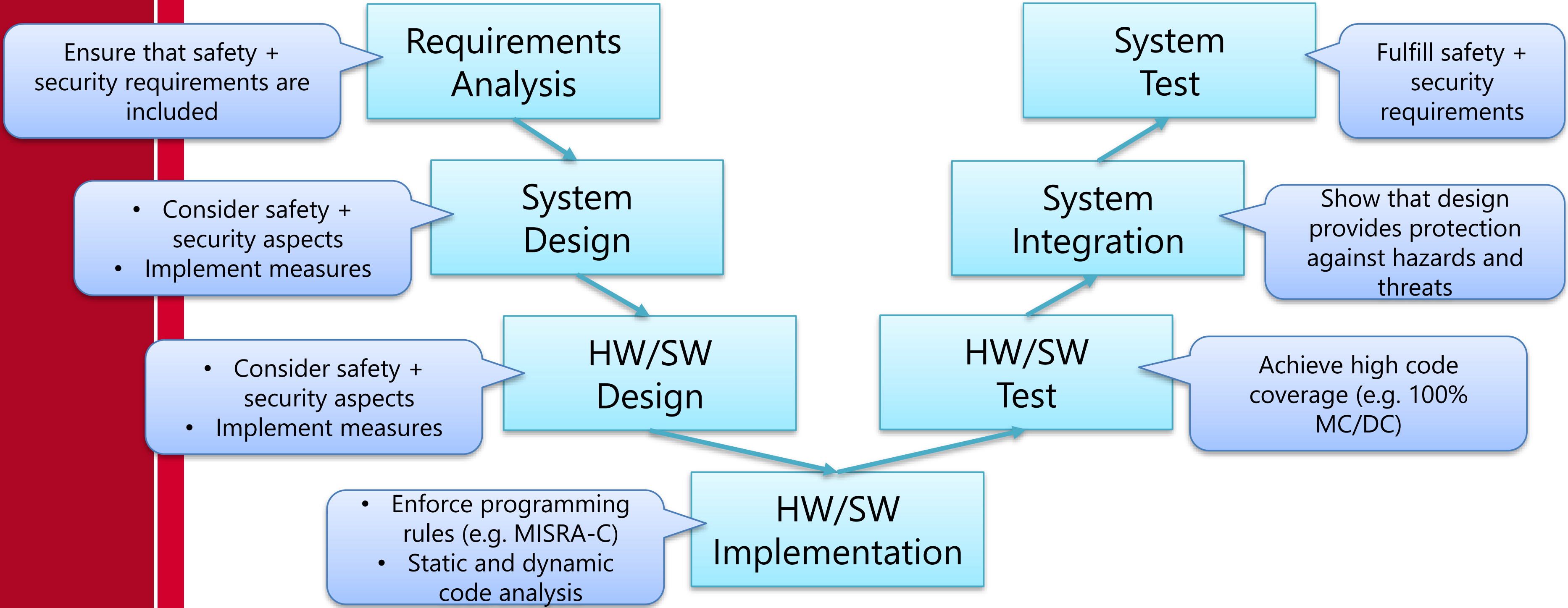
Source: „ Automotive Functional Safety = Safety + Security“, Simon Burton, *Jürgen Likkei, Priyamvadha Vembar, Marko Wolf*

Safety + Security Process



Source: „ Automotive Functional Safety = Safety + Security“, Simon Burton, *Jürgen Likkei, Priyamvadha Vembar, Marko Wolf*

Product Development Phase: Safety + Security by Design



Ensure that safety + security requirements are included

- Consider safety + security aspects
- Implement measures

- Consider safety + security aspects
- Implement measures

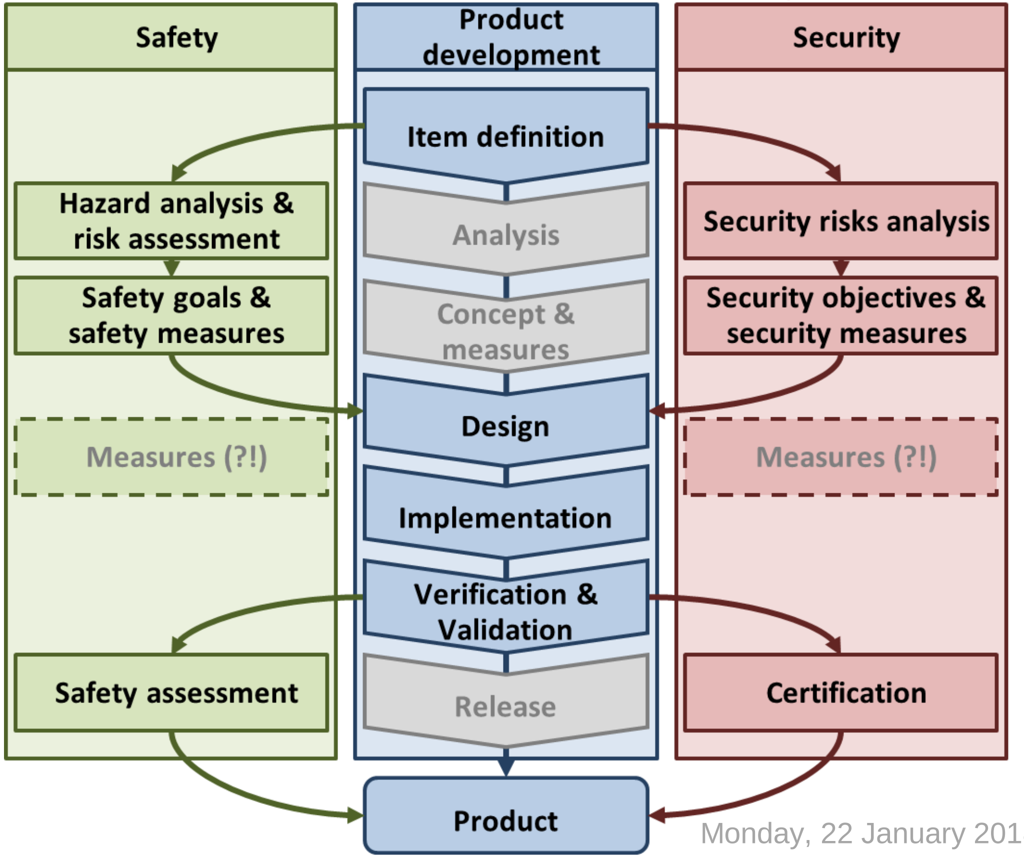
- Enforce programming rules (e.g. MISRA-C)
- Static and dynamic code analysis

Achieve high code coverage (e.g. 100% MC/DC)

Show that design provides protection against hazards and threats

Fulfill safety + security requirements

Combined Safety + Security Process



Source: „ Synergetic Safety and Security Engineering“, *Dr. Christian Eherer , Dr. Henrik J. Putzer, Franz Strasser, Dr. Marko Wolf*

Conclusion

- Combined process
  - Assists to identify synergies and potential conflicts at an early design phase
    - Synergies can then simplify development process
    - Conflicts can then be addressed separately
  - Similarities also in analyses (HARA & SRA)
  - Implementation & tests: measures from one domain also increase confidence in other (e.g. code coverage)
  - Security certification and safety assessment: achieved levels can be compared

SAFURE Grant Agreement No. 644080

"This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 644080.”

“This work was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.”

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@safure.eu

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.