

# MASP Chapter on Safety and Security

Daniel Watzenig  
Graz, Austria



<https://artemis.eu>

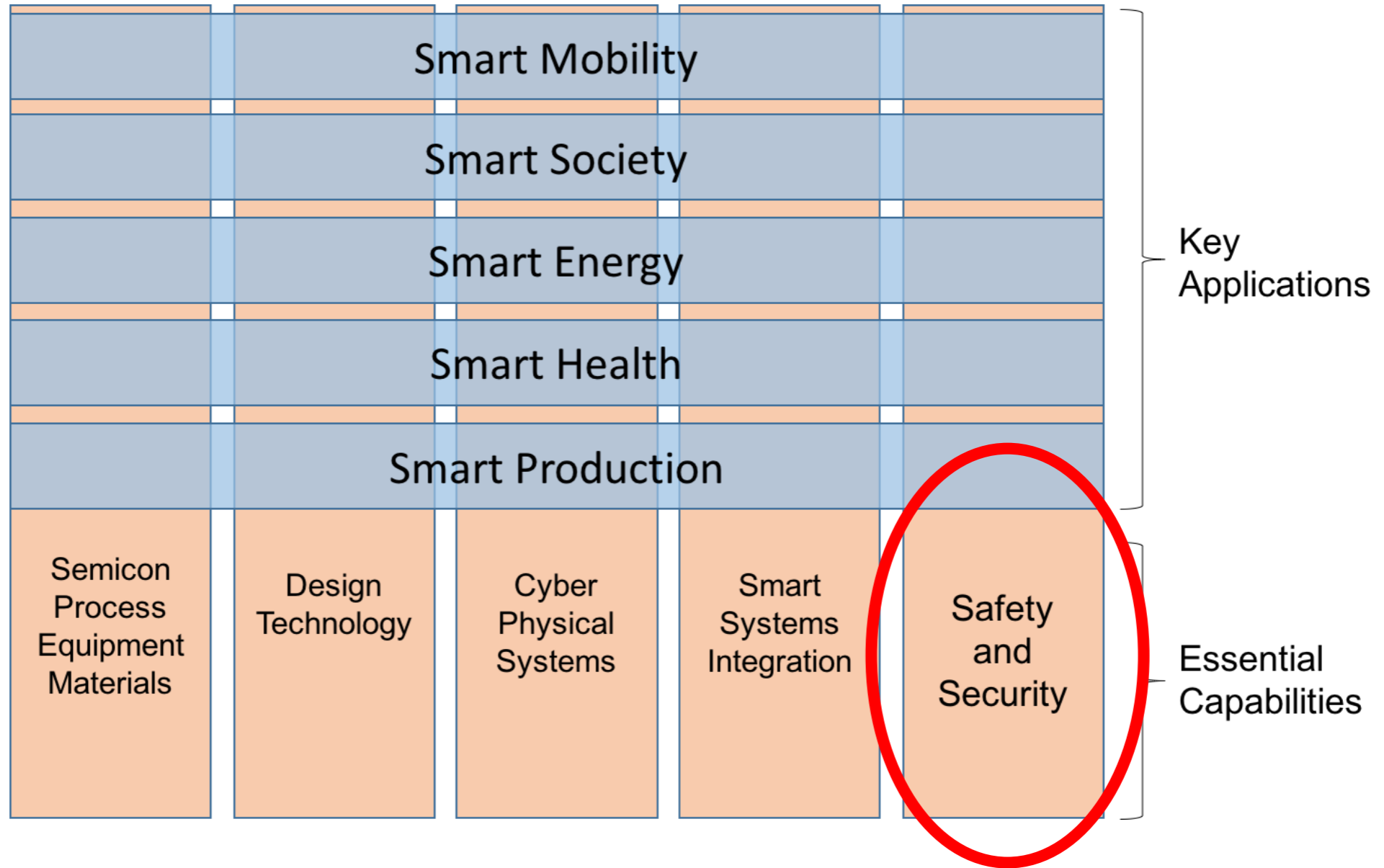
# MASP Chapter on Safety & Security

Daniel Watzenig  
[daniel.watzenig@v2c2.at](mailto:daniel.watzenig@v2c2.at)

Francois Tuot  
[francois.tuot@gemalto.com](mailto:francois.tuot@gemalto.com)

Antonio Escobar  
[antonio.escobar@infineon.com](mailto:antonio.escobar@infineon.com)





## Safety

Absence of catastrophic consequences on humans and the environment

## Security

Degree of resistance to or protection from harm

are both important criteria for **dependability** of

- Cyber-physical system (CPS)
- Embedded systems
- Industry 4.0 or Internet-of-things (IoT) environments

**Heterogeneous & contradictory** requirements: 24/7 reliability, 100% availability, 100% connectivity, real-time response, safety-critical ...

Goal: Achieve acceptable compromise between all criteria of reliability.

## Domains

- Systems engineering
- Software engineering
- Hardware engineering
- Electric/electronic systems
- Extended scope for complex systems:  
Mechanical, thermo-dynamic, mechatronic, ...

	Safety	Security
Concept phase	Hazards	Threats
System	Systematic faults	Vulnerabilities
Hardware	Faults, safety mechanism	Open HW interfaces, security mechanism
Software	Software architecture correct	Software architecture correct

## Methods

- Safety/security/reliability/dependability engineering

## Challenges:

1. Exploit expertise from each needed domain
2. Merge multiple aspects into single product

## Design challenges

- Low-cost, reliable, minimally redundant hardware
- Reliable software

## Rigorous qualification procedures

- Assess known failures, system malfunctions, subsequent failures
- New product development vs. changes & modifications
- Minimize re-certification cost

## Verification & validation

- Especially for connected and highly networked systems
- Better methods and tools
- Supporting (incremental) certification
- Achieve cost-savings

## **Security & privacy by design**

- Affects entire product life cycle, not just development
- Data loss, misuse, unwanted modification, unauthorized access

## **Quantified verification**

- For safety & security
- Definition of standard metrics & targets
- Measurable methods needed

## **Long term security**

- Increased availability of cheap, powerful hardware
- New threats and attacks appear, new interfaces used for attacks
- Low entry barriers for hackers & criminals, e.g. spoofing, jamming, eavesdropping

## **Systematically reduce complexity, increase reliability, robustness**

- Strategies: Enforce overall system views, re-use mechanisms, application of safety & security patterns, new cryptographic techniques & algorithms

## **New design tools**

- Strategies: Safety & security co-analyses, new metrics, simulation for safety & security analyses, specification of building blocks for safe & secure systems

## **Dynamic reconfiguration**

- Strategies: Virtual components, connection establishment & release

## **Robust control & self-diagnostics**

- Strategies: Adapt under security attacks, react to random faults and unpredictable events, deal with sensor misinterpretations



### **Evaluation and experimentation**

- Strategies: Extended simulation & test bed infrastructure, interfaces to human decision making

### **New architectures**

- Strategies: Integration of security by design, modularity and re-use of safe and secure components, secure HW building blocks, SW libraries & components

### **Safe & secure real-time systems**

- Strategies: Safe & secure fault diagnosis & maintenance, wireless protocols, dynamically reconfigurable systems, fault tolerance

### **(Re-)Certification**

- Strategies: Modular certification of composable designs, proof absence of high-impact failure modes, worst-case-execution time research

### **Identity & access management**

- Strategies: Identity management & authentication mechanisms, key generation & management, anti-counterfeiting techniques, trusted devices

### **Data protection**

- Strategies: Protection & update in the field, transmission and distribution, E2E security, secure storage, protection against HW trojans

### **Safe & secure execution platforms**

- Strategies: Trusted platform modules (TPM), trusted execution environments (TEE), embedded secure elements, secure boot processes

### **Infrastructures**

- Strategies: Vehicle interconnections (Car2X), infrastructure protection & monitoring, detection of abnormal behaviour, safe & secure behaviour

### **Cryptography**

- Strategies: homomorphic encryption, quantum cryptography, post quantum cryptography

### **Protocols**

- Strategies: Mathematical analyses to design new scalable protocols for mass distribution (connected smart devices)

### **Chip architecture**

- Strategies: Design of monolithic or distributed secure enclaves, dedicated processors plus additional protection units



**Increased competition**

**Business success**

by absence of theft, fraud,  
closure, downtime

**Scalability effects**

**New markets**

**New investments**

by saved costs

**High rated value-added chain**

by understanding and awareness

**Connected & smart systems:**

**Products, applications, services, devices**

**Smart cities**

**Smart energy solutions**

**Connected vehicles**

**Smart grids**

**Smart health care**

**Safety & Security**

### **Safety & security are valid criteria for all applications addressed in the MASP**

- Cyber-physical systems
- Smart systems integration

### **Relevant for all MASP key applications (Smart X)**

### **Standardization activities: some examples**

- ISO 26262: 2nd edition for automotive E/E engineering, Spring 2018
- ISO PAS 21448 SOTIF (Safety of the intended functionality)
- SAE J3061: “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”, 19.1.2016
  - Rationale: To provide a **cybersecurity process framework** and guidance to help organizations identify and assess cybersecurity threats and design cybersecurity into cyber-physical vehicle systems **throughout the entire development lifecycle process**
  - Relation to Safety: The process framework described in this document is **analogous to the process framework described in ISO 26262** Functional Safety Road Vehicles. These two processes are different, but are related and require integrated communications in order to maintain consistency and completeness between an organizations safety process outputs and their Cybersecurity process outputs.

## 11 topics are currently adressed

- **Safety, security & privacy by design**
- **Authentication**
- **Distributed models of trust**
- **Decentralized trust frameworks (blockchain)**
- **Data Protection**
- **Network Protection**
- **Safety and security risks related to infrastructures (systems of systems, cloud, new generation networks)**
- **Safe and secure execution platforms**
- **Safe and secure updates in the field**
- **Safety and security aware development**
- **Safe and secure services**



## 11 topics addressed

Example topic:

Safety, security & privacy by design

### 2020+

- Fully integrated requirements, frameworks, tools and standards
- Advanced authentication
- Unified computational trust models
- Continuous monitoring and certification
- Privacy and security by design
- Standardized models for most effective solutions
- Rollout of updateable systems

### 2018-2019

- Advanced security schemes & safety patterns
- Multiple authentication options
- Integration of secure architectures
- Deployment of trust models
- Secure data storage & management
- Safe & secure architectures, virtualization
- Increased automation in development

### 2017

- Requirement specification
- Scenario definition
- Architecture analysis
- Theoretical model studies
- Existing technology evaluation
- Identification of criteria, threats, metrics

#### Safety, security & privacy by design

Requirement specification for safety, security, privacy and trust

Advanced tools and methods to support security schemes and safety patterns for focused problem areas

Fully integrated safety and security requirements & generic components and frameworks

# MASP Chapter on Safety and Security

Daniel Watzenig  
Graz, Austria



<https://artemis.eu>