THINK SAFE THINK ICS

industrial engineering

Safety & Security

Integrated Development

industrial engineering

Benefit from our experience

Save expensive and lengthy training programs and start immediately in your project. Insert our engineers targeted precisely to the phases of the project in which their knowledge is required. This opens up the possibility of a holistic support of your project in a responsibility - from the first design to the finished system (process definition, concept creation, training and realisation).

Gain time in your projects, through the companionship of our experts in the execution of an integrated Safety-/Security process in your project landscape.

Minimize the risks of a project delay, which can occur through the integration of a new Safety-/Security process in your existing development environment. Our longstanding project experience with OEMs and Tier-1-supplier helps to effectively manage functional safety (Safety) in accordance to ISO 26262 (Security plan/proof, audits, reviews and assessments).

Secure the position of the independent observer at the:

- Execution of a systematical risk analysis for hazards/threats
- Safety analysis (FMEA, FTA, FMEDA, Attack tree analysis)
- Identification and creation of Safety-/Security-requirements

What is safety and security about?

Challenges at the networked vehicle

Today's automobiles have quite a few electronic and electrical systems (E/E systems) embedded to realize existing and new functions.

That includes basic functions like light, wiper, etc. but also diagnostic-interfaces, infotainment, driver assistance systems, e-mobility, mobile services up to autonomous driving.

Malfunctions in these E / E systems, which may lead to hazards for traffic users, must be sufficiently reduced. ***(Safety).***

Today's E/E systems are connected via Networks.

Therefore, cyberattacks which are focused on these systems and beyond, violate the systems security, the privacy of users and may lead to operational and financial damage. These new challenges must be counteracted with sufficient care in the form of cyber protection ***(Security).***

Challenges at the networked vehicle

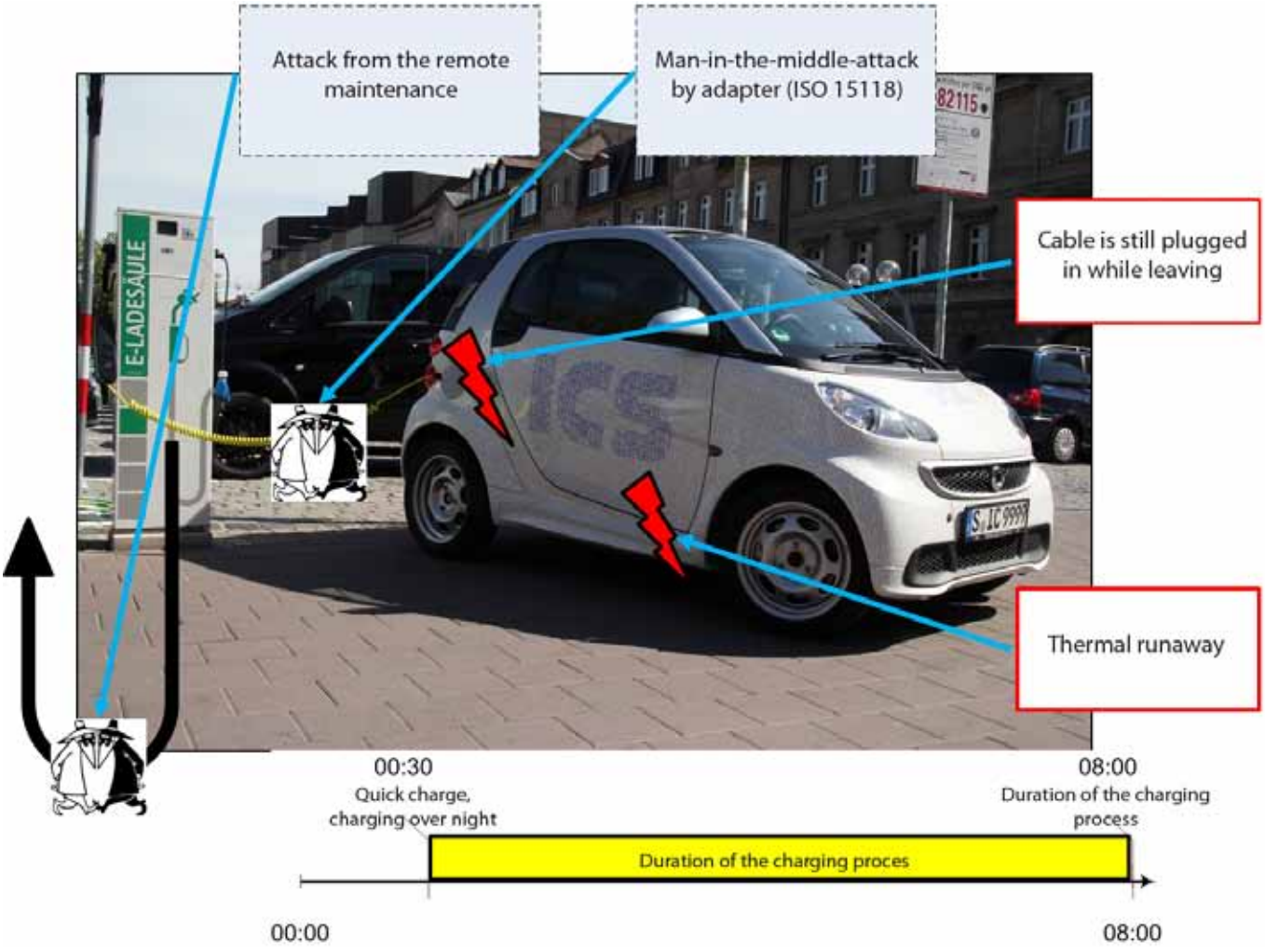

Figure 1:
Example of an electric vehicle charged on an intelligent charging station.
Hazards in the viewpoint of safety (red) are for example the self-heating of the HV battery (Thermal Runaway) or leaving of the plugged charging cable. Hazards in the viewpoint of Security (grey) are man-in-the-middle-attack through a manipulated charging adapter or malicious manipulation of the loading process through remote maintenance.

Safety and Security

Similarities and Differences

Is it possible to handle safety and security within a common process?

The challenge is that between the two disciplines exist significantly **differences** depending on the level of consideration:

Level of consideration	Safety	Security
System view	Technical system harms humans/environment unintended	Humans harm humans/environment purposefully
Danger assessment	Hazards are rated by statistics, experience values, knowledge about the system, its components and interactions	Threads are intended malicious activities and as such are difficult to predict
Goal	Safe state	Permanent IT- Security process
Risk analysis	Fault-Tree-Analysis	Attack-Tree-Analysis
Hardware failure	Random failures	Attacks from vulnerable locations
Goal of software validation	Proof of validity of software	Vulnerabilities of valid software
System integration test	Fault-Injection-Test	Penetration-Test

Safety and Security

Similarities

However, with all these differences, similarities between safety and security can be discerned:

- Safety as well as Security have to be considered in the concept and design phase; in both cases it isn't possible to force it "into the code" during implementation phase
- Risk analyses are the entry points for both life cycles
- The results of these risk analyses are the basis for the derivation of Safety and security requirements
- To fulfill these requirements, safety and security mechanisms have to be implemented and verified.

An integrated approach for both aspects

To derive an applicable process for safety and security, it is thus advisable to proceed in accordance with ISO 26262, using the definition of the item and to start with the risk analysis.

- For the sector Safety a Hazard and Risk Analysis according ISO 26262 is executed.
- Similarly, we undergo the subject of consideration a threat analysis. Here we use the golden rule:

  Risk = Threat x Vulnerability x consequence
- With these conclusions, resulting from both hazard an threat analysis - requirements for safety and security are derived, which have to be implemented by suitable measures

- The **threat landscape** is determined from the possible attackers, their motivation and their most likely attack vectors (attacker‘s characteristics).
- Vulnerability describes attack points of the system and the necessary level of skills and resources to exploit these.
- The **consequences** occur in different areas (reliability, data protection, finance, availability) in different gradations. The ICS AG offers a suitable classification in consequence classes here.
- In the **threat analysis** are the countermeasures already defined at the system level

- Safety analyses (fault tree analysis for safety, attack tree analysis for security) verifies whether the hazards or threats are used adequately compensated by measures.
- Once the measures been implemented, they shall be tested for compliance with the requirements. The testing procedures are analogous: At safety, the verification takes place through fault-injection-tests, security uses penetration testing.
- For the concept phase and the system development, the strategy for the major steps will look like E.g. as shown in the following figure:

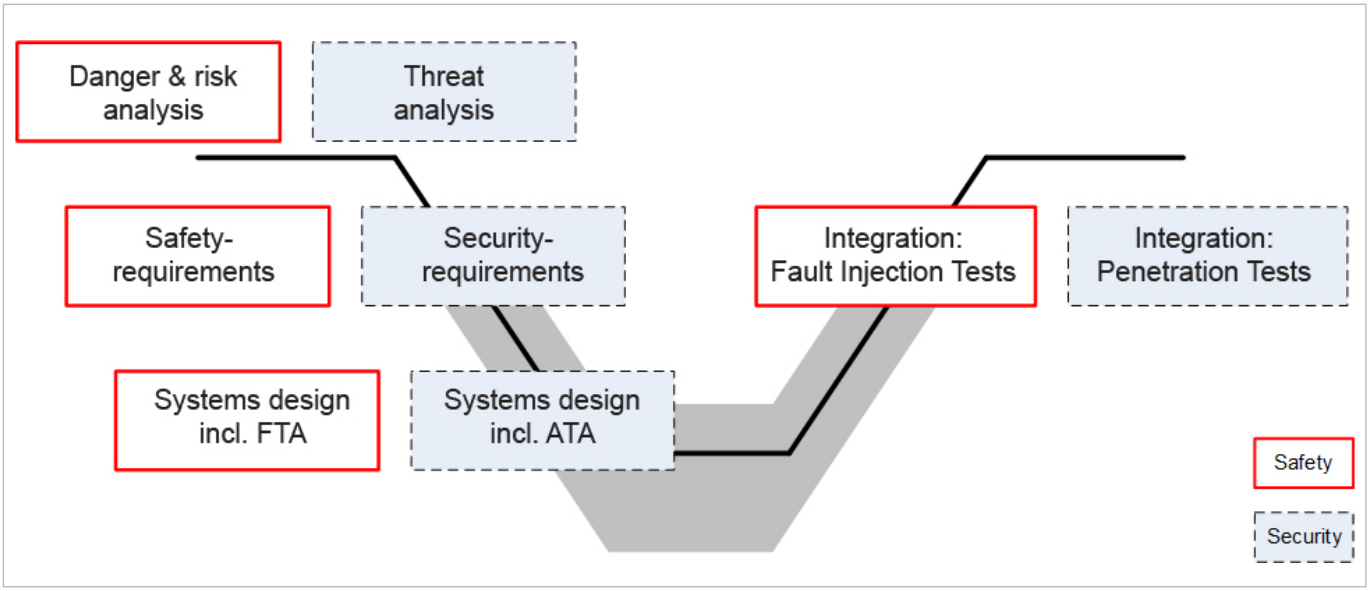

Figure 2:
Example of chronologycal steps at phase of conception and systems development.

About ICS AG

We are a medium-sized, family-owned IT consulting and engineering - company. Since 1966, we develop intelligent solutions for safety-critical environments. Our service comprises the entire product life cycle from conception to approval of a system.

With 50 years of experience in the IT industry, the ICS AG is one of the renowned Consulting and System and Software providers in the Stuttgart area and beyond.

Are you responsible for a component with special safety features? You want or need to reach a documentation requiring safety certification in your system to be developed?

In all respects, you are in good hands with our experts from the Business Unit Industrial Engineering.

Your Contact:
Martin.Zappe@ics-ag.de

Contact:

ICS AG
Sonnenbergstr. 13
70184 Stuttgart

T +49 711 2 10 37 00
industry@ics-ag.de
www.ics-ag.de