THINK SAFE THINK ICS

industrial engineering

Safety & Security

integrierte Entwicklung

industrial engineering

Profitieren Sie von unserer Erfahrung

Sparen Sie sich teure und langwierige Ausbildungsprogramme und **starten Sie** sofort in Ihr Projekt. Setzen Sie unsere Ingenieure zielgerichtet genau zu den Projektphasen ein, in denen ihr Wissen gefordert ist. Das eröffnet Ihnen die Möglichkeit einer ganzheitlichen Betreuung Ihres Projektes in einer Verantwortung - von der ersten Konzeption bis zum fertigen System (Prozessdefinition, Konzepterstellung, Schulung und Realisierung).

Gewinnen Sie Zeit in Ihrem Projekt, indem Sie sich von unseren Experten in der Umsetzung eines integrierten Safety-/Security-Prozesses in Ihrer Projektlandschaft begleiten lassen.

Minimieren Sie das Risiko eines Projektverzuges, der durch Einführung eines neuen Safety- / Sicherheitsprozesses in Ihren bestehenden Entwicklungsprozess eintreten kann. Unsere langjährige Projekterfahrung bei OEMs und Tier-1-Zulieferern hilft Ihnen, die funktionale Sicherheit (Safety) nach ISO 26262 effektiv zu managen (Sicherheitsplan/-nachweis, Audits, Reviews und Assessments).

Sichern Sie sich den Standpunkt eines **neutralen Betrachters** bei der:

- Durchführung von Risikoanalysen (FMEA, FTA, FMEDA, Angriffsbaumanalyse)
- Identifikation und Erstellung von Sicherheitsanforderungen
- Durchführung einer systematischen Bedrohungsanalyse

Abbildung 1:
*Beispiel E-Fahrzeug beim Laden an einer intelligenten Ladestation: Gefährdungen aus Sicht der **Safety (rot)** sind z.B. die Selbstaufheizung der Hochvolt-Batterie (Thermal Runaway) oder das Steckenlassen des Ladekabels. Bedrohungen aus Sicht der **Security (grau)** wären ein Man-in-the-middle-Angriff über einen manipulierten Ladeadapter oder eine böswillige Manipulation des Ladevorgangs über die Fernwartung.*

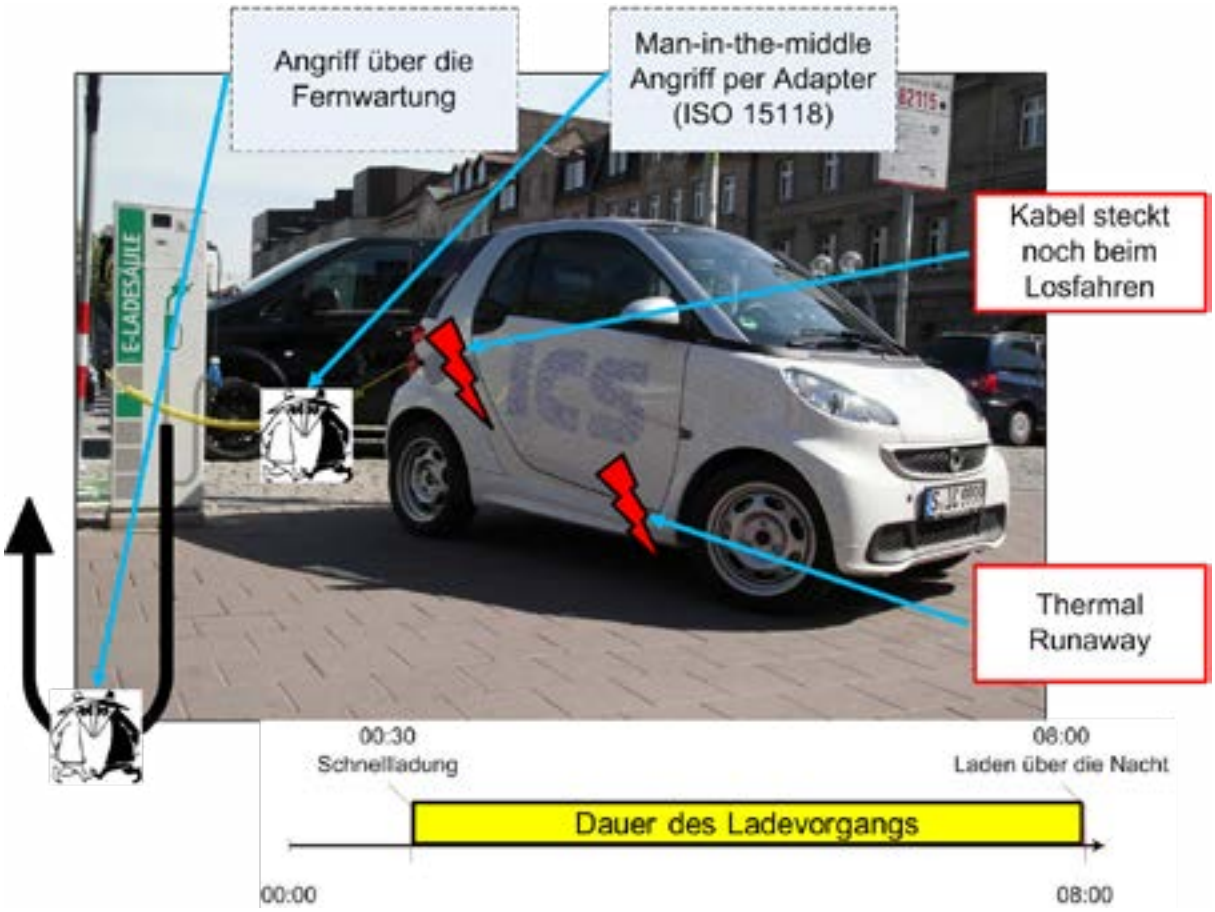
Worum geht es bei Safety und Security?

Herausforderungen im vernetzten Fahrzeug

In heutigen Fahrzeugen wird eine hohe Anzahl an elektrischen und elektronischen Systemen (kurz E/E-Systeme) eingesetzt, um bestehende und neue Funktionen zu realisieren. Dazu zählen die Grundfunktionen (wie z.B. Licht, Scheibenwischer etc.), aber auch Diagnoseschnittstellen, Infotainment, Fahrerassistenzsysteme, E-Mobilität, Mobile Dienste bis hin zum autonomen Fahren.

Fehlfunktionen in diesen E/E-Systemen, die zu Gefährdungen für die Verkehrsteilnehmer führen können, müssen hinreichend gemindert werden *(Safety)*.

Die heutigen E/E-Systeme führen ihre spezifischen Funktionen in der Regel im Netzverbund aus. Deshalb können Cyber-Attacken die Sicherheit von diesen Systemen und darüber hinaus die Privatsphäre der Nutzer verletzen, sowie zu operativen und finanziellen Schäden führen. Diesen neuen Herausforderungen muss mit hinreichender Sorgfalt in Form des Cyber-Schutzes entgegengewirkt werden *(Security)*.



Safety und Security

Gemeinsamkeiten und Unterschiede

Ist es möglich, Safety und Security innerhalb eines gemeinsamen Prozesses zu behandeln?

Die Herausforderung besteht darin, dass zwischen den beiden Disziplinen je nach Betrachtungsebene deutliche **Unterschiede** bestehen:

Betrachtungsebene	Safety	Security
Systemsicht	Technisches System gefährdet Menschen/Umwelt unabsichtlich	Menschen gefährden Menschen/ Umwelt absichtlich
Gefahreneinschätzung	Gefährdungen können durch Statistiken, Erfahrungswerte, Wissen über das System, seine Komponenten und seine Wechselwirkungen eingeschätzt werden	Bedrohungen sind absichtliche, bösartige Aktivitäten und sind als solche schwer vorherzusehen
Ziel	Sicherer Zustand	Permanenter IT-Sicherheitsprozess
Risikoanalyse	Fehlerbaumanalyse	Angriffsbaumanalyse
Hardwarefehler	Zufällige Ausfälle	Angriffe über verwundbare Stellen
Ziel der Softwarevalidierung	Nachweis der Gültigkeit des Programmcodes	Verwundbarkeiten des gültigen Programmcodes
Systemintegrationstest	Fault-Injection-Tests	Penetration-Testing

Gemeinsamkeiten

Bei all diesen Unterschieden sind jedoch auch Gemeinsamkeiten zwischen Safety und Security auszumachen:

- Sowohl Safety als auch Security müssen schon während der Konzept- und der Design-Phase betrachtet werden; beide lassen sich nicht später „hineintesten“
- Die Risikoanalysen sind die Einstiegspunkte für den Sicherheitslebenszyklus
- Die Ergebnisse dieser Risikoanalysen bilden die Basis für die Herleitung von Safety- bzw. Security-Anforderungen
- Um die Anforderungen zu erfüllen, sind entsprechende Safety-Mechanismen bzw. Security-Maßnahmen zu implementieren und zu verifizieren.

Ein integriertes Vorgehen für beide Aspekte

Um einen für Automotive anwendbaren Prozess für Safety und Security zu erhalten, bietet es sich also an, analog zur ISO 26262 vorzugehen und nach Definition des Betrachtungsgegenstandes mit den Gefahrenanalysen zu beginnen.

- Für den Bereich Safety wird eine Gefährdungs- und Risikoanalyse gemäß ISO 26262 durchgeführt.
- Analog dazu unterziehen wir den Betrachtungsgegenstand einer Bedrohungsanalyse. Hier gilt die Faustregel

  Risiko = Bedrohung × Verwundbarkeit × Konsequenz
- Aus den Ergebnissen der beiden Gefahrenanalysen werden Anforderungen für Safety und Security abgeleitet, die durch geeignete Maßnahmen umzusetzen sind.
- Durch Risikoanalysen (Fehlerbaumanalyse bei Safety, Angriffsbaumanalyse bei Security) wird überprüft, ob die Gefährdungen und Bedrohungen ausreichend durch Maßnahmen abgewendet werden.

- Die **Bedrohungslage** bestimmt sich aus den möglichen Angreifern, deren Motivation und deren wahrscheinlichsten Angriffsmethoden (Angreifersteckbriefe).
- Die **Verwundbarkeit** beschreibt Angriffspunkte des Systems und die notwendigen Level an Fähigkeiten und Ressourcen, diese auszunutzen.
- Die **Konsequenzen** treten in verschiedenen Bereichen (Betriebssicherheit, Datenschutz, Finanzen, Verfügbarkeit) in unterschiedlichen Abstufungen auf. Die ICS GmbH bietet hier eine geeignete Einordnung in Konsequenzklassen.
- In der **Bedrohungsanalyse** werden bereits die Gegenmaßnahmen auf Systemebene festgelegt.

- Wurden die Maßnahmen umgesetzt, sind diese auf Erfüllung der Anforderungen zu testen. Die Testverfahren sind analog: Bei Safety findet die Überprüfung durch Fault-injection-Tests statt, bei Security benutzt man Penetration-Test-Verfahren.
- Für die Konzeptphase und die Systementwicklung wird das Vorgehen bei den wichtigsten Schritten dann z.B. wie in nachstehender Abbildung aussehen:

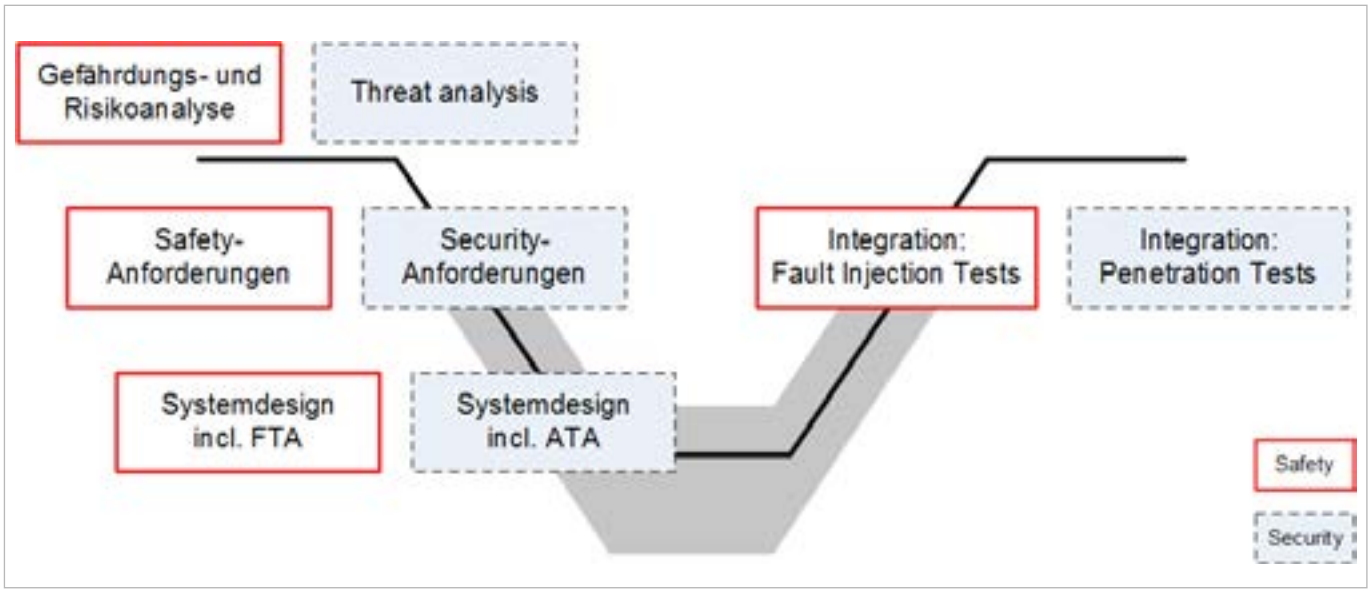


Abbildung 2:
Beispielhafte Abfolge der einzelnen Schritte für Konzeptphase und Systementwicklung.

Über die ICS GmbH

Die ICS GmbH ist seit mehr als 50 Jahren ein erfolgreiches IT-Beratungs- und Engineering-Unternehmen. Seit 1966 entwickeln wir zuverlässige Lösungen für sicherheitskritische IT-Umgebungen. Intelligente und sichere Prozesse in komplexen Umgebungen sowie zufriedene Kunden zeichnen uns aus.

Wir sind spezialisiert auf die Geschäftsfelder Industrial Engineering (Automation, Supply Chain, Logistics, Automotive), Transportation (Railway) und die Bereiche Funktionale Sicherheit, Security & Safety sowie Informationssicherheit und DSGVO.

Sie sind verantwortlich für ein Bauteil mit besonderen sicherheitsrelevanten Merkmalen? Sie wollen oder müssen eine dokumentationspflichtige Sicherheits-Zertifizierung Ihres zu entwickelnden Systems erreichen?

In allen Punkten sind Sie gut aufgehoben bei unseren Experten der Business Unit Industrial Engineering.

Ihr Ansprechpartner:
Martin.Zappe@ics-ag.de

>>ICS-Downloads

Kontakt

ICS GmbH
Sonnenbergstr. 13
70184 Stuttgart

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