

Safety & Security

Thomas Jäger
Betreuerin: Bettina Buth

SAFETY & SECURITY

Agenda

- **Motivation**
- **Einführung in das Thema**
 - Begriffe und Abgrenzung
 - Verschmelzung
- **Beispiel**
- **Probleme und Herausforderungen**
- **Forschungsstand Lösungsansätze**
- **Mögliche Projekte / Zielsetzung**
- **Konferenzen**
- **Quellen**

SAFETY & SECURITY

Motivation

- Bachelorarbeit im Bereich Security
 - „Implementierung eines Intrusion Detection Systems auf einem Single Board Computer“
- Nebenjob: Softwaretester in FinTech-Unternehmen
 - Safety-kritische Bestandteile

=> Safety + Security

SAFETY & SECURITY

Einführung in das Thema: Begriffe und Abgrenzung

Safety-kritische Systeme

- Traditionell von der Umwelt isolierte Einheit
- Beispiele:
 - Autos
 - Produktionsmaschinen

Security-kritische Systeme

- Nicht-isoliertes System
- Beispiele:
 - Clouds
 - Firmennetzwerke
 - Software für Finanzdienstleistungen

SAFETY & SECURITY

Einführung in das Thema: Begriffe und Abgrenzung

Safety Systeme

Gefahren

- Finanzieller Schaden
- Personenschäden
- Umweltschäden



Schutz der Umwelt vor System:

- Isolation
- Gegen zufällig auftretende, systeminterne Fehlfunktionen/Ausfälle
- Security-Maßnahmen oft auf Offline-Datenschutz beschränkt

Security Systeme

Gefahren

- Datenverlust
- Datenmanipulation
- Datendiebstahl



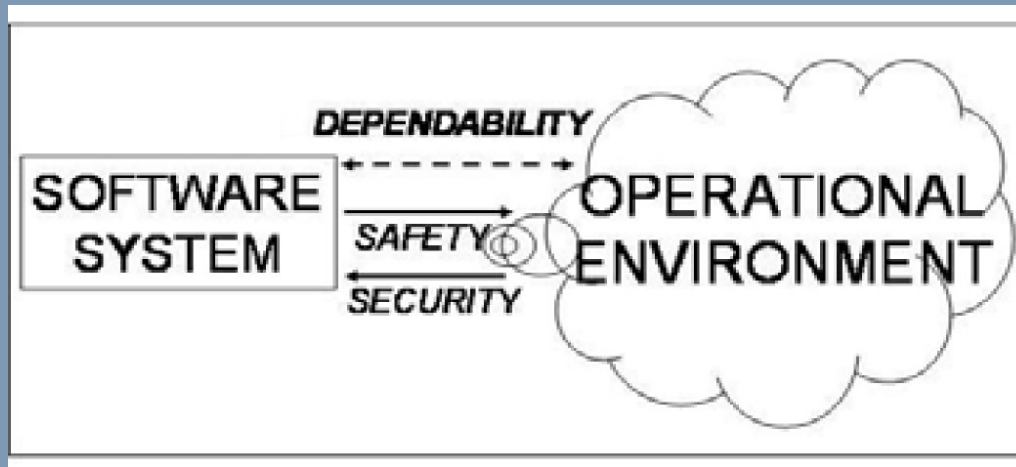
Schutz des Systems vor Umwelt:

- Isolation
- Kryptographische Methoden
- Authentifizierung

SAFETY & SECURITY

Einführung in das Thema: Verschmelzung

- Ausbreitung des Internets/Digitalisierung
 - Verbreitung vernetzter Komponenten in Safety-kritischen Systemen
 - Schnittstellen bieten Angriffsfläche
- => Angriff führt kann zu Fehlfunktion/Ausfall in kritischem System führen



Andrew J. Kornecki and Janusz Zalewsky "Safety and Security in Industrial Control"[1]

SAFETY & SECURITY

Beispiel: Automobilindustrie^[3]

Wachsende Anzahl safety-kritischer Komponenten in Fahrzeugen

- Steigende Komplexität und Grad der Interaktion der Komponenten
 - Untereinander
 - Mit anderen Systemen
- Steigende kabellose Kommunikation der Komponenten

SAFETY & SECURITY

Beispiel: Automobilindustrie[3]

Beispiel: Spurhalteassistent

- Löst aus, wenn Fahrzeug ungewollt die Spur verlässt
- Sendet Warnung an Fahrer und korrigiert die Richtung

Potentielle Gefahrenquellen:

- Verwendet verschiedene, zusammenwirkende Komponenten (z.B. visuelle Quellen, wie Kamera)
- Viele Schnittstellen, mögliche Angriffspunkte

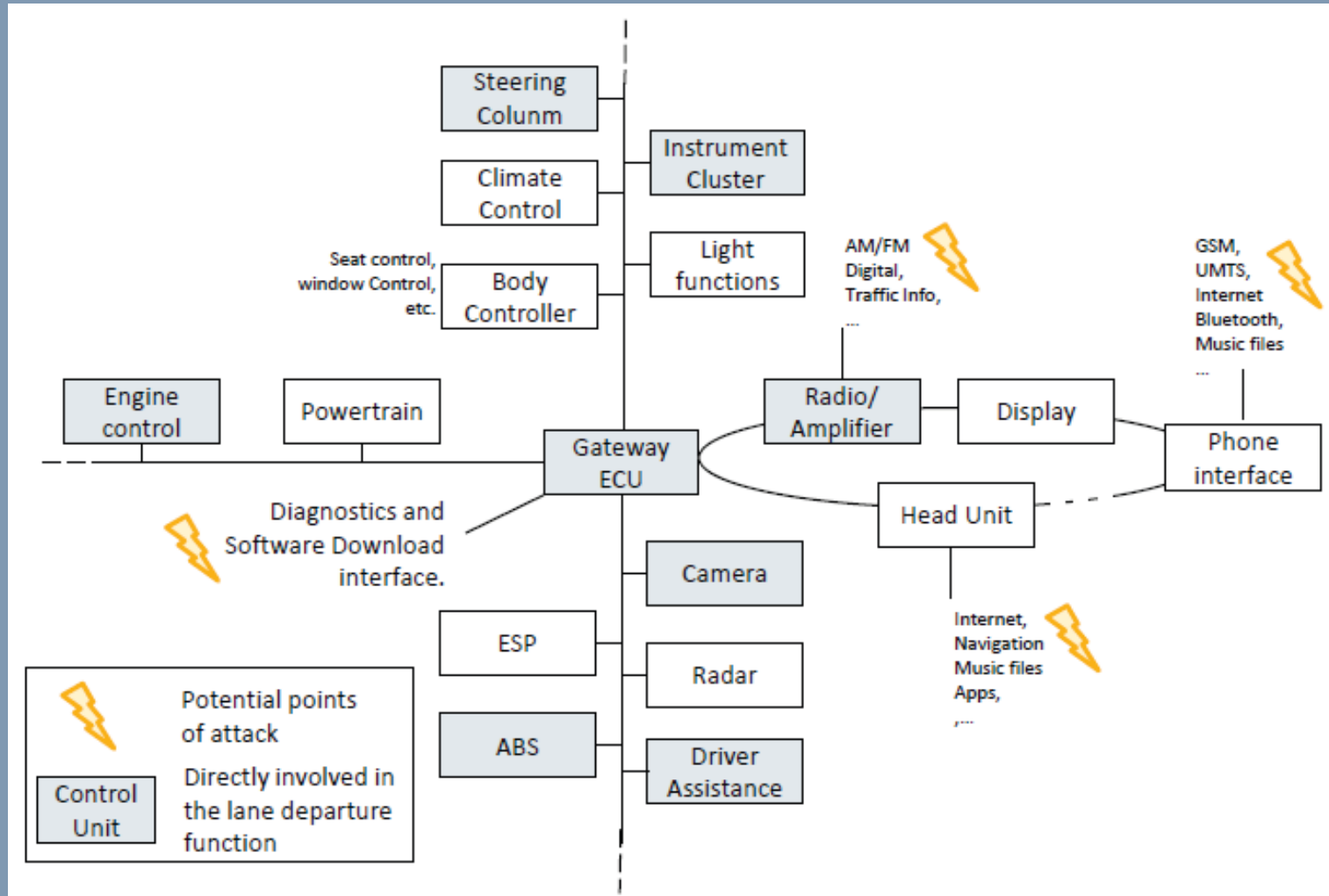
=> Einschleusen von falschen Nachrichten
(z.B. Kamera, falsche Vorfälle)

Mögliche Folgen:

- Ungewollte Warnungen
- Ungewollte Steuerung
- Verhinderte Ausweichmanöver

SAFETY & SECURITY

Beispiel: Automobilindustrie[3]



Simon Burton, Jürgen
Likkei, Marko Wolf
"Automotive Functional
Safety = Safety + Security"
[3]

SAFETY & SECURITY

Probleme und Herausforderungen

„Safety and Security in Industrial Control“^[1]

Andrew J. Kornecki: Electrical, Computer, Software & System Eng. , Embry Riddle Aeronautical University

Janusz Zalewski: Computer Science, Florida Gulf State University

SAFETY & SECURITY

Probleme und Herausforderungen^[1]

- Safety und Security werden als zwei getrennte Bereiche betrachtet
- Bisherige Safety Systeme sind nicht gegen Attacken von Außen konzipiert
 - Bei Integration entstehen ungeschützte Schnittstellen
- Kabellose Verbindungen machen Systeme von Außen verwundbar
- Security-Spezialisten sind nicht mit Safety-Richtlinien vertraut
- Wissenslücke für Safety-Security Problematik

SAFETY & SECURITY

Forschungsstand Lösungsansätze

„Automotive Functional Safety = Safety + Security“ [3]

Simon Burton: ETAS GmbH

Jürgen Likkei & Priyamvadha Vembar: Robert Bosch GmbH

Marko Wolf: ESCRYPT GmbH

- Erweitert klassischen Entwicklungsprozess um Safety und Security Anteile
- Kombiniert ISO 26262 und ISO 14508

SAFETY & SECURITY

Forschungsstand Lösungsansätze

„Automotive Functional Safety = Safety + Security“ [3]

ISO 26262

(International standard for functional safety in passenger vehicles)

- Erweitertes V-Modell
- Reduzierung der Risiken durch System- und Hardwarefehler
- Klassische Analysemethoden während Konzeptionierungsphase
 - FTA (Fault Tree Analysis)
 - FMEA (Failure Mode and Effects Analysis)

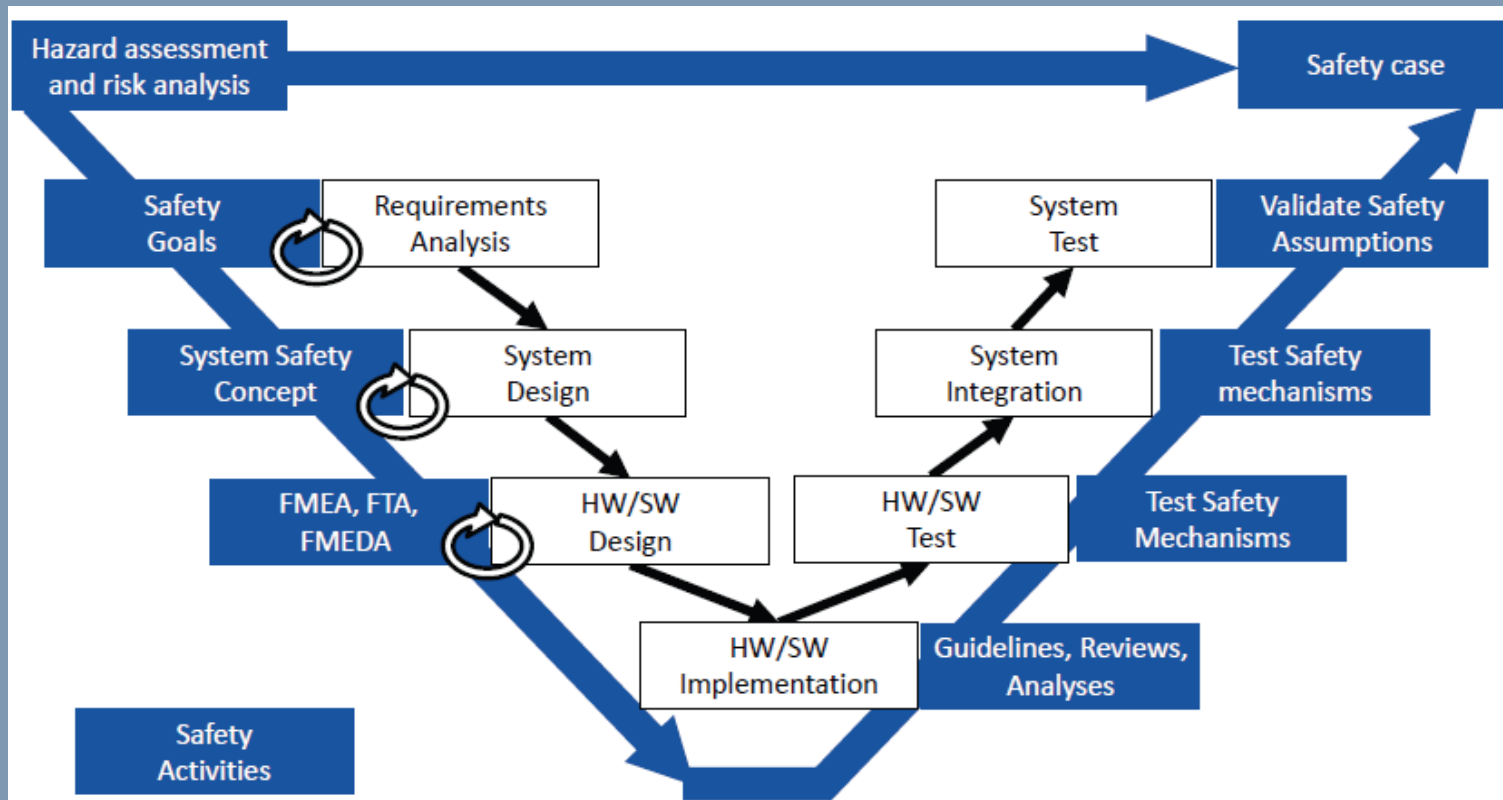
SAFETY & SECURITY

Forschungsstand Lösungsansätze

„Automotive Functional Safety = Safety + Security“ [3]

ISO 26262

(International standard for functional safety in passenger vehicles)



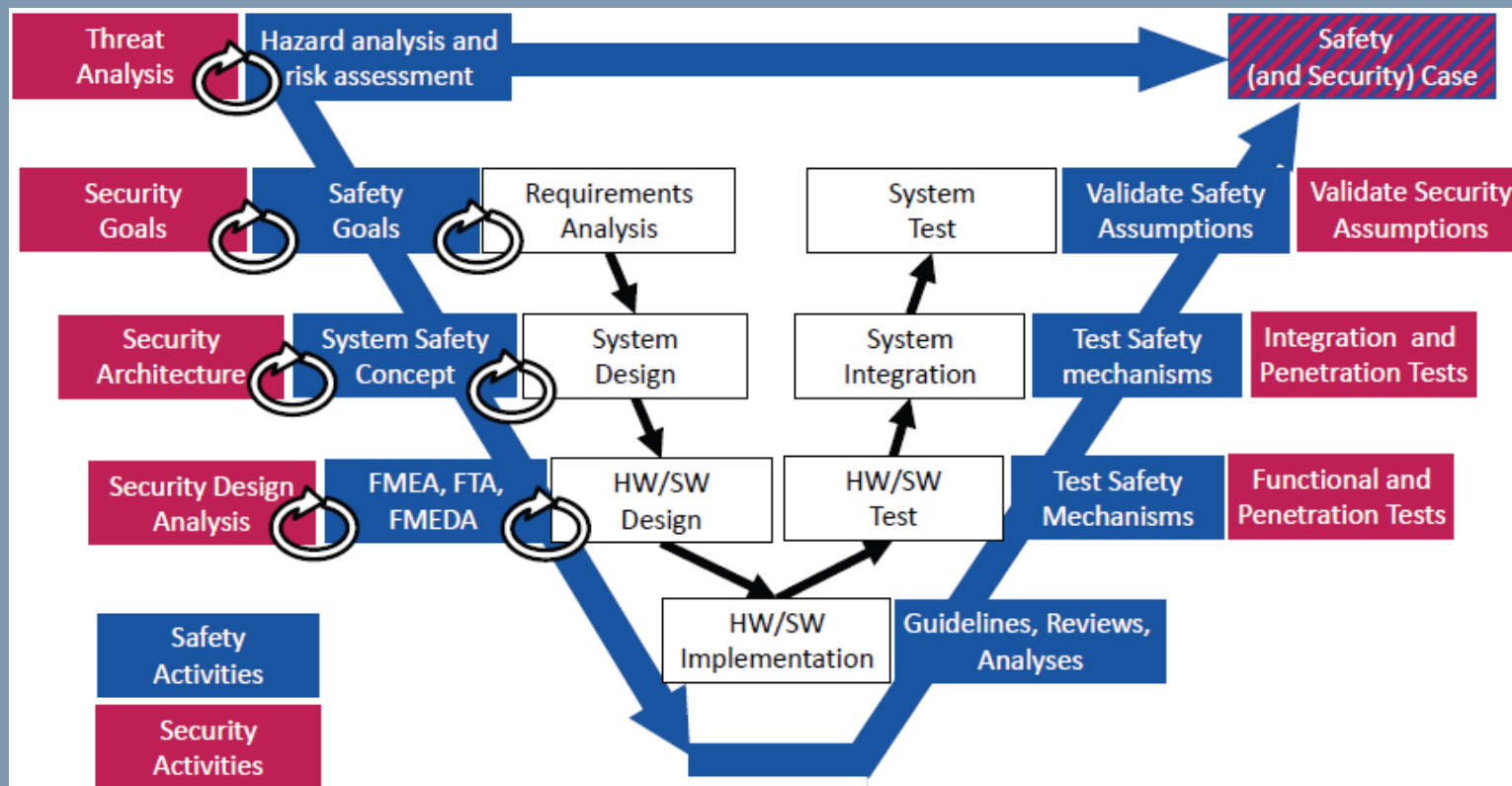
Simon Burton, Jürgen
Likkei, Marko Wolf
"Automotive Functional
Safety = Safety + Security"
[3]

SAFETY & SECURITY

Forschungsstand Lösungsansätze

„Automotive Functional Safety = Safety + Security“ [3]

ISO 26262 + ISO 14508



Simon Burton, Jürgen
Likkei, Marko Wolf
"Automotive Functional
Safety = Safety + Security"
[3]

SAFETY & SECURITY

Forschungsstand Lösungsansätze

„Automotive Functional Safety = Safety + Security“ [3]

Zusammenfassung

- Security Ziele werden auf Basis von Safety Zielen entwickelt
=> Gibt es Safety Ziele, die durch Attacken von Außen gefährdet werden?
- Aus identifizierten Zielen können Testfälle entwickelt werden

Nachteile

- Umsetzung erfordert strikte Einhaltung des vorgegeben Entwicklungsprozesses
 - Nicht praxisnah

SAFETY & SECURITY

Forschungsstand Lösungsansätze

„An Integrated Approach to Safety and Security Based on System Theory“ [2]

William Young: Ph.D. Candidate in the Engineering Systems division at Massachusetts Institute of Technology, Cambridge, MA.

Nancy G. Leveson: Professor of Aeronautics and Astronautics and also Professor of Engineering Systems at Massachusetts Institute of Technology, Cambridge, MA.

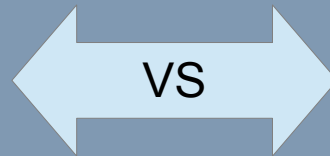
SAFETY & SECURITY

Forschungsstand Lösungsansätze

„An Integrated Approach to Safety and Security Based on System Theory“ [2]

Taktik

- WO sind Schwachstellen?
- Lücken werden geschlossen
- Priorisierung von Lücken nötig
- Kenntnisse über Angreifer notwendig
- Verteidigung aus nachteiliger Position
- Bottom-Up Konzept



Strategie

- WAS muss geschützt werden?
- Welche Verluste sind möglich?
- Welche Verluste sind (nicht) akzeptabel?
- Von Abstrakt zu Konkret
 - Hierarchische Strukturen gut für menschliche Vorstellungskraft
- Top-Down Konzept

SAFETY & SECURITY

Forschungsstand Lösungsansätze

„An Integrated Approach to Safety and Security Based on System Theory“ [2]

- **Komponenten werden in hierarchische Kontrollstruktur abgebildet**
- Startet mit hohem Abstraktionslevel
 - Stufenweise Konkretisierung
 - => Kleinere und besser kontrollierbare Menge an potenziellen Verlusten
- Unvollständigkeiten werden einfacher gefunden
 - => Dennoch kein Anspruch auf Vollständigkeit

SAFETY & SECURITY

Forschungsstand Lösungsansätze

„An Integrated Approach to Safety and Security Based on System Theory“ [2]

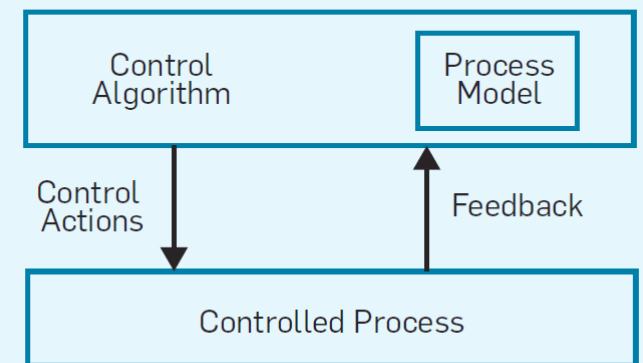
STAMP

(System-Theoretic Accident Model and Processes)

- Modell für Ursache und Wirkung zwischen Systemkomponenten
- Control Loops zwischen den Stufen der hierarchischen Kontrollstruktur

Figure 1. A basic control loop.

Controller (automated or human)



William Young and Nancy G. Leveson
"An Integrated Approach to Safety and Security
Based on Systems Theory" [2]

SAFETY & SECURITY

Forschungsstand Lösungsansätze

„An Integrated Approach to Safety and Security Based on System Theory“ [2]

STPA

(System-Theoretic Process Analysis)

- Analysetechnik basierend auf STAMP
- Durchführungsschritte:
 1. Identifizierung des möglichen Fehlverhaltens
 2. Identifizieren von ungewollten, unsicheren Control Commands
 3. Untersuchen der Control Loops zum Identifizieren von ursächlichen Szenarios
- STPA-Sec: STPA mit Security Analyse
 - Unterschied zu STPA: Hinzufügen von Security-Szenarios (3.)

Mögliche Projekte / Zielsetzung

Projekte

- Analyse eines Systems auf Basis der System Theorie [2]
 - Entwickeln entsprechender Testfälle
- Testautomatisierung möglich?

Ziele

- Tieferes theoretisches Verständnis
- Einlesen/Einarbeitung testgetriebene Entwicklung im Themengebiet [1]
- Kenntnisk Gewinn in FTA / FMEA

SAFETY & SECURITY

Konferenzen

- **SafeComp 2015: International conference on computer safety, reliability and security**
 - **Keynote:** Andrey Nikishin, Director Special Projects & Future Technologies, Kaspersky Lab, London, UK
„Does IoT stand for Internet of Threats and other stories?“
- **Cor Kalkman:** Professor of Anesthesiology at University Medical Center Utrecht, NL,
„Medical devices, Electronic Health Records and assuring Patient Safety: future Challenges?“

Konferenzen

- **ASQF Quality Days 2015: Qualitätssicherung von vernetzten Systemen**
 - **Keynote:** Prof. Dr. Ina Schieferdecker, Leiterin des Fraunhofer FOKUS Berlin & ASQF-Präsidentin
 - Dr. Jürgen Großmann, Fraunhofer Fokus

„Systematically combine security risk assessment and testing based on standards“
 - Nils Röttger, imbus AG

„Softwareintegration im Kontext von Industrie 4.0 – eine Herausforderung an die Qualitätssicherung?“

SAFETY & SECURITY

Quellen

- **[1] Andrew J. Kornecki and Janusz Zalewsky**
"Safety and Security in Industrial Control"
- **[2] William Young and Nancy G. Leveson**
"An Integrated Approach to Safety and Security Based on Systems Theory"
- **[3] Simon Burton, Jürgen Likkei, Marko Wolf**
"Automotive Functional Safety = Safety + Security"