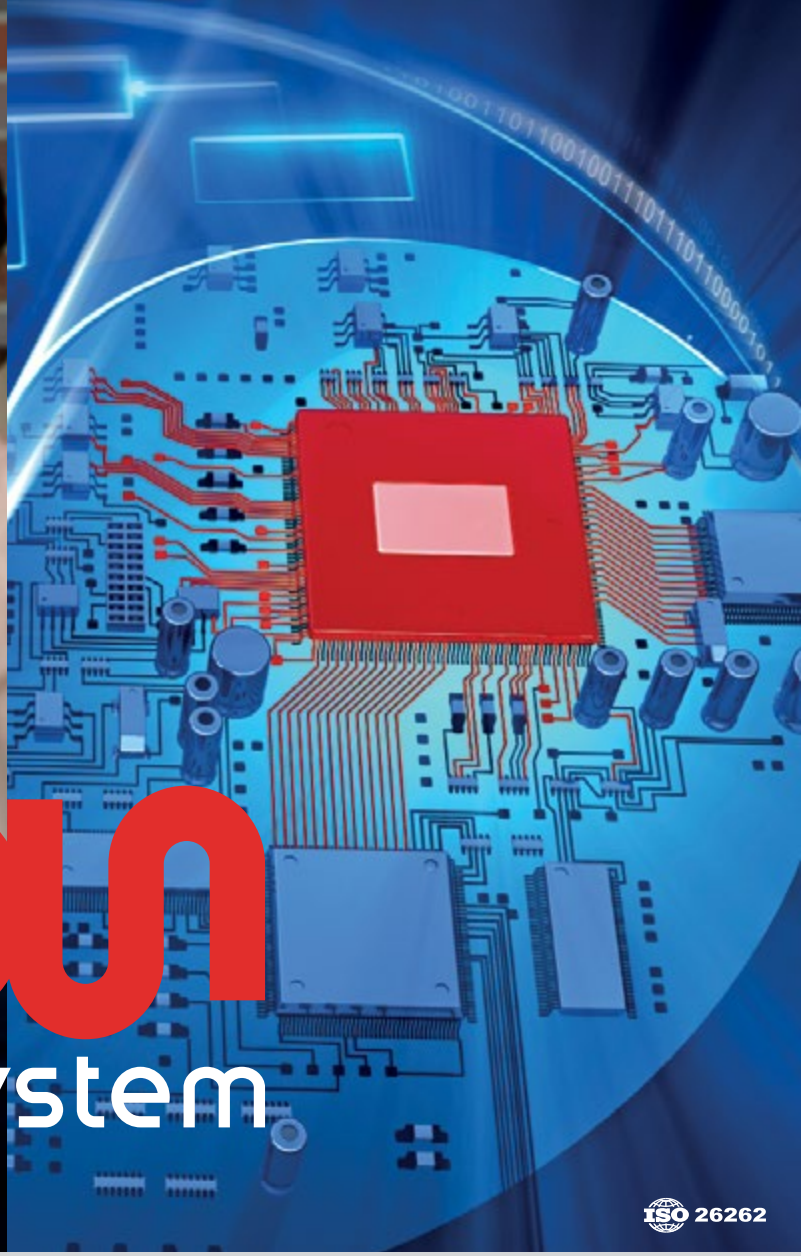


assystem

AUTOMOTIVE
COMPETENCE CENTRE
SAFETY & SYSTEMS ENGINEERING

KOMPLEXE SYSTEME. SICHER ENTWICKELN.

Sichere E/E-Systeme im Automobilbereich schützen vor Haftungs- und Rückrufrisiken und bilden die Basis für den erfolgreichen Markteintritt innovativer Technologien. Domänen wie hochautomatisiertes Fahren oder Elektrifizierung im Fahrzeug fordern dazu ein ganzheitliches Verständnis von Funktionen, Systemkomponenten und Safety-Engineering. Unser hochvernetztes Competence Centre mit Automotive Safety-Experten und Systemingenieuren bietet praxisadäquate Beratung und realisiert sämtliche Aktivitäten der funktionalen Sicherheit. Zwar ist die Bedeutung der funktionalen Sicherheit nach ISO 26262 zur technischen Realisierung der Sicherheitsanforderungen branchenweit schon lange bekannt, in der Praxis erfolgt der Umgang mit zugrundeliegenden Fachnormen jedoch nicht immer problemadäquat und effizient: Kostenintensives Over-Engineering und Sicherheitslücken infolge unsystematischer Umsetzung stellen zwei Ausprägungen der genannten Problematik dar. Darüber hinaus deckt die aktuelle ISO 26262 in Bereichen, in denen die nominelle Performanz von Sensorik und Algorithmen für die Verhütung von Unfällen relevant ist, z.B. Fahrerassistenzsysteme und automatisierte Fahrfunktionen, nicht alle Aspekte ab. Mit dem Competence Centre Safety & Systems Engineering bieten wir daher Lösungen zur Systemabsicherung, die über reine Normerfüllung hinausgehen, und setzen für unsere Kunden sicherheitsrelevante elektronische Systeme stringent, technisch adäquat, modular und kosteneffizient um.

UNSER ANSPRUCH

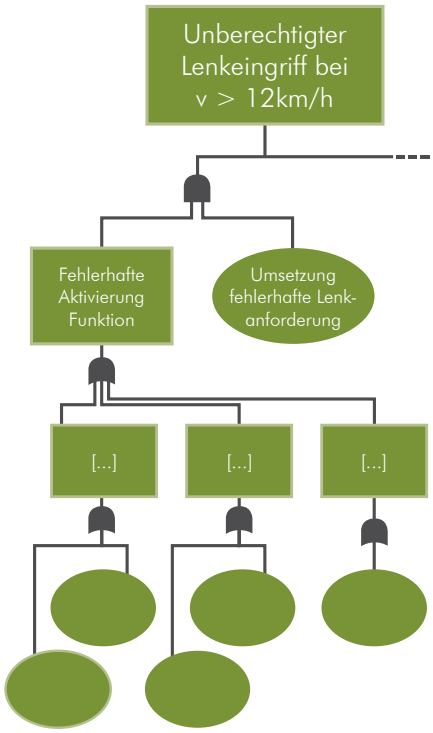
Praxisgerechte Lösungen und Sicherheit über reine Normerfüllung hinaus durch die integrierte Betrachtung von nomineller Funktion und funktionaler Sicherheit.

UNSER KONZEPT

Experten aus dem Bereich Embedded Systems mit Schwerpunkt im Safety und Systems Engineering sowie fundiertem Domänenwissen arbeiten in überregional vernetzten Teams. Bei Bedarf ziehen wir Expertise aus angrenzenden Bereichen wie Sensorik, AUTOSAR, Security oder Softwarequalität sowie unsere Experten aus weiteren Domänen hinzu. Durch Mitwirkung in Forschungsprojekten und regelmäßige Teilnahme an Fachkonferenzen integrieren wir zeitnah neueste Erkenntnisse in unsere Arbeit und sichern kontinuierlich unser hohes Qualitätsniveau.

KUNDENNUTZEN

Wir bringen unsere Kunden schneller und kostengünstiger zum sicheren, technisch adäquaten System und bauen systematisch „Verständnisschwierigkeiten" zwischen Hardware/Software, OEM/Zulieferer sowie zwischen funktionaler Sicherheit und „normaler" Produktentwicklung ab.



UNSERE LEISTUNGEN IM SAFETY-LEBENSZYKLUS

SAFETY-ENGINEERING

- Gefährdungs- und Risikoanalysen
- Qualitative und Quantitative Safety-Analysen (FTA, FMEA, FMEDA) und Metriken-Berechnung
- Erstellung funktionaler und technischer Sicherheitskonzepte für OEM und Lieferant
- Modellbasierte Spezifikation von (Sicherheits-) Architekturen, Design adäquater Safety-Maßnahmen auf System-, Hard- und Software-Ebene, problemadäquate Sicherheitsanforderungen und Traceability
- Verifikations- und Validierungskonzepte, problemadäquate und effiziente Testfallerstellung
- Unterstützung an der OEM/Lieferanten-Schnittstelle, Assessments, Freigabeempfehlungen

SAFETY-PROZESSBERATUNG

- Bewertung existierender Entwicklungsprozesse (Gap-Analyse) gem. ISO 26262, auch in Verbindung mit Automotive SPICE
- Safety-Einführungs- und Verbesserungsprojekte, Zulieferer-Kompetenzbewertung
- Unternehmensspezifisches Tailoring der Normvorgaben, integrierte Guidelines (Single-Source-Prinzip)
- Beratung in Überlappungsbereichen Safety/Security, Safety/Softwarequalität, Safety/Performance

BEREIT FÜR NEUE SAFETY-HERAUSFORDUNGEN

SICHERES HOCHAUTOMATISIERTES FAHREN

Die rasante Entwicklung moderner Fahrerassistenzsysteme hin zu teilautonomen und autonomen Fahrzeugen stellt neuartige Anforderungen an die Sicherheit. Der Einfluss der Sensor-Performanz, der Dateninterpretation sowie der komplexen Entscheidungslogik muss daher in modernen Sicherheitskonzepten deutlichen Eingang finden. Zum anderen darf das heute noch weitgehend übliche Abschalten einer Funktion künftig in vielen Fällen nicht mehr als sicherer Zustand betrachtet werden; vielmehr wird auch in einem Fehlerfall noch die zeitweise Aufrechterhaltung von Grundfunktionen im Rahmen eines Degradationskonzeptes sicherzustellen sein.

VERNETZTE FAHRZEUGFUNKTIONEN

Wo bislang ein Steuergerät eine in sich geschlossene Funktion realisierte, sind heute mehrere Funktionen darauf allokiert und fahrzeugweit vernetzt. Die Herausforderung: Statt jede Komponente für sich funktional sicher zu entwickeln, müssen auch die Gefährdungen durch fehlerhaftes Zusammenspiel antizipiert und analysiert werden. Eine effiziente und sichere Entwicklung verteilter Systeme erfordert daher eine enge Kooperation im Team mit fundierten Kenntnissen aller Fahrzeugdomänen, wie auch im „virtuosen" Umgang mit den Methoden von Requirement Engineering, Architektur-Modellierung, Verifikation und Validierung. Nur die global optimierte Lösung ist die sicherste und letztendlich preiswerteste Lösung.

INKREMENTELLE UND AGILE ENTWICKLUNG

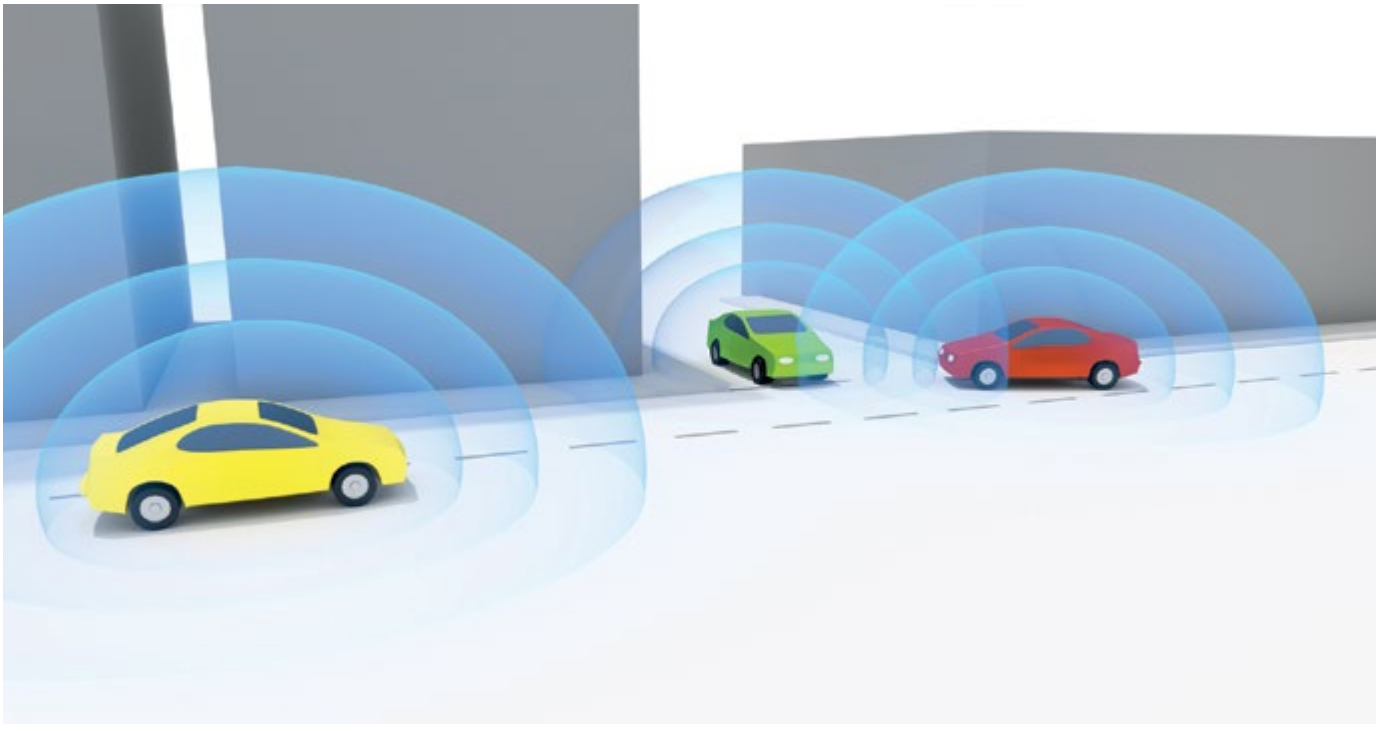
Neue Funktionen – etwa im ADAS-Bereich – werden verstärkt auf bereits bestehenden aufgebaut. Die Sicherheit jeder neuen Produktvariante muss trotz verkürzter Entwicklungszyklen und Trends wie agiler Entwicklungsmethoden oberste Priorität besitzen. Dies kann nur gelingen, wenn ein solider Systems-Engineering-Prozess etabliert ist, bei dem alle Module und Signale samt zugrundeliegenden Annahmen (z.B. erwartete Fehlerdiagnosen der Nachbarsysteme), Garantien (z.B. Signalgenauigkeit) oder der assoziierte ASIL-Level, sauber in Modellen annotiert sind. So lässt sich bei Re-Engineering, Re-Use und Variantenbildung effizient ein neuer Sicherheitsnachweis erstellen und die notwendigen Delta-Maßnahmen stringent ableiten.

SYSTEMS-ENGINEERING

- Herstellen von Produktverständnis und Dokumentation/ Modellierung, u.a. mit UML/SysML, Simulink
- Technische Analyse von Anforderungen und Abbildung auf konkrete Lösungen
- Erstellung (modellbasierter) Systemarchitektur-Dokumentationen
- Reverse Engineering und Refactoring gewachsener Produktarchitekturen
- Analyse systemischer Eigenschaften wie Sicherheit, Zuverlässigkeit, Performanz, Reaktionszeit
- Machbarkeitsstudien und technische Risikoanalysen, Lösungs- und Alternativenbewertung

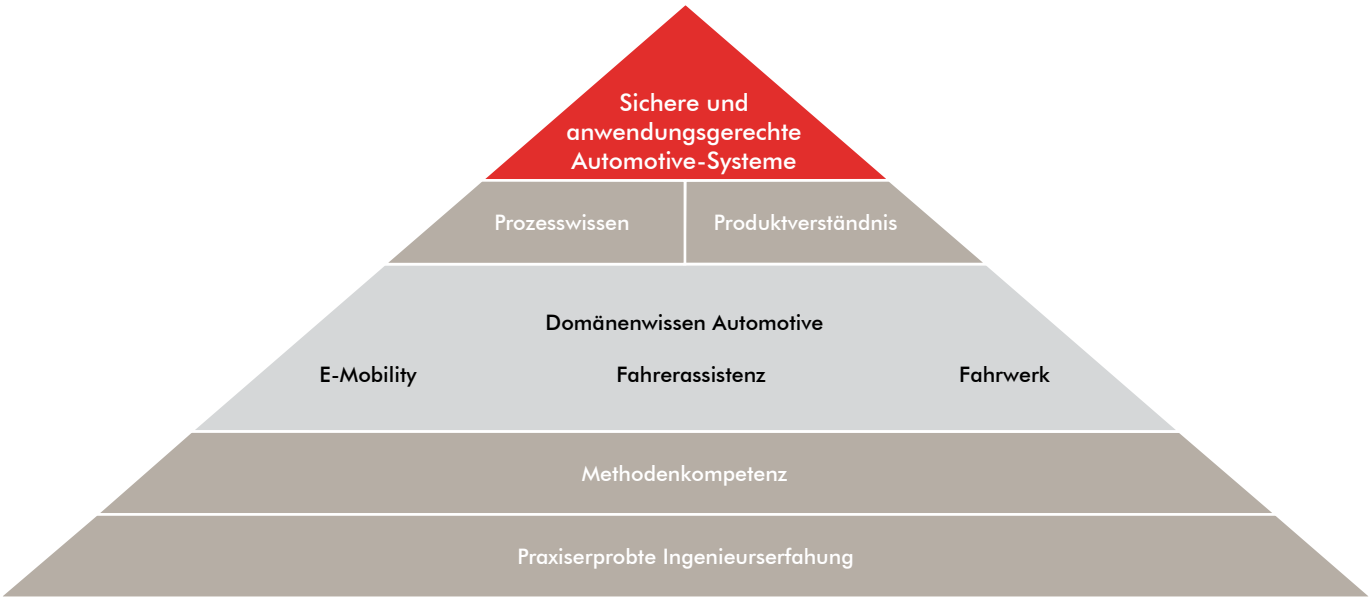
GEWERKKOMPLEXITÄT IM GRIFF

- Bei großen Gewerken, z.B. der Entwicklung kompletter Steuergeräte oder verteilter Fahrzeugfunktionen, sind professionelles Systems Engineering und umfassende Safety-Kompetenz die Schlüsselfaktoren für ein korrektes und sicheres Zusammenspiel der Systemteile untereinander und der künftigen Fahrzeugumgebung
- Das Competence Centre begleitet daher externe wie interne Entwicklerteams bei Aufgaben mit hoher Systemkomplexität und fungiert auch als Beratungsdienstleister für eine sichere Umsetzung



SAFETY & SECURITY – GANZHEITLICH SICHER?

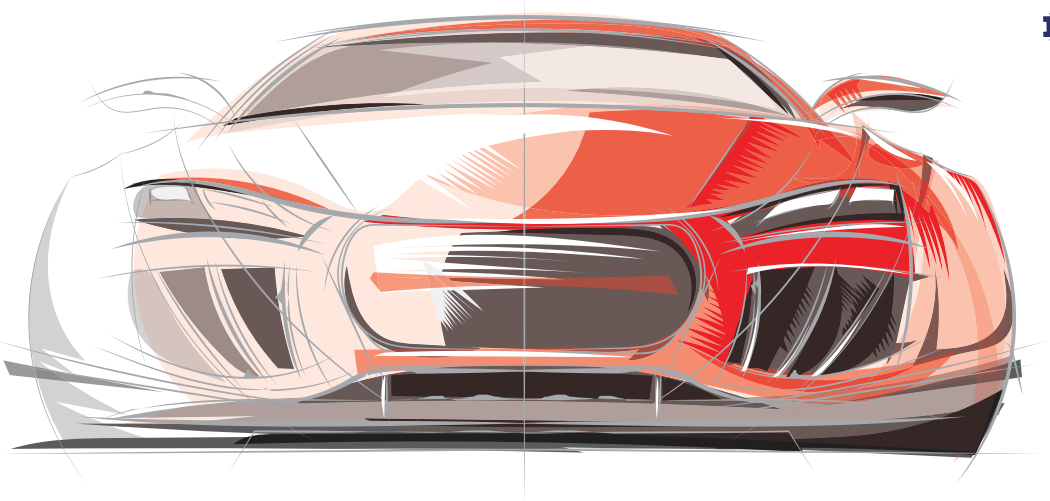
Der technologische Wandel der Fahrzeuge von einem geschlossenen System hin zu einer Fahrzeug-IT mit drahtlosen Schnittstellen, Update-Optionen und Connectivity-Lösungen kann längst auch eine Gefährdung von Personen mit sich bringen. Die Bedrohung der Datensicherheit im Fahrzeug durch unerwünschte externe Zugriffe oder Manipulaton ist Teil eines Szenarios, das auch Auswirkungen auf die Arbeit der Safety Ingenieure hat. Die Herausforderung: Die traditionell separaten Disziplinen Security und Safety müssen weiter zusammenwachsen und erfordern integrale Konzepte und Kompetenzen. Das Competence Centre Safety & Systems Engineering arbeitet dazu eng vernetzt mit dem Competence Centre für Automotive Security Engineering.



LÖSUNGEN FÜR PRAXISGERECHTE SICHERHEIT

- **Ganzheitliche Sicherheit** statt Beschränkung auf Normkonformität
- **Schneller und kostengünstiger** zum sicheren und technisch adäquaten System
- **Neueste Safety-Expertise** – auch in noch nicht normierten Feldern – durch aktive Forschung, Weiterbildung und Serienprojekte bei OEMs und Automobilzulieferern
- **Erfahrene Ingenieure** mit intensiver Safety-Ausbildung und weitreichendem Entwicklerhintergrund in sicherheitskritischen Bereichen wie Lenkung, E-Antrieb, Fahrerassistenz, Zentralelektronik
- **Überbrückung von Know-how- und Kommunikationslücken** zwischen Fachdisziplinen und Zentralabteilungen
- **Systematische Wiederverwendung** von Komponenten durch Synergien zwischen modellbasierter Entwicklung und FuSi

ISO 26262



PROJEKTBEISPIELE

- Sicherheitskonzepte für elektrische Antriebe
- Sicherheitskonzepte für Batteriesysteme
- Sicherheitskonzepte für teilautonome Fahrerassistenzsysteme
- Assessierung von Software- und Sicherheitsarchitekturen einer elektrischen Lenkunterstützung

A NEW PATH TO GROWTH

WWW.ASSYSTEM-GERMANY.COM

assystem

7/2017