

Insight



berner & mattner
optimizing your development

Automotive

Themenspecial: Funktionale Sicherheit

Berner & Mattner etabliert Competence Center für Funktionale Sicherheit

Safety & Systems Engineering:
ganzheitliche, normkonforme Entwicklung

Berner & Mattner bündelt sein Know-how für Funktionale Sicherheit in seinem Competence Center "Safety & Systems Engineering" und stellt somit ein Expertenteam zusammen, das OEMs und Zulieferer bei der effizienten Realisierung von sicherheitskritischen Produktentwicklungen unterstützt. Durch die Kombination aus Safety-Experten und Systemingenieuren mit unterschiedlichen Fachschwerpunkten deckt das Competence Center alle Entwicklungsbereiche für elektronische Systeme ab, die unter die neue Norm ISO 26262 für Funktionale Sicherheit fallen.

Grundlage des Competence Centers ist die Konsolidierung, Anwendung und Weitervermittlung der in vielen Jahren gesammelten Methoden- und Domänenenerfahrung der Safety- & Systemingenieure von Berner & Mattner. Entscheidend für die effiziente Realisierung sicherheitskritischer Produktentwicklungen ist das gebündelte Know-how auf den Gebieten der Sicherheitstechniken, gepaart mit Systemverständnis sowie der Verifikation und Validation dieser Systeme. Heute leidet die reibungslose Entwicklung eines sicheren Produkts oft darunter, dass das System nicht in allen Aspekten erfasst und beschrieben wird. Es bestehen Verständnisschwierigkeiten zwischen Produktentwicklern und Sicherheitsanalysten, aber auch zwischen OEM und Zulieferer oder den Disziplinen Hardware und Software. Das überregional aufgestellte Safety & Systems-Team hilft durch den vernetzten Teameinsatz bei der Lösung dieser Problemfelder und hat bereits mehrere Serienprojekte bei namhaften Automobilherstellern und Zulieferern erfolgreich abgeschlossen.



"Funktionale Sicherheit wird von vielen lediglich als eine Sammlung zusätzlicher Prozessaktivitäten verstanden", sagt Dr.-Ing. Bernhard Kaiser, Leiter des Competence Centers. "Dieser Ansatz wird dem Thema jedoch

nicht gerecht, denn bei der Komplexität heutiger Systeme – etwa im Bereich Fahrerassistenz oder E-Mobilität – können machbare und wirtschaftliche Lösungen zur Erfüllung der Sicherheitsvorgaben nur im Team mit erfahrenen Fachingenieuren gefunden werden. Die Ingenieure müssen dafür sowohl die Funktionsweise des Systems verstehen als auch einen querschnittlichen Blick auf das Zusammenwirken aller Komponenten haben – Funktionale Sicherheit ist eine Ingenieursdisziplin."

Safety & Systems Engineering

Aufbau Competence Center
"Safety & Systems Engineering"



Produktverständnis



Technologieexpertise



Safety-Prozessverständnis



Veranstaltungen:

ESE-Kongress 2011

5.-9.12.2011 - Sindelfingen
Besuchen Sie uns!

embedded world 2012

28.2.-1.3.2012 - Nürnberg
Sie finden uns in Halle 5 am Stand 326.

Automotive Testing Expo Europe 2012

12.-14.6.2012 - Stuttgart
Berner & Mattner begrüßt Sie am Stand 1537.

Fortschritte in der Automobil-Elektronik 2012

19.-20.6.2012 - Ludwigsburg
Besuchen Sie uns!

➔ www.berner-mattner.com/de/veranstaltungen

Vortragsthemen:

"Sicherheitserhöhende Assistenzsysteme – bietet die ISO 26262 die richtigen Werkzeuge?"

"AUTOSAR 26262 – wie werden AUTOSAR-Systeme sicher?"

"Qualifizierung der Konfiguration eines Integrations-HiL zum Nachweis einer Fahrerassistenzfunktion im Kontext der ISO 26262"

➔ www.berner-mattner.com/de/vortraege

Aktuelle Stellenangebote:

Experte (m/w) für Funktionale Sicherheit

Trainee Automotive (m/w)

➔ www.berner-mattner.com/de/stellenangebote

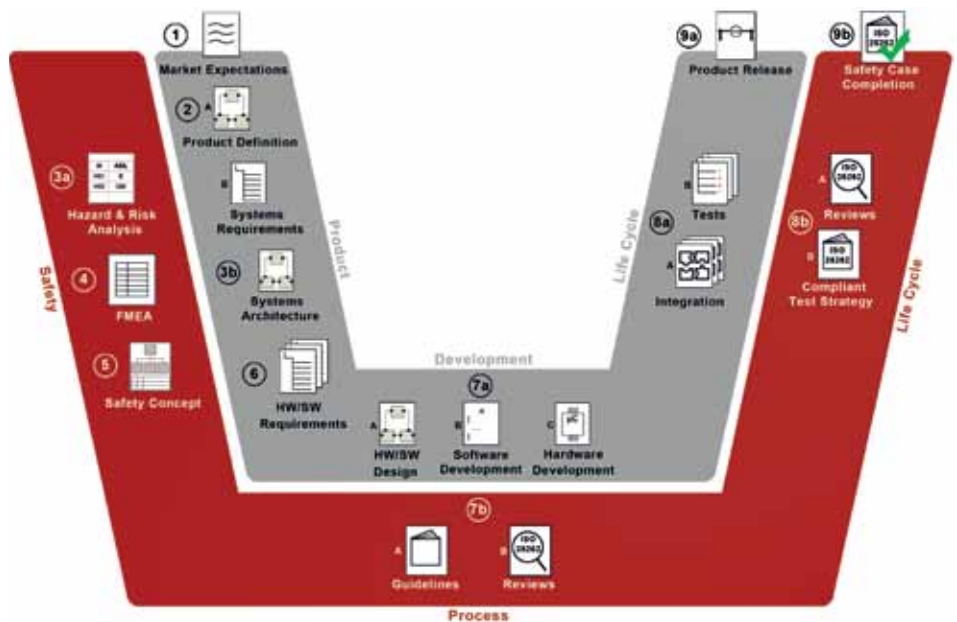
ISO 26262

Integration von Funktionaler Sicherheit im Entwicklungsprozess

Die neue Sicherheitsnorm ISO 26262 zwingt die Hersteller elektronischer Fahrzeugsysteme, sämtliche Entwicklungsprozesse auf das Thema Sicherheit auszurichten. Allerdings sind die "Safety-Aktivitäten" oft von den "normalen" Tätigkeiten der Entwickler komplett isoliert. Die Sicherheitsvorgaben fließen deswegen erst spät in den Entwicklungsprozess ein. Kostspielige und zeitintensive Änderungsschleifen werden notwendig. Berner & Mattner stellt eine neue Methodik vor, die Sicherheitsaktivitäten werkzeuggestützt mit der klassischen Systementwicklung verzahnt und Sicherheitsanforderungen frühzeitig ins Systemdesign einbezieht.

Die Methode vereint hierarchisches Modellieren von Systemarchitektur und Fehlernetzen, die Zuordnung der Sicherheitsmechanismen und eine systematische Anforderungsverfolgung samt Nachweis der Testabdeckung. Diese Methodologie besteht aus der geschickten toolintegrierten Kombination grundsätzlich bekannter und bewährter Ansätze. Zusätzlich sind die entstehenden Modelle und Konzeptbausteine modular und wiederverwendbar. In verschiedenen Kundenprojekten konnten mit dieser Methode deutliche Effizienzsteigerungen erzielt werden.

➔ Lesen Sie hierzu den in der ATZ Elektronik 5 veröffentlichten Fachartikel "Integration von Funktionaler Sicherheit im Entwicklungsprozess" auf www.berner-mattner.com/de/fachartikel



Überblick: Integration von Funktionaler Sicherheit im Entwicklungsprozess

1. Produktsteckbrief auf Basis von Markterwartung
2. Produktdefinition und Systems Requirements durch Safety- und Systemingenieure
3. Parallele und ineinandergreifende Arbeit an Funktionaler Sicherheit und Produktentwicklung
4. Erstellung der hierarchischen FMEA (Failure Mode and Effects Analysen)
5. Erarbeitung des Safety-Konzepts
6. Einspeisung des Safety-Konzepts in das bestehende Requirements-Management
7. Umsetzung und Durchführung von HW-/SW-Design (7aA), SW- und HW-Entwicklung (7aB, 7aC) nach Vorgaben der ISO 26262
8. Stufenweise Integration (8aA) und Test (8aB) nach Vorgaben der ISO 26262 Teststrategie (8bA) sowie Reviews der Testfälle und -ergebnisse unter Safety-Gesichtspunkten (8bB)
9. Komplettierung des Safety Cases (9b) und Fahrzeugfreigabe (9a)

Vorteile unseres Leistungsportfolios

- Verringerung des Fehler-, Rückruf- und Produkthaftungsrisikos
- Abdeckung aller Aktivitäten des Safety-Lebenszyklus gem. ISO 26262
- Schließung der Know-how-Lücke zwischen den Fachdisziplinen bei der Entwicklung softwaregesteuerter Elektroniksysteme
- Schneller zum sicheren und spezifikationsgemäß funktionierenden System: Senkung der Entwicklungskosten und -zeiten, Vermeidung von Produktrisiken
- Alle Neuerungen und Änderungen der Normanforderungen sowie der neueste Stand der Interpretation der Norm in der Praxis werden durch kontinuierliche Weiterbildung unserer Mitarbeiterinnen und Mitarbeiter direkt in die betroffenen Entwicklungsprojekte übertragen.

Projektbeispiel:

"Grünes Projekt"

Start-/Stopp-Systeme auf dem Vormarsch

Start-/Stopp-Systeme mit zusätzlichen Energiespeichern zur Stützung des Bordnetzes halten bereits in vielen Fahrzeugen Einzug. Deren Entwicklung und Realisierung nach den Anforderungen der ISO 26262 befindet sich jedoch erst in der Anfangsphase. In einem Pilotprojekt für einen großen Zulieferer hat Berner & Mattner das Requirements Engineering, die Erstellung der Systemarchitektur, alle Aktivitäten zur Funktionalen Sicherheit sowie die Fehleranalysen und das Testmanagement übernommen. In diesem umfassenden Projekt haben sich die Experten des Competence Centers perfekt ergänzt und das Projekt nach den Anforderungen der ISO 26262 und unter engen Kosten- und Zeitaspekten effizient realisiert.

Projektbeispiel:

Herausforderung CO₂-Reduktion

Steuergeräteentwicklung für Energiespeicherung

Lösungen für die Energieversorgung des E-Motors liegen nicht allein in der Batterietechnologie. Die Daimler AG hat durch die Weltumfahrung mit ihrer wasserstoffbetriebenen Forschungsflotte im Sommer 2011 gezeigt, dass sich auch andere umweltfreundliche Technologien zum Antrieb von Fahrzeugen eignen. Für einen namhaften OEM übernimmt Berner & Mattner die Entwicklung und Sicherheitsanalyse eines sicherheitskritischen Steuergeräts zur Speicherung von Energie. Dabei sind sowohl das Know-how der Steuergeräteentwicklung gefordert als auch das Expertenwissen für die Funktionale Sicherheit. Dokumentation, Gefährdungsanalyse, FMEA (Failure Mode and Effects Analysen) und

pragmatische Vorschläge für die Umsetzung der Sicherheitsanforderungen sind zentrale Elemente dieses Projekts.

Projektbeispiel:

Sichere E-Mobilität

Herausforderung Elektrifizierung Antriebsstrang angenommen

Elektronische Antriebe stellen die Entwicklung nicht nur im Hinblick auf neu zu entwickelnde Antriebskonzepte vor große Herausforderungen. Auch für die Gewährleistung der Funktionalen Sicherheit stark elektrifizierter Systeme müssen neue Wege beschritten werden. Berner & Mattner hat bereits in mehreren Projekten die Aktivitäten im Rahmen der Funktionalen Sicherheit übernommen – unter anderem in einem Projekt für einen weltweit tätigen Zulieferer. Zentrale Bausteine: Die Erstellung von Gefährdungsanalysen und Sicherheitskonzepten sowie die Erarbeitung und Durchführung der Testkonzepte von Stromrichtern für Synchronmaschinen für Elektro- und Hybridfahrzeuge europäischer OEMs. Ergebnis: Erfolgreiche, entwicklungsgerechte Einbindung umfangreicher Safety-Aktivitäten in den bereits bestehenden Entwicklungsprozess beim Kunden.

Projektbeispiel:

Entwicklungen in der höchsten Gefährdungsstufe

Lenksystem im ASIL-Level D

Die elektronische Lenkung fällt nach der ISO 26262 unter das ASIL-Level D und damit in die höchste Gefährdungsstufe. Entsprechend umfangreich sind die Sicherheitsmaßnahmen bei der Entwicklung, Absicherung und Dokumentation. Berner & Mattner hat für dieses hoch sicherheitskritische System das technische

Sicherheitskonzept für einen Zulieferer ausgearbeitet und diesen bei der Prozessorauswahl beraten. Zum Einsatz kommt ein hochmoderner Doppelkernprozessor mit speziellen hardwareseitigen Fehlerdetektionsmechanismen. Weitere Aufgaben im Rahmen des Projekts: Erstellung der Software-Architektur, Definition von Hardware-Diagnosen, Durchführung der FMEA sowie Erstellung der Fehlerbaum- und Common Cause Fehleranalysen. In diesem Projekt wurden alle Fachschwerpunkte des Competence Centers gefordert: Definition und Ausführung der Safety-Aktivitäten im Produktlebenszyklus, Embedded Systems Engineering, Methoden-anwendung und Schnittstellenkommunikation zwischen Unternehmensstandorten sowie zum OEM und Prozessorhersteller. Der Kunde profitiert von einer ganzheitlichen Unterstützung und einer nahtlosen Einbindung in seine Entwicklungsaktivitäten ohne Abstimmungsschwierigkeiten.

Projektbeispiel:

Safety-Prozesse

Auch für LKWs ein Thema!

Beratung zu Safety-Prozessen ist ein wichtiger Leistungsbereich des Competence Centers. Für einen LKW-Hersteller führte Berner & Mattner u. a. die Safety-Prozesseinführung inkl. Gap-Analyse und das Training mit Fokus auf konventioneller wie modellbasierter Codeerzeugung durch. Zusätzlich wurde ein pragmatischer Ansatz für das Vorgehen im schon laufenden Projekt vorgeschlagen, da der OEM – in Vorbereitung auf die künftige Gültigkeit der Norm – auch für LKWs frühzeitig die richtigen Weichen stellen wollte. In diesem Zusammenhang erfolgte auch eine Bewertung hinsichtlich Absicherungstechniken für Prozesse und der Anwendbarkeit von Standard-Safety-Architekturen (z. B. E-Gas). Zudem wurden Empfehlungen zur Qualifizierung von Entwicklungstools und zur Verbesserung des Testprozesses ausgesprochen.



Workshop

Reden wir alle vom Gleichen und verstehen wir dasselbe?

Regelmäßiger Bestandteil unserer Kundenprojekte sind Workshops zur Prozessdefinition und Modellierung, zum Methodentraining und Produktverständnis und zur Überbrückung von Verständnisschwierigkeiten zwischen Fachabteilungen – gehalten von erfahrenen Senior-Beratern mit langjähriger Branchenerfahrung. Selbstverständlich können diese Workshops auch einzeln gebucht werden.



Ausblick

Welche Herausforderungen kommen mit der ISO 26262 auf die Branche zu?

Die Einhaltung der Norm ISO 26262 ist seit ihrer Veröffentlichung im November 2011 Standard für die Entwicklung sicherheitskritischer Systeme. Die Berücksichtigung der Funktionalen Sicherheit wird u. a. bei der Entwicklung von Brems- und Lenksystemen und alternativen Antriebskonzepten gefordert, da von diesen Systemen ein hohes Gefährdungspotential ausgeht. Aber auch alle anderen elektronischen Kraftfahrzeugsysteme sind betroffen bis hin zu Systemen zur Steuerung von Licht und Scheibenwischern. Trends wie steigende Komplexität und Vernetzung, Funktionalitätsverlagerung auf Software, funktionsorientierte Entwicklung neuartiger Sicherheits-Assistenzfunktionen, Variantenvielfalt und AUTOSAR fallen mit der Einführung der ISO 26262 zeitlich zusammen und stellen im Verbund noch weitergehende Anforderungen an den Entwicklungsprozess. Was wird also wichtig werden, um Fahrzeugsysteme nach Anforderungen der Norm praxisgerecht zu entwickeln?

AUTOSAR und ISO 26262 – Sicherheit für Gesamtsysteme

Der AUTOSAR-Standard bewirkt die Verlagerung von Funktionalitäten auf Software mit dem Ziel, mehr Funktionen in einem Steuergerät zu platzieren. Diese sollen zudem frei auf Steuergeräte allozierbar sein. Die Zusammenführung birgt jedoch das Sicherheitsrisiko einer gegenseitigen Beeinflussung. Um dieses Risiko im Sinne der Norm abzusichern, müssen alle Funktionen bereits bei der Anforderungsspezifikation auf ihr Gefährdungspotential hin untersucht und deren Beeinflussungspotential auf andere Funktionen geprüft werden. Darüber hinaus müssen die Funktionen, deren Entwicklung über Standort- und Firmengrenzen hinweg erfolgt, den Anforderungen der Norm im Entwicklungs- und Absicherungsprozess gerecht werden. Die Sicherheit des Gesamtsystems lässt sich nur aus der Kombination dieser Aspekte begründen.

Das Competence Center hilft hier schon in der frühen Phase mit einer an firmenübergreifenden Erfahrungen orientierten Einschätzung des Gefährdungspotentials einzelner Funktionen. Darüber hinaus fungiert es bei der Entwicklung sicherheitskritischer Funktionen als Bindeglied

zwischen OEM und den beteiligten Zulieferern. Bei der Definition von Sicherheitskonzepten wird auf die AUTOSAR-eigenen Mechanismen (ab Version 4.0) Bezug genommen – beispielhafte Zuordnungen zu Fehlermodi und Diagnoseabdeckungsgraden liegen uns bereits vor! Mit namhaften Herstellern wird derzeit am Ansatz des "Kompositionalen Safety Case" gearbeitet, der den Nachweis im Falle der Portierung von Funktionen drastisch reduziert.

Autonomes Fahren – weitere Technologien von der ISO 26262 betroffen

Fahrzeuge, die ohne Eingreifen des Fahrers im Stop-and-Go-Verkehr Tempo und Spurführung bestimmen, automatisch einparken oder vor unvermeidlichen Kollisionen selbständig bremsen sind eine Vision, an der alle Automobilhersteller bereits intensiv arbeiten. Bis zur Zulassungsfähigkeit solcher Systeme müssen entwicklungsseitig jedoch noch einige Hürden genommen werden. So auch die Frage: Wie kann die Funktionssicherheit autonomer Fahrereingriffe gewährleistet werden? Dies ist ein komplexes Thema, das über den Geltungsbereich der ISO 26262 weit hinausreicht, bis hinein in Disziplinen wie Sensorik, Ergonomie, Haftungs-

und Zulassungsrecht. Neben den fahrzeugeigenen Sensoriken beziehen solche Funktionen zunehmend auch Daten in ihre Strategie ein, die von anderen Fahrzeugen oder der stationären Infrastruktur übertragen werden, etwa zur Geländebeschaffenheit, der Straßenauslastung oder zu Gefahrenwarnungen. Diese Form des Datenaustausches wird unter dem Begriff "Car-to-X-Communication" geführt.

Die Erweiterung der Schnittstellen, die auf das Fahrverhalten Einfluss nehmen, erfordert die Berücksichtigung weiterer Technologien im sicherheitskonformen Entwicklungsprozess – Sensorfusionsalgorithmen, Datenübertragung und Datensicherheit sind nur einige davon. Automobilhersteller und Zulieferer profitieren von der umfangreichen Erfahrung von Berner & Mattner, die in vielen erfolgreich abgeschlossenen Projekten wie z. B. in der Entwicklung und Absicherung von diversen Fahrerassistenzfunktionen (z. B. kamera- oder radarbasiert), im Infotainment-Bereich sowie bei Standardisierungsleistungen (z. B. im Umfeld von TPEG) gewonnen wurde.

Sicherheit für Fahrzeugindividualisierung?

Fahrzeuge müssen sich flexibel auf die Ansprüche und Bedürfnisse der Konsumenten anpassen lassen, um konkurrenzfähig zu bleiben. Variantenvielfalt, die sich kostengünstig nur über Softwarevarianten und Parametrierung darstellen lässt, ist eine Konsequenz der unterschiedlichen Konsumentennachfrage. Eine weitere Entwicklung ist die Integration zukünftiger Fahrerassistenzsysteme in das Fahrzeug mittels Apps. Hier spielen Security (Schutz vor unbefugter Manipulation) und Safety (Schutz vor Unfällen) eng zusammen. Durch die Integration externer Technologien müssen auch diese in die Aktivitäten der Funktionalen Sicherheit eingebunden werden. Die Entwicklung schreitet rasant voran – Berner & Mattner sichert Sie ab.



berner & mattner
optimizing your development

Ansprechpartner

Gudrun Wehrle

Tel. +49 (0) 89 608090-255
gudrun.wehrle@berner-mattner.com

Ute Herold

Tel. +49 (0) 89 608090-270
ute.herold@berner-mattner.com

Impressum

Herausgeber:

Berner & Mattner Systemtechnik GmbH
Erwin-von-Kreibitz-Str. 3
80807 München
Tel. +49 (0) 89 608090-0
Fax +49 (0) 89 6098182
www.berner-mattner.com
marketing@berner-mattner.com

Redaktion und Gestaltung:

Martina Heinze, Gudrun Wehrle
© Berner & Mattner / Dezember 2011