Funktionale Sicherheit und IT-Sicherheit. Gemeinsamkeiten, Unterschiede und integrierte Lösungen.

Datenbank
TEMA, Copyright WTI-Frankfurt eG

Deskriptoren
Anlagensicherheit; Anwendungsbeispiele; bösartige Bedrohung; Bussystem; Diagnosesystem; Elektroauto; Fahrzeugsicherheit; Fehlerbaumanalyse; Fehlfunktion; Funktionssicherheit; Gefährdungsanalyse; IEC-Norm; ISO-Norm; IT-Sicherheit; Kraftfahrzeug; Ladestation; Navigationssystem; SAE-Norm; Sicherheitsanalyse; Sicherheitskonzept; Systemvergleich; Überlastung; Vernetzung (Kommunikation)

Abstract
Moderne Fahrzeuge sind zweifach vernetzt, einmal durch interne Bussysteme, die über Gateways Informationen austauschen und zum anderen über externe Schnittstellen zu Diagnosesystemen und Navigationssysteme. Im ersten Fall können elektrische und elektronische Fehlfunktionen Gefährdungen auslösen: funktionale Sicherheit (Safety), im zweiten Fall können bösartige Angriffe zu Schäden führen: IT-Sicherheit (Security). Für die Gefahren- und Sicherheitsanalyse (Hazard and Risk Analysis; HARA) im ersten Fall und die Bedrohungs- und Risikoanalyse (Threat Agent Risk Assessment; TARA) im zweiten Fall werden Gemeinsamkeiten und Unterschiede im grundsätzlichen Vorgehen beschrieben. Die Fehlerbaumanalyse (Fault Tree Analysis; ATA) wird der Bedrohungsanalyse (Attack Tree Analysis; ATA) zur Absicherung von Sicherheitskonzepten gegenübergestellt. Damit werden mögliche Bedrohungsszenarien am Beispiel des Ladens eines Elektrofahrzeugs (E-Fahrzeug) an einer intelligenten Ladestation analysiert und bewertet. Die ISO 26262 ist als spezifische Norm für die funktionale Sicherheit im Fahrzeug etabliert. Sie bestimmt den Automotive Safety Integrity Level (ASIL). Bezüglich der IT-Sicherheit ist die Norm SAE J3061 im Jahr 2015 noch nicht weit genug entwickelt; bis dahin gilt noch die Beschränkung auf die Normen IEC 62443, die NIST 800er-Reihe und die Veröffentlichungen zum EVITA-Forschungsprojekt. Wichtige Unterschiede bestehen beispielsweise in der unabsichtlichen oder absichtlichen Gefährdung von Menschen und Umwelt, in der Einschätzung von Gefahren (vorhersehbar oder schwer vorhersehbar) oder in der Risikoanalyse (Fehlerbaum oder Angriffsbaum). Gemeinsamkeiten ermöglichen eine parallele Bearbeitung während der Design- und Konzeptphase. Bei dem Anwendungsbeispiel können aus Sicht der funktionalen Sicherheit Überlastungen oder Fehlbedienungen problematische Situationen ergeben. Die IT-Sicherheit wäre verletzt wenn ein Angreifer über den Ladeadapter Schadsoftware oder falsche Busnachrichten einspielen würde. Gegenmaßnahmen werden aus der HARA und der TARA angeleitet.

Autor
Hoch, Stefan; Kiank, Stephan; Hipp, Udo; Kiefner, Dominique

Institution
ICS, Stuttgart, DE

Konferenzangaben
VDI/VW-Gemeinschaftstagung, 31., Wolfsburg, DE, 2015-10-21 - 2015-10-22
publiziert als: 31. VDI/VW-Gemeinschaftstagung, Automotive Security, Wolfsburg, DE, 21. - 22. Okt, 2015

Quelle
Automotive Security, VDI/VW-Gemeinschaftstagung, 31, in: VDI-Berichte * Band 2263 (2015) Seite 69-80 (12 Seiten, Bilder, Tabellen, 9 Quellen)
Düsseldorf: VDI-Verlag

Sprache
DE Deutsch

Dokumentart
CA Beitrag (Konferenz)
BC Kapitel (Buch)

Erscheinungsjahr
2016