Stefan Kubica, Hagen Ringshausen,
Jörg Reiff-Stephan, Marius Schlingelhoff (Hrsg.)
1. Automobil Symposium Wildau: Tagungsband
Technische Hochschule Wildau 2016

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

Safety & Security – Sicherheit und Sicherheit im Zeitalter kommunizierender Fahrzeuge

Ronald Melster, Tilo Schneider

doi: 10.15771/ASW_2016_3

Zusammenfassung

Globale Megatrends wie die Digitalisierung, Internet of Things (IoT) oder Software Defined Everything beeinflussen die Zukunft des Automobils in nie dagewesener Weise und Geschwindigkeit (Dannenberg & Burgard 2015). OEM entwickeln unter diesem Druck, moderne Car2X-Services, um die Attraktivität ihrer Modelle zu steigern. Offene Standards werden es auch bisher branchenfremden Playern ermöglichen, Applikationen zu entwickeln, die sich außerhalb der »Hoheit« der OEM befinden (Borchert & Slusser 2014). Der Austausch von Informationen von Fahrzeugen mit jedem nur denkbaren externen Kommunikationspartner bricht mit dem Paradigma, dass das Fahrzeug ein in sich geschlossenes System sei (Harding et al. 2014). Der Einsatz von Diensten der klassischen Informationstechnologie im Fahrzeug führt zu Sicherheitsrisiken, die in der Branche bisher bestenfalls aus Büro- oder Produktionsumgebungen bekannt waren. Die Auswirkungen für die Sicherheit des Gesamtfahrzeuges sind gravierend.
Das Management der Sicherheit elektrischer, elektronischer oder programmierbarer Fahrzeugsysteme ist daher nicht mehr nur auf die Funktionale Sicherheit (Safety) beschränkt, sondern muss den Aspekten der Vertraulichkeit, Integrität und Verfügbarkeit (Security) Rechnung tragen.
Die Herausforderung besteht in der Beantwortung der Fragen, ob die bestehenden Ansätze aus der Informationstechnologie den Anforderungen der Branche gerecht werden und die beteiligten Experten beider Fachrichtungen zueinander finden und die jeweils andere Seite verstehen. Innerhalb der ISO wird zurzeit ein Projektvorschlag zur ISO 26262 in Verbindung mit dem Management der Informationssicherheit diskutiert.

Keywords: Functionals Safety, Information Security

1. Safety – Funktionale Sicherheit elektrischer, elektronischer und programmierbarer Systeme

Im Jahre 2015 starben in Deutschland ca. 3450 Menschen im Straßenverkehr. Ein Großteil der Unfälle wird derzeit noch durch menschliches Versagen verursacht, so dass die Hersteller sich vorgenommen haben, diese Zahl durch technische Systeme drastisch zu senken. Dies soll durch den Einsatz von passiven und aktiven Sicherheitssystemen erreicht werden. So hat sich der Hersteller Volvo vorgenommen, dass im Jahre 2020 niemand mehr durch einen Volvo verletzt oder getötet werden soll (Süddeutsche Zeitung 2010).
Doch durch den Einsatz von elektronischen Systemen werden nicht nur Gefahren reduziert, sondern es werden auch neue Gefahren in die Systeme eingebracht. Fahrerassistenzsysteme haben die Möglichkeit, direkt in das Fahrverhalten einzugreifen und somit Beschleunigungen, Bremsungen und Lenkeingriffe zu bewirken, die nicht mehr vom Fahrer initiiert und kontrolliert werden. Dies bedeutet, dass ein fehlerhaftes Verhalten eines Fahrerassistenzsystems zu einer gefährlichen Situation für die Fahrzeuginsassen und andere Verkehrsteilnehmer führen kann. So führt beispielsweise eine ungerechtfertigte Bremsung ohne einen äußeren Auslöseimpuls (erkanntes Hindernis) zu einer gefährlichen Situation für den nachfolgenden Verkehr, die als Folge ein Auffahren haben kann. Mit zukünftigen Funktionen wie z. B. Car2X kommt dieser Auslöseimpuls zunehmend von außen, ohne dass das Ego-Fahrzeug die Möglichkeit hat, den Impuls durch redundante Sensorik zu überprüfen. Für diese Auslöseinformationen ist es dringend erforderlich, die Quelle zu überprüfen und den Übertragungsweg abzusichern, so dass Manipulationen ausgeschlossen werden können.

1.1 Trends in der Automobilindustrie

Derzeit beobachten wir verschiedene Trends, die gleichzeitig zum Wirken kommen und die Erreichung der Ziele zum einen begünstigen, aber auch erschweren:
Die Komplexität der Fahrzeugsysteme steigt seit Jahren stark an. Anfang der 90er wurden erste Steuergeräte verbaut, ein Großteil der Funktionalität im Fahrzeug wurden rein mechanisch realisiert.
In heutigen Fahrzeugen sind eine steigende Anzahl von Bussegmenten und Übertragungssystemen verbaut, über die Tausende unterschiedliche Botschaften geschickt werden können. Die ermittelten Sensordaten werden zunehmend von Funktionalitäten geteilt, um Kosten für doppelte Sensorik mit dem gleichen Zweck zu sparen. Ein weiterer Grund für die steigende Komplexität ist der o.g. Einbau von Fahrerassistenzsystemen als Komfortsysteme.

Ein weiterer Trend ist das autonome oder pilotierte Fahren, bei dem die Fahraufgabe zu einem immer größeren Teil an automatisierte Systeme übergeben werden. Die Konsequenzen:

- Die Fahrer sind nicht aufmerksam bzw. erwarten, dass das Assistenzsystem eingreift (Spiegel Online 2016).
- Fahrer sind nicht mehr in der Lage, das Fahrzeug zu beherrschen, wenn Systeme in Grenzsituationen ausfallen (wenn das ESP in der Regelung versagt, können nur trainierte Fahrer das Fahrzeug in einen kontrollierten Zustand übeführen).
- Wir sehen eine Entwicklung, die in anderen Branchen bereits durchlebt wurde. Die Piloten von hochautomatisierten Flugzeugen fliegen nur noch einen Bruchteil der Zeit das Flugzeug selbst. Dennoch sind sie verantwortlich, wenn die Systeme in einen instabilen Zustand gelangen. Diese Gefahr ist seit langem bekannt und ihr wird durch intensives und regelmäßiges Training von Systemausfällen begegnet. Dieses Vorgehen ist in der Automobilbranche nicht anwendbar, wodurch sich sehr hohe Anforderungen an die Zuverlässigkeit von automatisierten Fahrsystemen ergeben (Spiegel Online 2009).

1.2 Aufgabe der Safety-Norm ISO 26262

Mit der ISO 26262 soll diesen Gefährdungen durch technische und nicht-technische Maßnahmen begegnet werden, um das Restrisiko, das von einem Fahrzeugsystem ausgeht, in einen gesellschaftlich vertretbaren Rahmen zu bringen. Die ISO 26262 hat zur Aufgabe,

- die Konsequenzen von Fehlfunktionen von Fahrzeugfunktionen systematisch zu untersuchen und zu klassifizieren (GuR),
- die mögliche Ursache von Fehlfunktionen zu analysieren und zu dokumentieren und
- durch geeignete Maßnahmen in einem akzeptablen Rahmen zu halten.

1.2.1 Vorgehensmodell in der ISO 26262

Der erste Schritt innerhalb des Sicherheitslebenszyklusses ist die Bewertung der Gefährdung, die von einem zu realisierenden System ausgeht. Dabei werden üblicherweise die Aktoren des Systems und deren Einflussmöglichkeiten auf das Fahrverhalten des Automobils betrachtet. Weitere Kriterien bei der Bestimmung der Gefährdung sind das erwartete Schadensmaß, die Kontrollierbarkeit durch den Fahrer sowie die Häufigkeit der relevanten Fahrsituationen.
Das Ergebnis der Gefährdungsbewertung ist eine Einstufung der Kritikalität des Systems auf einer Skala von A bis D – der sogenannte Automotive Safety Integrity Level (ASIL), wobei A die geringste Kritikalität und D die höchste Kritikalität bezeichnet.
Um mit den Gefährdung durch das System umzugehen werden im Laufe der Entwicklung Sicherheitsmaßnahmen definiert, die entweder

- die Auftretenswahrscheinlichkeit eines Fehlers reduzieren (Verwendung höherwertiger Bauteile)
- die Fehler innerhalb des Systems erkennen und das System in einen vorher definierten Zustand überführen,
- die Kontrollierbarkeit durch den Fahrer erhöhen, indem zum Beispiel die Reaktionen des Systems verlangsamt werden, damit der Fahrer die Möglichkeit erhält, einen Fehler im Systems zu erkennen und abzuwenden bzw.
- das Schadensmaß durch das System zu verringern.

Für die meisten Systeme wird eine Kombination dieser Maßnahmen definiert und umgesetzt. Die Wirksamkeit muss durch entsprechende Studien und/oder Analysen nachgewiesen werden, um tatsächlich den gewünschten Effekt auf die geforderte Sicherheit zu erreichen.

1.2.2 Ursachenanalyse

Die Ursachen für ein sichtbares Fehlverhalten können vielfältig sein:

- Ausfall von einzelnen Systemkomponenten wie Widerständen, Transistoren, Spulen, Relais etc.
- Nicht korrekte Funktion komplexer Bauteile wie Prozessoren, auf denen die Steuerungssoftware ausgeführt wird
- Bereitstellung fehlerhafter Sensorwerte bei Ausfall eines Sensors
- Übertragungsfehler zwischen Sensor, Steuergerät und Aktorik
- Software-Fehler im weitesten Sinne, also Spezifikationsfehler, Programmierfehler oder Fehler während der Ausführungszeit durch Ausfälle der genutzten Hardware

In allen Fällen geht es darum, diese Fehler zu erkennen und geeignet zu reagieren – durch Warnung des Fahrer und/oder Überführung des Systems in den sicheren Zustand.
Die derzeitigen Ursachenanalysen umfassen keine Untersuchung auf

- unberechtigten Zugriffe auf die genutzten Signale/ Daten,
- auf Befall durch Malicious Code,
- Ausnutzung der Schwächen von Client-/Server-Applikationen.

In der derzeitig vorliegenden Version der Norm ISO 26262 gibt es nur eine Anforderung bzgl. der Untersuchung von Security Breaks als mögliche Ursachen für Verletzungen von Sicherheitszielen (safety goals). Im Rahmen des Fault Injection Tests soll u. a. auf »Mutationen des Codes« geprüft werden: »This includes injection of arbitrary faults (e. g. by corrupting values of variables, by introducing code mutations, or by corrupting values of CPU registers)« (Deutsches Institut für Normung 2011b).
Mit der Integration von *fahrzeugexternen* Signalen muss deren Korrektheit in entsprechenden Sicherheitsanalysen systematisch geprüft bzw. durch Sicherheitsmaßnahmen verifiziert werden. So kann ein von einem anderen Fahrzeug gesendetes Signal dazu führen, dass das System des eignen Fahrzeugs (scheinbar) fehlerhaft reagiert, wenn das Eingangssignal entweder falsch war oder mutwillig gefälscht wurde. Die dafür notwendigen Methoden sind im Bereich »Security« beschrieben und müssen für die Ziele der funktionalen Sicherheit angewandt und ggf. adaptiert werden.

2. Security – Vertraulichkeit, Integrität und Verfügbarkeit

Die Ziele der Informationssicherheit werden seit vielen Jahren mit dem Vorhandensein von Vertraulichkeit, Integrität und Verfügbarkeit für elektronische Daten beschrieben. Dies bedingt die Anwendung und das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Bedrohungen (Deutsches Institut für Normung 2011a).
Bei der praktischen Umsetzung von Maßnahmen zur Informationssicherheit gilt es eine große Komplexität der zu beherrschenden Disziplinen zu meistern. Bei dieser Herausforderung bietet es sich an, sich an bekannten und weltweit anerkannten Referenzmodellen und Methoden zu orientieren.
Eine herausragende Rolle bei der Betrachtung der technischen Grundlagen der modernen Kommunikation zwischen beteiligten Systemen stellt z. B. das TCP-Referenzmodell dar.
Disziplinen, die sich aus einem solchen Modell ableiten lassen sind z. B.

- Management der passiven Netzwerk-Infrastruktur (z. B. Medien, Verteilerstandorte etc.)
- Management der aktiven Netzwerk-Infrastruktur (Router, Switches etc.)
- Management von Netzwerk-Basisdiensten (Adressvergabe, Namensauflösung, Routing etc)
- Management von Betriebssystemen (PC, Server, Mobil etc.)
- Management von Applikationen (PC, Server, Mobil etc.)

Bei der Software der drei erstgenannten Schichten (Link-, Network- u. Transport-Layer) handelt es sich um Code, der auf der Basis offener Standards entwickelt wird. Solche Standards werden maßgeblich durch die Beteiligung der Internet Engineering Task Force (IETF), der Internet Research Task Force (IRTF), und des Internet Architecture Board (IAB) entwickelt.
Handelt es sich bei der Software der drei erstgenannten Schichten häufig sogar um offenen Code, dessen Schnittstellen in einem definierten Normungsprozess

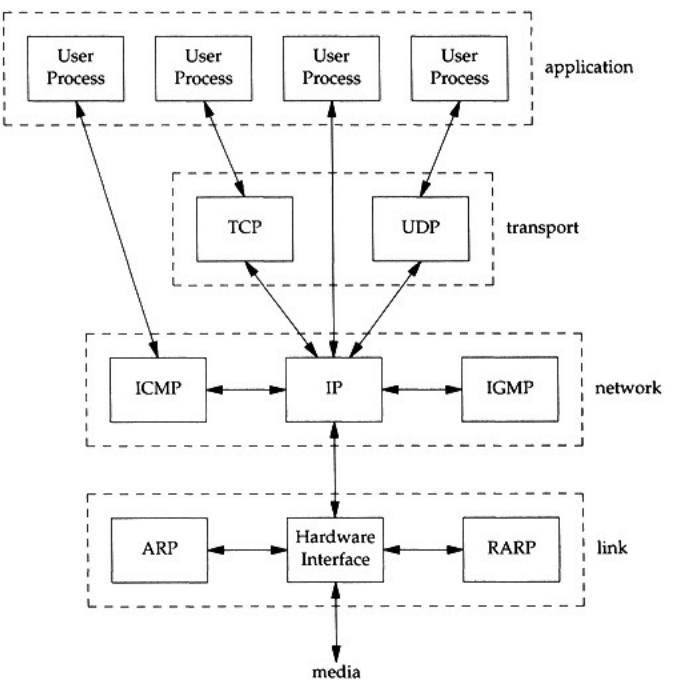

Abb. 1 TCP-Referenzmodell (Stevens 1994)

entstanden sind und Codereviews durch eine weltweite Entwicklergemeinde ermöglichen, so existiert in der Applikationsschicht weitgehend Wahlfreiheit, was den Entstehungsprozess und die Lizenzierung von Software betrifft. Die Beurteilung des Reifegrades proprietärer Software bzgl. Sicherheitsanforderungen fällt daher regelmäßig schwer.
Die Bedrohung für die Ziele der Informationssicherheit ergibt sich daher immer aus Schwächen der Software/ Protokolle der genannten Disziplinen. Solche Schwächen in der Standard-Software aller Schichten sind z. B. Grund für spektakuläre Einbrüche in Datenbanken, das Einschleusen von Schadcode in Industrieanlagen (Zetter 2011) und millionenfach infizierte Computer weltweit (Eikenberg 2016).

Um den Gefahren zu begegnen, die erst durch die Vernetzung digitaler Systeme entstanden sind, werden in der klassische Informationstechnologie eine Vielzahl unterschiedlicher Komponenten eingesetzt.

2.1 Schutzmechanismen der einzelnen Schichten

In der Applikationsschicht gilt es, den Bedrohungen der Informationssicherheit durch unberechtigte Zugriffe, Befall durch Malicious Code, Ausnutzung der Schwächen von Client-/Server-Applikationen, Einsicht durch Dritte sowie menschlichem Versagen zu begegnen. Um diesen Bedrohungen zu begegnen, wird in der klassischen Informationstechnologie eine große Zahl verschiedener Werkzeuge bereit gestellt.

- Datenbackup
- Virenschutz
- Verschlüsselung (z. B. Festplatten, Dateien, E-Mails)
- Zugangssteuerung und Authentisierung (z. B. Passwörter, Zweifaktorauthentifizierung, Zertifikate)
- Schutz gegen unberechtigte Verbindung (z. B.Hostbasierte Firewallsysteme)
- Einbruchserkennung (z. B. Hostbasierte Intrusion Detection Systeme, IDS)
- Secure Software Develop Lifecycle (SSDL)

Die Maßnahmen zur Absicherung der Transportschicht richten sich gegen die Bedrohung der Einsicht von Daten während der Datenübertragung durch Dritte. Da die Standard Protokolle der Transportschicht Transmission Control Protocol (TCP) und User Datagram Protocol (UDP) aufgrund Ihrer Architektur zunächst keine eigenen Methoden zur Verschlüsselung liefern, kommen nach-

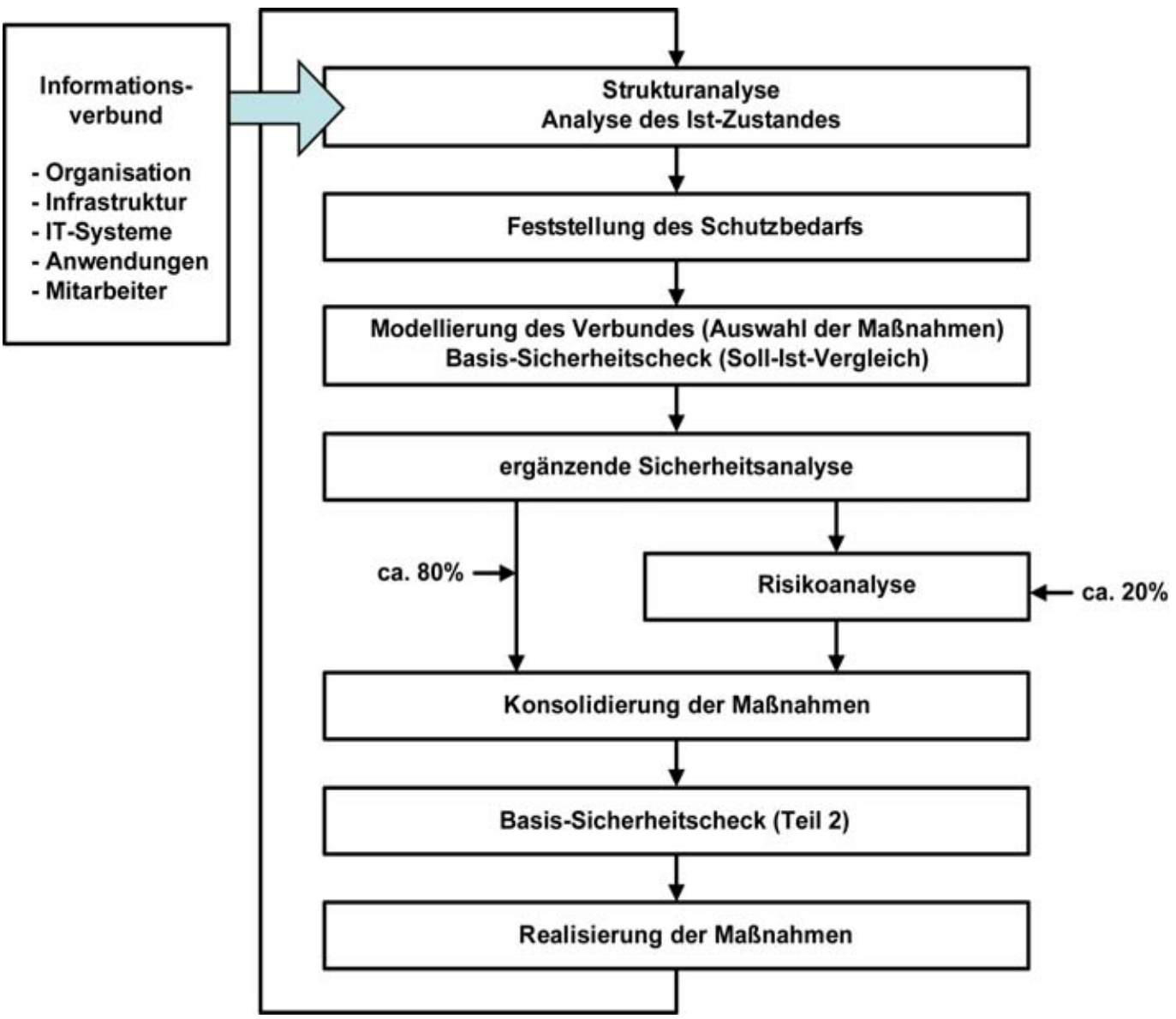

Abb. 2 Erstellen der Sicherheitskonzeption im Sicherheitsmanagement (Bundesamt für Sicherheit in der Informationstechnologie 2008)

träglich entwickelte Protokolle Secure Socket Layer (SSL) bzw. Transport Layer Security (TLS) zur Anwendung.
Das Standard Protokoll der Netzwerkschicht ist das Internet Protocol (IP) in den beiden Versionen 4 und 6 (IPv4, IPv6). Die Hauptaufgabe des Protocols besteht in der logischen Adressbildung und der Möglichkeit, Datagramme zu fragmentieren. Auch das Internet Protocol verfügt aufgrund der Architektur über keine eigenständigen Sicherheitsfunktionen.
Bedrohungen der Netzwerkschicht richten sich insbesondere gegen die Integrität und Verfügbarkeit der übertragenen Daten. Sicherheitssysteme der Netzwerkschicht analysieren daher die Headerinformationen von Netzwerkprotokollen und nutzen Regelwerke, um eine Kommunikation zu erlauben oder zu unterbinden. Netzwerkübergänge werden mit Hilfe sogenannter Statefull Inspection Firewalls abgesichert.
Mit Hilfe der Analyse des gesamten Netzwerkverkehrs und der Suche nach auffälligem und von der Norm abweichendem Verhalten innerhalb von Datenströmen ist es möglich, Eindringversuche und Angriffe, aber auch falsch konfigurierte Systeme zu erkennen. Sogenannte Einbruchserkennungssysteme (Intrusion detection Systems, IDS) werden ebenfalls an den Übergängen von Netzwerken verwendet, um Firewallsysteme zu ergänzen.
Darüber hinaus wird eine dritte Art von Sicherheitssystemen an den Übergängen von sicheren in die ungesicherten Netze der Provider verwendet. Es handelt sich um sogenannte Application Layer Gateways (sog. Proxy Systeme), die jeweils für ein Anwendungsprotokoll (z. B. HTTP/HTTPS) bereit gestellt werden. Proxy Systeme analysieren die Protocol Informationen sowie die Inhalte der übertragenen Daten. Aktuelle Proxiesysteme erlauben es, den Datenstrom auf Schadsoftware zu untersuchen. In den Unternehmen werden für das Erkennen von Schadsoftware sogar verschlüsselte Verbindungen terminiert und anschließend wieder verschlüsselt.

2.2 ISMS »family of standards«

Das Management der Informationssicherheit ist seit vielen Jahren integraler Bestandteil einer umfassenden Risikovorsorge in den Unternehmen. Als weltweit anerkannter Standard für das Management der Informationssicherheit gilt das Informationsmanagementsystem (ISMS) »familiy of standards« der Normenreihe ISO/IEC 2700x. Die ISMS »familiy of standards« soll Organisationen jeder Art und Größe bei der Umsetzung und dem Betrieb eines ISMS unterstützen (Deutsches Institut für Normung 2011a) und wurde vom Joint Technical Committee ISO/IEC JTC 1, »Information technology«, Subcommittee SC 27, »IT Security techniques« erarbeitet.
Sie gilt damit als Stand der Technik zur Handhabung der Informationssicherheit.

2.3 Common Criteria (CC)

Eine Aussage über den Reifegrad von IT-Sicherheitskomponenten ist mittels ISO 15408 (Common Criteria, CC) möglich. Auch diese internationale Normenreihe gilt als Stand der Technik und definiert einen Prozess, mit dem ein internationaler Vergleich von Security-Komponenten ermöglicht wird. Die Zertifizierung in Deutschland erfolgt durch das Bundesamt für Sicherheit in der Informationstechnologie.

3. Security for Safety

Die Bedeutung klassischer Disziplinen der Informationstechnologie für die Automobilbranche wird durch einen Blick auf die Projektliste der International Organization for Standardization (ISO) TC22 deutlich (z. B. GBit Ethernet, DoIP, ExVe Webservices etc.).
Im Hinblick auf Bestrebungen, ein ISMS für die Entwicklung elektrischer, elektronischer oder programmierbarer Systeme der Automobilbranche zu entwickeln, sei auf die internationalen Normen ISO/IEC 27011 »Informationssicherheitsmanagement-Leitlinien für Telekommunikationsunternehmen auf Basis von ISO/IEC 27002«, 27015 »Informationssicherheitsmanagement-Leitlinie für Financial Services«, 27019 »Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002« und ISO 27799 »Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002« hingewiesen.
So wird innerhalb der ISO zurzeit ein Projektvorschlag zur ISO 26262 in Verbindung mit dem Management der Informationssicherheit diskutiert. Der DIN unterstützt den Projektvorschlag und wird im Fall einer Projektannahme einen deutschen Spiegelkreis einrichten. Mit einem Ergebnis zur Annahme des Projektvorschlages wird Anfang Mai gerechnet.
Obwohl Safety- und Security-Prozesse sich auf den ersten Blick durchaus ähneln und sowohl ähnliche Rollen, als auch ähnliche Begriffe verwenden, wird es bei der künftigen Entwicklung von sicherheitsgerichteten Fahrassistenzsystemen nicht ausreichen, beide Disziplinen getrennt voneinander zu betrachten. Vielmehr ist es notwendig, die Methoden beider Disziplinen in einem Entwicklungszyklus zu integrieren und die Ergebnisse auszutauschen. Dazu wird es zwei Sicherheitsbetrachtungen zu einem Fahrzeugsystem geben, deren Aussagen zueinander in Übereinstimmung gebracht werden müssen.

Literatur

Borchert J, Slusser S (2014) Automotive (R)evolution: Defining a Security Paradigm in the Age of the Connected Car. http://www.infineon.com/dgdl/car_security_white_paper111914_lowres.pdf?fileId=5546d4614bcaeeb6014bef227039027d. Accessed 22 Feb 2016

Bundesamt für Sicherheit in der Informationstechnologie (2008) BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise Version 2.0. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard02/ITGStandard02_node.html. Accessed 22 Feb 2016

Dannenberg J, Burgard J (2015) Car Innovation 2015. Innovationsmanagementin der Automobilindustrie. http://www.car-innovation.de/fileadmin/user_upload/pdf/downloads/studie_car_innovation_2015.pdf. Accessed 22 Feb 2016

Deutsches Institut für Normung (2009) ISO/IEC 15408-1. Information technology – Security techniques – Evaluation criteria for IT security. Part 1: Introduction and general model. Beuth, Berlin

Deutsches Institut für Normung (2011a) DIN ISO/IEC 27000. Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC DIS). Beuth, Berlin

Deutsches Institut für Normung (2011b) ISO 26262. Road vehicles – Functional safety. Beuth, Berlin

Eikenberg R (2016) Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde. http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html. Accessed 22 Feb 2016

Harding J, Powell G, Yoon R, Fikentscher J, Doyle C, Sade D, Lukuc M, Simons J, Wang J (2014) Vehicle-to-vehicle communications: Readiness of V2V technology for application, Report DOT HS 812 014. National Highway Traffic Safety Administration, Washington DC

Spiegel Online (2009) Die Ohnmacht der Piloten. Wenn Computer im Cockpit zum Risiko werden. http://www.spiegel.de/spiegel/print/d-66208623.html. Accessed 29 Feb 2016

Spiegel Online (2016) USA: Unfall mit selbstfahrendem Auto – Google räumt Mitschuld ein. http://www.spiegel.de/auto/aktuell/selbstfahrendes-google-auto-in-unfall-verwickelt-konzern-raeumt-mitschuld-ein-a-1079957.html. Accessed 01 Mar 2016

Stevens WR (1994) TCP/IP illustrated. Volume 1: The Protocols. Addison-Wesley, Boston. ISBN: 978-0-201-63346-7

Süddeutsche Zeitung (2010) Schwedens “Vision Zero”: Bis 2020 keine Verkehrstoten mehr. http://www.sueddeutsche.de/auto/crashtest-jubilaeum-bei-volvo-auftrag-totalschaden-1.941807-3. Accessed 29 Feb 2016

Zetter K (2011) How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/1. Accessed 22 Feb 2016

Autoren

Dipl.-Inf. Ronald Melster
Croniq Ingenieurgesellschaft mbH
ronald.melster@croniq.de

Dipl.-Ing. Tilo Schneider
Croniq Ingenieurgesellschaft mbH
tilo.schneider@croniq.de