Herausforderung Security und Safety
Anforderungen an die Security im Kontext der ISO 26262

Dr. Jens Christian Lisner, TÜV NORD Mobilität

Bedingt durch die aktuellen Entwicklungen im Bereich der Automobilindustrie, wie etwa verschiedene Telematik-Anwendungen, entstehen auch für sicherheitskritische Systeme im Sinne von Safety zusätzliche Anforderungen durch die Car-Security. Dabei stellt sich die Frage ob sich die beiden Disziplinen gegenseitig ergänzen oder sogar behindern, und welche Konsequenzen daraus gezogen werden können.

Anders als im Deutschen kennt das Englische zwei Begriffe von Sicherheit. Die Safety ist die Abwesenheit von Risiken in Form von Unfällen. Security bezieht sich dagegen auf die Abwehr gegen Angreifer zum Beispiel bei Diebstahl oder Vandalismus. In der IT-Industrie haben beide Begriffe ihren festen Platz.

Funktionale Sicherheit und Car-Security

Klassischerweise ist ein Auto ein geschlossenes System, so dass Gefahren durch elektrische und/oder elektronische (E/E-) Systeme im Ausfall von Hardware- oder Softwarekomponenten zum Beispiel durch zufällig Auftretende Bauteilfehler oder Software-Fehler, bestehen. Dies ist die Spielwiese der funktionalen Sicherheit („functional safety“), die nach ISO 26262 als die Abwesenheit unzumutbarer Risiken durch fehlerhafte E/E-Komponenten (s. [1] Teil 1 1.51) definiert ist. Welches Risiko noch zumutbar ist, das ergibt sich aus den Anforderungen eines Standards, wie der ISO 26262, die sich speziell an die Automobilindustrie richtet.

Die ISO 26262 wurde in der aktuellen Fassung 2011 veröffentlicht und ist bis heute in der Automobilindustrie weitgehend adaptiert worden. Eine überarbeitete zweite Edition ist für 2018 geplant. Inhaltlich beschäftigt sich die ISO 26262 mit funktionaler Sicherheit für Personenfahrzeuge, d.h. unter 3,5 t. Dafür werden Anforderungen entlang des Sicherheitslebenszyklus‘ von sicherheitsrelevanten Fahrzeugfunktionen (z.B. adaptive Geschwindigkeitsregelung oder elektronisch Parkbremse) gestellt. Ein solches System soll so entwickelt werden, das es im Fall von Fehlern der Hard- oder Software-Komponenten in einen sicheren Zustand geht. In den meisten Fällen besteht der sichere Zustand in der Abschaltung des Systems.

Sicherheit im Sinne von Security hat auch in der Automobilindustrie eine lange Tradition in Form von Autotürschlössern und Wegfahrsperren. Relativ neu ist allerdings die Gefahr durch den Angriff auf programmierbare Systeme in Form von Steuergeräten, die auch sicherheitskritische Funktionen übernehmen können (im folgenden Car-Security genannt). Gerade in diesem Jahr sind mehrere spektakuläre Angriffe auf Steuergeräteebene, bekannt geworden (siehe z.B. [2], [3]). Möglich werden solche Angriffe durch die verstärkte Benutzung nach außen offener Schnittstellen für, unter anderem, Telematiksysteme, Car2x Anwendungen, Online Software Updates und auf Internet-Technologie beruhenden Infotainment-Systemen. Während die klassischen

Schließsysteme noch von einem Angreifer am Auto durch direktes Eingreifen überwunden werden müssen, sind Angriffe im Sinne der Car-Security potentiell auf eine ganze Fahrzeugflotte anwendbar und können gegebenenfalls auch entfernt und sogar automatisiert durchgeführt werden.

Im Gegensatz zur Funktionalen Sicherheit gibt es noch keinen etablierten Security-Standard im Bereich der Automobilindustrie. Verschiedene Arbeitsgruppen von Standardisierungsgremien, oder Interessenvertretungen der Industrie, wie der VDA, entwickeln derzeit noch entsprechende Standards. Bis dahin finden bekannte Security-Standards wie die ISO 27001 (siehe [4]) oder die Common Criteria (siehe [5]) Anwendung.

Wechselwirkung zwischen Safety und Security

Funktionale Sicherheit (Safety) und Car-Security sind beide „First-Class“ Probleme, d.h. beide sehen sich von der Wichtigkeit an erster Stelle. Die Funktionale Sicherheit soll vor Gefahren für Leib und Leben schützen, während die Car-Security den Schutz des Fahrzeugs, und eben auch der sicherheitskritischen Systeme, vor Angreifern sicher stellt. Kommt es dabei zu wiedersprechenden Anforderungen, ist es nicht möglich einseitig entweder der Security oder der Safety Vorrang einzuräumen. So ist Kryptographie für sicherheitsrelevante Systeme mit harten Echtzeitanforderungen derzeit noch eine Herausforderung, da die bekannten starken kryptographische Algorithmen einen nicht unbeträchtlichen Mehraufwand an Speicherplatz, Bandbreite und Rechenkapazität benötigen. Auch wenn die Forschung auf dem Gebiet im laufenden Gange ist (siehe z.B. [6]), ist derzeit noch ein Spagat zwischen Safety, Security und nicht zuletzt Kosten nötig. Dazu kommt, dass die Erfahrungen mit dem Internet zeigen, dass die Anforderungen an die Kryptographie steigen, und damit der Bedarf an Rechenkapazität in den Steuergeräten. Für ein Auto, das zehn bis fünfzehn Jahre im Gebrauch ist, bedeutet das unter Umständen, dass die Hardware nach ein paar Jahren nicht mehr in der Lage ist die geforderte Security unter Beibehaltung der notwendigen Echtzeitanforderungen sicherzustellen.

Im Folgenden werden drei verschiedene Arten wie Safety und Security wechselwirken können vorgestellt.

Einfluss der Safety auf die Security

Zunächst kann ein Fehler die Security beeinträchtigen. Bei einer elektronischen Wegfahrsperre (ESCL – Electronic Steering Column Lock) beispielsweise kann ein Fehler dazu führen das die Wegfahrsperre öffnet. Zwar ist die ESCL selbst ein Sicherheitsrelevantes System, da ein fehlerhaftes Schließen während der Fahrt Gefährlich ist, aber der Fall des fehlerhaften Öffnens der die Security beeinträchtigt, würde von einer Gefahren- und Risikoanalyse (HARA – Hazard Analysis an Risk Assessment) nach ISO 26262 nicht als Gefahrensituation identifiziert, da das Fahrzeug in diesem Szenario nicht fährt, und es damit nicht zu Schaden kommen kann. Andere Folgen von zufälligen Hardware- oder systematischen Hardware- oder Software-Fehlern können Sicherheitslücken in der Software, oder ein Aushebeln der Krypto-

graphie sein. Ein Beispiel für ein Szenario könnte ein Zufallsgenerator sein, der auf Grund eines Stuck-at-Fehlers konstante Werte zurück gibt. Eine andere Möglichkeit wäre der Ausfall einer Firewall im Systembus des Autos. Das könnte zur Folge haben, dass Security-Mechanismen Safety-Anforderungen haben, z.B. diversitär ausgelegt werden müssten, was einem Angreifer wiederum zwei potentielle Angriffswege eröffnet.

Einfluss der Security auf die Safety

Auf der anderen Seite kann ein Angriff auf die Safety beeinträchtigen. Im offensichtlichen Fall eines direkten Angriffs auf z.B. Fahrerassistenzsysteme, kann ein Angreifer die Kontrolle über sicherheitsrelevanter Systeme erlangen. In diesem Fall kann der ASIL zumindest einen Anhaltspunkt bei der Bewertung der Kritikalität bieten.

Ein Sonderfall liegt vor, wenn die sicherheitskritischen Systeme gar nicht Ziel des Angriffs sind, aber die Absicherungsmechanismen eines Sicherheitskritischen Systems (z.B. als Seiteneffekt eines Angriffs) ausfallen. In solchen Fällen arbeiten Security- und Safety-Maßnahmen nicht richtig zusammen; möglicherweise sogar gegeneinander.

Ein Fehlschluss ist übrigens die Annahme, dass die Sicherheitsmechanismen zur Erkennung von Fehlern Angriffe ausreichend erkennen und behandeln können in dem das System in den sicheren Zustand gebracht wird. Wenn das Ziel des Angriffs nicht sowieso der sichere Zustand (d.h. Abschaltung) ist, dann muss davon ausgegangen werden, dass die Sicherheitsmechanismen ebenso von dem Angriff betroffen sind. In der Safety werden beim Design von Sicherheitsmaßnahmen verschiedene vereinfachende Annahmen gemacht. Zufällige Hardware-Fehler werden grundsätzlich als statistisch erfassbar angenommen. Insgesamt ist die Sicherheitsarchitektur in der ISO 26262 auf der Annahme von einem Einzelfehler und einem latenten Fehler aufgebaut. Solche Grundannahmen sind in der Security aber nicht mehr haltbar. Ein intelligenter Angreifer ist also möglicherweise in der Lage ein System so anzugreifen, das die Sicherheitsmechanismen den Angriff nicht erkennen.

ISO 26262 und Security

Obwohl es also die Notwendigkeit gibt Safety und Security gleichermaßen zu berücksichtigen, und beide Disziplinen wechselwirken, kommt die Security in der ISO 26262 nicht vor. Als Norm aus der funktionalen Sicherheit beschäftigt sie sich ausschließlich mit Safety-Anforderungen. Zusätzliche Anforderungen aus externer Quelle sind während der Software-Entwicklung ab dem Design der Software-Architektur vorgesehen. Dies ist in der Regel zu spät, wenn bedingt durch widersprechende Anforderungen zusätzliche Anforderungen auf Systemebene entstehen, oder das komplette Design überarbeitet werden muss. Deshalb müssen Anforderungen der Safety und Security bereits ab der Designphase zusammen entwickelt werden. Für die Entwicklung von COTS-(Commercial-of-the-shelf) Komponenten, bedeutet dies auch, dass Annahmen und Hinweise bezüglich der Security im Safety Manual dokumentiert werden.

Erweiterter Fokus der HARA

Um die Entwicklung von Security Anforderungen von Seiten der Safety von Beginn an zu Unterstützen, kann bereits mit der HARA begonnen werden. Dazu kann bei der Analyse von Gefährdungssituationen der Fall „Manipulation“ als allgemeiner Oberbegriff eingeführt werden um zusätzliche gefährliche Situationen zu betrachten. Dadurch ließen sich auch Szenarien wie „Verlust der Fahrfunktion in ungewöhnlichen Umständen“, Mehrfehlerszenarios und Täuschung des Fahrers, beispielsweise durch bewusst falsche Anzeigen auf der Armatur. Zusätzlich wären hier schon die Ergebnisse einer Threat-Analyse zu berücksichtigen.

Zusammenfassung

Neben der Safety ist auch die Security als zweites „First Class“ Problem im Automobil angekommen. Obwohl es zur Car-Security noch keinen allgemein anerkannten Standard gibt, ist es bereits jetzt notwendig die Security in der Entwicklung zu berücksichtigen. Da Safety und Security miteinander wechselwirken müssen Safety und Security Anforderungen von Beginn an zusammen entwickelt werden. Dabei muss die Security auch in den Safety Manuals Eingang finden. Als erster Ansatzpunkt kann die Berücksichtigung von Threat-Analysen beginnend mit der HARA sein. Der Fall Manipulation kann hilfreich sein, um zusätzliche Szenarien zu betrachten. Richtig ist aber auch, dass Security und Safety Methoden nicht einfach vermischt werden können. Safety- und Security-Anforderungen müssen gleichwertig berücksichtigt werden.

Literatur

[1] ISO 26262 – Road vehicles – Functional safety, Teil 1-10, International Standard, 2011

[2] Spaar, Dieter: Auto öffne dich! – Sicherheitslücken bei BMWs ConnectedDrive. www.heise.de/ct/ausgabe/2015-5-Sicherheitsluecken-bei-BMWs-ConnectedDrive-2536384.html (abgerufen am 16.10.2015)

[3] Timberg, Craig: Hacks on the Highway. www.washingtonpost.com/sf/business/2015/07/22/hacks-on-the-highway/ (abgerufen am 16.10.2015)

[4] ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements, International Standard, 2013

[5] Common Criteria for Information Technology Security Evaluation, Version 3.1 Rev. 4, International Standard, 2012

[6] Philipp Mundhenk, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. Fahmy, and Samarjit Chakraborty. 2015. Lightweight authentication for secure automotive networks. In Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE '15). EDA Consortium, San Jose, CA, USA, 285-288.

Autor

Dr. Jens Christian Lisner (jlisner@tuev-nord.de) ist Informatiker und hat promoviert im Bereich Fehlertoleranz von Echtzeitsystemen. Er ist seit 2007 beim TÜV NORD Institut für Fahrzeugtechnik und Mobilität als Experte für eingebettete Netzwerke im Automobilbereich und funktionale Sicherheit. Den TÜV NORD IFM vertritt er im deutschen Arbeitskreis "Software und Prozesse" des Normenausschuss zur ISO 26262.