Funktionale Sicherheit in der Luft- und Raumfahrt

Funktionale Sicherheit kommt zum Einsatz, wenn Produkte, Anlagen und Prozesse so komplex sind, dass deren Sicherheit auf einfachem Weg nicht mehr ausreichend getestet werden kann – dies gilt sowohl für den Boden als auch für die Luft.

Im Vorfeld der VDE DKE Tagung zur funktionalen Sicherheit haben wir mit Florian Lumpe vom Deutschen Zentrum für Luft- und Raumfahrt gesprochen.

VDE DKE: *Herr Lumpe, was ist Ihre Funktion beim Deutschen Zentrum für Luft- und Raumfahrt?*

Lumpe: Beim DLR nehme ich eine querschnittsübergreifende Rolle ein und koordiniere Produktsicherungsthemen bei den Instituten und Einrichtungen für den Bereich Forschung und Technologieentwicklung. Das betrifft alle Forschungsschwerpunkte des DLR wie Raumfahrt, Luftfahrt, Energie, Verkehr sowie Sicherheit und Digitalisierung. Das macht die Arbeit komplex, aber auch wahnsinnig spannend.

Das DLR ist sowohl horizontal als auch vertikal sehr stark diversifiziert, was für Querschnittsaufgaben eine große Herausforderung darstellt, um alle Themen unter einen Hut zu bekommen. Wir konnten jedoch in den letzten Jahren eine gute Struktur schaffen. Zudem ändern sich vielleicht die Anwendungen der verschiedenen Fachthemen, jedoch nicht unbedingt die Methodiken.

VDE DKE: *Sie werden bei der VDE DKE Tagung zur funktionalen Sicherheit einen Vortrag zur „Sicherheit in der Raumfahrt“ halten. Sicherheit in der Raumfahrt klingt sehr spannend, weil bei Fehlschlägen schnell dramatische Bilder entstehen wie bei der Starship-Explosion von SpaceX. Wie muss ich mir das vorstellen: Wenn ein Satellit im Orbit ist, dann kann man diesen ja nicht mehr einfach reparieren, wie es bei Industrieanlagen möglich ist?*

Lumpe: Die Fragen und Anmerkungen sind aufgrund der Komplexität nicht schwarz oder weiß zu beantworten. Zunächst ein paar gängige Begriffe aus der Raumfahrt, die mit der funktionalen Sicherheit vergleichbar wären:

In der europäischen Raumfahrt wird der Begriff „Produkt Assurance“ verwendet. Das schließt alle Aktivitäten zur Absicherung eines Projektes ein – von der Planung und Umsetzung bis hin zur Überwachung von Aktivitäten, um letztendlich die Qualität eines Produktes sicherzustellen. Produktsicherungsmanagement bedeutet in unserem Sinne eine Teildisziplin des Qualitäts- und Projektmanagements. Ziel der Produktsicherung ist es, eine sichere, erfolgreiche und zuverlässige Weltraummission zu gewährleisten.

Bei der NASA oder JAXA wird deshalb von „Safety and Mission Assurance“ gesprochen. Die Produktsicherung behandelt das Management von Risiken, und häufig das Management von Anomalien und Abweichungen, die

während der Tests auftreten. Dies umfasst alle technischen Subsysteme eines Raumfahrtproduktes und insbesondere deren Materialien und Fertigungsprozesse, Software, EEE-Komponenten, Zuverlässigkeit, Fehlerverkettung und deren Vermeidung sowie Safety und Security.

Die aktuellen Vorkommnisse bei den Tests von SpaceX mit der SN8 sehen dramatisch aus, jedoch handelt es sich dabei um sehr innovative Technologien mit einem niedrigen „Technological Readiness Level“. Dies sollte man von den klassischen Raumfahrtaktivitäten oder aktuellen Missionen getrennt beachten. Allein schon die Verwendung von Edelstahl als Primärstruktur des StarShip ist ein unglaublicher Paradigmenwechsel. Zudem verlief das Flipover-Manöver so zuverlässig wie ein Schweizer Uhrwerk. Leider ist zum Schluss ein Triebwerk ausgefallen und es kam zum Absturz.

Der große Unterschied zwischen Raumfahrtprojekten und klassischen Industrieprojekten ist, dass Reparaturen bei Fehlfunktionen so gut wie unmöglich werden. Deshalb muss so weit wie möglich prophylaktisch gearbeitet und entwickelt werden. Reparaturen im Sinne der Raumfahrt werden nur am Boden, zum Beispiel während des Produktionsprozesses, durchgeführt. Jedoch gilt es nach Möglichkeit immer die Ursache zu finden und nicht die Symptomlinderung durch Reparaturen.

Befindet sich ein Satellit im All, besteht nur noch die Möglichkeit, die Software durch Updates zu modifizieren, um in seine Funktionalität einzugreifen. Das hat einen sehr begrenzten Effekt und hilft nur selten bei schweren Ausfällen der Hardware. Es wäre theoretisch denkbar, einen Astronauten ins Weltall zu schicken, wie das bei der Reparatur des Hubble-Teleskops erfolgte, aber das ist im Augenblick durch den Wegfall des Space Shuttles nicht mehr möglich und viel zu teuer. Je sorgfältiger am „Boden“ gearbeitet wird desto zuverlässiger und sicherer werden die Mission und der Betrieb im All. Wir dürfen nicht vergessen: Raumfahrt ist immer noch Technik am Rande des Möglichen.

VDE DKE: *Welche anderen Möglichkeiten gibt es, abgesehen von einem kontrollierten Absturz und Verglühen, wenn es zu Problemen im Orbit kommt?*

Lumpe: Für geostationäre Satelliten existiert noch die Möglichkeit, den Satelliten auf einen Friedhofsorbit zu steuern, der außerhalb des geostationären Orbits von 36.000 km Höhe liegt. Dieser Orbit ist international genau festgelegt und hält auf diese Weise wichtige Umlaufbahnen frei und vermeidet Weltraummüll, was allen Nachfolgemissionen zugutekommt. Voraussetzung dafür ist es, genügend Treibstoff und ein funktionierendes Triebwerks- und Kommunikationssystem an Bord zu haben. Für Satelliten, die der Erde näher sind, sollte der Wiedereintritt in die Erdatmosphäre immer kontrolliert erfolgen.

Am Beispiel von ROSAT wird deutlich, wie schnell so etwas außer Kontrolle geraten könnte, denn der Satellit ist 2011 nicht kontrolliert in die Erdatmosphäre eingetreten. Es bestand damals die Sorge, dass große Teile des Satelliten den Wiedereintritt überstehen und auf dem Boden einschlagen könnten. Am Ende verlief aber alles gut, denn mittels permanenter Positionsüberwachung der Position durch das Weltraumlage-Zentrum und entsprechende internationale Zentren konnte schnell Entwarnung gegeben werden. Für alle weiteren Missionen gilt dies aber als Warnschuss.

VDE DKE: *Mit dem Aufkommen von Megakonstellationen, Starlink ist wohl die bekannteste, wird immer wieder von den Gefahren durch Trümmer und dem sich daraus ergebenden Kessler-Syndrom berichtet. Sehen Sie hier eine Gefahr und müssen sich die Betreiber von Satelliten besser vernetzen?*

Lumpe: Starlink ist ein sehr ambitioniertes Projekt. Es sollen insgesamt 42.000 Satelliten in den Orbit geschossen werden. Wie SpaceX mit den Gefahren des Weltraumschrotts umgehen will, kann ich nicht beurteilen. Ich hoffe, dass die Satelliten über genügend Performance und Zuverlässigkeit verfügen, kontrolliert in die Erdatmosphäre einzutreten. Bei der Menge an Satelliten ist es nicht abwegig, dass der eine oder andere außer Kontrolle gerät. Wenn es dann zur Kollision kommt, werden die Orbiter in tausende Einzelteile pulverisiert. Diese wiederum bergen die Gefahr, in andere Satelliten einzuschlagen. Da reicht nur die Größe eines Senfkorns und schon ist die Katastrophe perfekt und der

Weltraummüll wächst exponentiell an. Diesen Effekt hatte man mit dem Beginn der Raumfahrt vernachlässigt, doch heute gefährdet er zunehmend den Betrieb von Satellitenmissionen. Ganz besonders gefährlich wird es für die bemannte Raumfahrt – im Worst Case macht es diese sogar unmöglich.

Fakt ist, dieses Problem lässt sich nur auf internationalem Parkett lösen, denn die Vermeidung und Entfernung von Weltraumschrott wird sehr viel Geld kosten.

VDE DKE: *Bei Industrieanlagen werden für Sicherheitsfunktionen häufig separate Geräte verwendet – also eigenständige Systeme, die autonom von anderen Systemen laufen. Wie ist das bei den Satelliten und Raketen? Ist dort alles direkt integriert und es wird keine Unterscheidung zwischen Betriebs- und Sicherheitsfunktion gemacht?*

Lumpe: Eine separate Sicherheitstechnik in dem Sinne existiert nicht. Es gibt die jedoch die recht junge Disziplin „Security“ in der Raumfahrt. Damit ist aber eher der Bereich Cybersecurity gemeint und soll das Hacken oder den physischen Angriff auf Satelliten verhindern.

Meistens sind Betriebsfunktionen und Sicherheitsfunktionen zusammenhängend aufgebaut. Bei der Lageregelung handelt es sich zum Beispiel sowohl um ein Navigationsinstrument als auch um Sicherheitselement, denn nichts ist ernster als ein außer Kontrolle geratener Satellit. Es gibt auch Notfallsysteme, die mehr oder weniger unabhängig vom Hauptsystem aufgebaut sind. Das kommt jedoch sehr auf die Mission und die Satelliten-Architektur an.

Das übergeordnete Ziel der Produktsicherung ist es, die Systeme sicher und zuverlässig zu gestalten. Das kann einerseits durch strahlenharte Elektronik erfolgen, anderseits durch eine redundante Systemarchitektur oder durch autonome Funktionen, die Fehler erkennen und auf Systemebene entsprechend reagieren. Das wird als „Failure Detection, Isolation and Recovery“ (FDIR) bezeichnet. Der Weltraum ist die denkbar ungünstigste Umgebung, um Systeme zuverlässig zu betreiben. Das liegt vor allem an den unwirklichen Bedingungen wie elektromagnetischer Strahlung sowie Beschuss des Raumfahrzeugs durch stark energetische Teilchen wie Elektronen, Protonen und Neutronen und starke Hitzeeinwirkungen. Nicht zu vergessen das Hochvakuum, das unter Umständen dazu führen kann, dass Materialien ausgasen. Unter Langzeitaspekten ist auch die Mikrogravitation nicht zu unterschätzen, denn unter Langzeitfolgen kann beispielsweise das Material der Elektronik anfangen, eigenartig zu fließen.

Grundsätzlich ist das alles sehr stark abhängig von der Mission. Im DLR Bereich Forschung und Technologie geht es hauptsächlich um Technologieerprobung, Grundlagenforschung, Erdbeobachtung oder Deep Space Exploration. Das DLR Raumfahrtmanagement deckt das gesamte Spektrum ab bis hin zur bemannten Raumfahrt.

Bei der bemannten Raumfahrt kommen nur Technologien zum Einsatz, die schon lange erprobt oder intensiv getestet wurden, denn hier steht die Sicherheit der Astronauten sowie ein ausgeklügelter Katastrophenschutz auf dem Spiel. Bei kommerziellen Satellitenprojekten steht die Zuverlässigkeit im Vordergrund, denn ein Totalausfall wäre ein finanzielles Desaster.

VDE DKE: *Unterscheidet sich bei der Infrastruktur am Boden die Herangehensweise an Sicherheit, wenn das Gewicht keine Rolle spielt?*

Lumpe: Ja, es unterscheidet sich zum Beispiel der Aufbau von Ground Support Equipment (GSE) zur Flug-Hardware. Für den Aufbau von GSE gelten grundsätzlich die nationalen Gesetzgebungen, Direktiven und harmonisierte Normen sowie die Kundenanforderungen wie für jedes andere Industrieprodukt in Europa auch. Zudem macht es an einigen Punkten keinen Sinn, die strengen Richtlinien der Raumfahrt anzuwenden.

Also könnten auch beim Bodenequipment Normen, zum Beispiel die der funktionalen Sicherheit auf Basis der Maschinenrichtlinie oder Druckgeräterichtlinie, eine große Rolle spielen. Wenn es beispielsweise darum geht, Betankungsanlagen aufzubauen, bewegen wir uns auf dem Gebiet der klassischen Prozessindustrie.

Die meisten wissenschaftlichen Aktivitäten des DLR finden sowieso am Boden statt. Nach Satzung des DLR sollen den Instituten und Einrichtungen, also den Wissenschaftlerinnen und Wissenschaftlern, „Großanlagen“ zur Verfügung gestellt werden. Die Forschungsanlagen entsprechen meistens der Größe einer Industrieanlage oder gehen noch darüber hinaus. Gemeint sind hier beispielsweise Weltraumsimulationsanlagen, Triebwerksprüfstände oder Hochgeschwindigkeitswindkanäle. Auch diese Anlagen müssen den gesetzlichen Bestimmungen und Direktiven entsprechen, um erstens den DLR Mitarbeitern einen sicheren Arbeitsplatz zu gewährleisten und zweitens, um Schäden beim Forschungsequipment auszuschließen. Da es sich meistens um Prototypen-Anlagen handelt, macht das die ganze Sache sehr anspruchsvoll. Keine Anlage gleicht der anderen. Wichtig dabei ist schon am Anfang der Planung einer solchen Anlage die Standards, Direktiven und Normen auf das Projekt zuzuschneiden. In der Raumfahrt spricht man von „Tailoring“.

VDE DKE: *An welchen Normen orientieren Sie sich?*

Lumpe: Normen spielen beim DLR eine sehr große Rolle. Für die europäische Raumfahrt gelten die Standards der European Cooperation for Space Standardization, kurz ECSS. Alle wichtigen Raumfahrtagenturen und industriellen Partnerfirmen Europas, aber auch Kanada und die Schweiz, sind dort vertreten und arbeiten in Working Groups an dem System zur Standardisierung mit. Die ECSS umfasst mehrere Disziplinen: Projektmanagement, Engineering und Produktsicherung. Die ECSS wird zudem durch CEN eins zu eins übernommen und offiziell in das europäische Normenwerk überführt.

Hinzugekommen ist noch das Thema der Nachhaltigkeit (Sustainability), welches sich mit den Fragen des Weltraummülls (Space Debris) und dessen Vermeidung beschäftigt. Oft werden aber auch ISO-Normen referenziert oder gar vollständig überführt. Bestes Beispiel ist Space Debris Mitigation Requirement, welches durch die Norm ISO 24113 übernommen wurde. Probleme wie Weltraummüll lassen sich nur auf internationaler Ebene und durch Standardisierung lösen wie die meisten terrestrischen Nachhaltigkeitsprobleme auch. Das DLR engagiert sich auf internationaler Ebene in den Normungsgremien von ISO TC 20/ SC14 in den jeweiligen Arbeitsgruppen der einzelnen Raumfahrt-Themen. Die meisten Nationen sind hier mit ihren Agenturen und Industrien vertreten.

VDE DKE: *Wie sehen in Ihrem Bereich die Trends der Zukunft aus? Wie ist Deutschland bzw. Europa darauf vorbereitet?*

Lumpe: Die Raumfahrt entwickelt sich – wie alles andere auch – rasant weiter. Neue Materialien, neue Missionsziele, modernes Marketing und vor allen Dingen die Kommerzialisierung der Raumfahrt sind die entscheidenden Schlüsselfaktoren. Wir beobachten einen Trend hin zu eigenständigen und autarken Organisationen wie SpaceX, Blue Origin und Virgin Orbital. In einem solchen Kontext herrscht ein geringerer Bedarf an Abstimmung mit externen Partnern. Das wiederum führt dazu, dass derartige Teams weniger eingeschränkt agieren können. Die Teammitglieder sind in der Regel hochmotiviert, hochkompetent und sie können sich immer wieder grundlegende Systemfragen stellen, um das Produkt weiter zu optimieren. Durch das Wegfallen externer Partner und vertraglicher Starrheit in Kombination mit finanzieller Unabhängigkeit entsteht eine Agilität, die revolutionäre, technologische Durchbrüche vorantreibt.

Unser Ziel sollte es sein, Rahmenbedingungen zu schaffen, in denen sich Ingenieure aller Parteien – Staat, Industrie und Forschung – frei austauschen können. Im Prinzip ein Forum, in dem Firmenzugehörigkeit und vertragliche Interessen temporär ausgeblendet werden. Nur durch den Wegfall von Barrieren und das Gefühl von Einigkeit kann ein Team dazu beflügelt werden in kurzer Zeit brillante Lösungen zu hochkomplexen Herausforderungen zu finden.

Wichtige Trends sind Software-Verbesserungen, Hardware-/Software-Systemintegration und Künstliche Intelligenz.

Das kann man sehr deutlich an der Dragon-Kapsel erkennen. Fast alles wird über Displays gesteuert, was sich in der aufgeräumten Innenarchitektur einer Kapsel bemerkbar machtbefindet. Das ist ein Zeichen dafür, dass die Systeme integraler angeordnet wurden als bisher.

Die Software spielt eine entscheidende Rolle, auch weil Gesamtsysteme dementsprechend gut simuliert, optimiert und getestet werden können. Ebenfalls erhält künstliche Intelligenz bei der Datenauswertung und Bewertung vermehrt Einzug, um den Datenmengen Herr zu werden.

Aber auch die Verwendung von Commercial of the Shelf (COTS) Bauteilen findet immer mehr statt. EEE-Komponenten, qualifiziert für die Raumfahrt, sind in der Regel kostenintensiv. Inzwischen geht man dazu über, kommerzielle Bauteile aus anderen Bereichen, vor allem dem Automotive-Bereich zu verwenden. Die Herausforderung hierbei ist es, die Gefahr von zum Beispiel Bit-Flip-Fehlern zu kompensieren. Auch Strahlungsaspekte müssen beachtet werden, weil diese im Automobilbereich eine geringere Relevanz haben. Daher werden COTS-Komponenten aus dem Automobilbereich häufig entsprechenden Delta-Tests unterzogen, um ihre Tauglichkeit für die Raumfahrt zu verifizieren.

Mit integralen Bauweisen und Verfahren will man ebenfalls die Anzahl von differenzierten Einzelteilen minimieren. Es gibt zum Beispiel sehr starke Aktivitäten, große Triebwerkskomponenten aus einem Stück zu drucken.

Zu guter Letzt sind es auch gerade politische Ambitionen, die der Raumfahrt Auftrieb geben. Barack Obama hat in seine Amtsperiode die Kommerzialisierung der Raumfahrt eingeleitet. Damit war es kommerziellen Anbietern möglich, Raumfahrttechnologie direkt anzubieten. Das hat zu einem starken Innovationsschub geführt. Für die europäische Raumfahrtindustrie wäre das auch ein gangbarer Weg, vielleicht mit einem neuen Raumfahrtgesetz?

Zudem steht in Zukunft die direkte gesellschaftliche Nutzung vermehrt im Vordergrund. Im Bereich der Forschung werden mittlerweile immer mehr Satelliten zur Erd-, Klima- und Wetterbeobachtung eingesetzt.

VDE DKE: *Vielen Dank für dieses Gespräch!*

Weiterführende Links:

Interview mit Florian Lumpe: dke.de/fusi-luftfahrt-raumfahrt

DKE Fachinformation zur funktionalen Sicherheit: dke.de/fusi

VDE DKE Tagung zur funktionalen Sicherheit 2021: dke.de/fusi21

Ansprechpartner:

Holger Lange

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
Stresemannallee 15
60596 Frankfurt am Main
Tel. +49 69 6308-291
Holger.Lange@vde.com

Über VDE DKE

Die vom VDE getragene DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (VDE DKE) ist die Plattform für rund 9000 Experten aus Wirtschaft, Wissenschaft und Verwaltung zur Erarbeitung von Normen, Standards und Sicherheitsbestimmungen für die Elektrotechnik, Elektronik und Informationstechnik. Normen unterstützen den weltweiten Handel und dienen u. a. der Sicherheit, Interoperabilität und Funktionalität von Produkten und Anlagen. Als Kompetenzzentrum für elektrotechnische Normung vertritt die DKE die Interessen der deutschen Wirtschaft in europäischen (CENELEC, ETSI) und internationalen Normenorganisationen (IEC). Darüber hinaus erbringt die DKE umfangreiche Dienstleistungen rund um die Normung und das VDE Vorschriftenwerk.

Mehr Informationen unter:

www.dke.de