SCHUTZGEBIETE

DLR-Fachleute erforschen, wie sich autonome und vernetzte Systeme gegen Cyberangriffe schützen lassen

von Dr. Hannes Bartz und Dr. Okuary Osechas

Flugzeuge ohne Piloten, Kontrolltürme ohne Fluglotsen und vernetzte Schiffe – es ist das Zeitalter der Vernetzung, die mit bahnbrechenden Entwicklungen auch neue Bedrohungen mit sich gebracht hat. Beispielsweise wurden im Juli 2019 im Hafen von Shanghai die Navigationssysteme mehrerer Schiffe so getäuscht, dass sie falsche Koordinaten kommunizierten und scheinbar geisterhaft an verschiedenen Stellen auftauchten und wieder verschwanden. Cybersicherheit ist aber auch für andere Bereiche relevant: So kommt es immer wieder zu Zwischenfällen, bei denen Unbekannte nicht autorisierte Anweisungen per Funkspruch an Flugzeuge senden. Die zunehmende Automatisierung von Systemen fördert zwar deren Zuverlässigkeit, aber ihre IT-Abhängigkeit öffnet sie gegenüber Cyberangriffen. Die dynamischen Entwicklungen lassen stets neue Schwachstellen und Bedrohungsszenarien entstehen. Im DLR-Querschnittsprojekt Cybersicherheit für vernetzte und autonome Systeme entwickeln Fachleute aus vier DLR-Instituten aus den Bereichen Sicherheit, Raumfahrt und Luftfahrt Technologien und Methoden, mit denen sich solche Angriffe verhindern lassen.

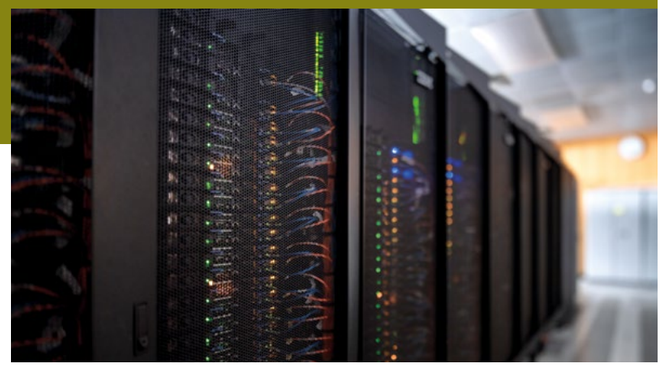
Was ist Cybersicherheit?

Die globale Vernetzung produziert riesige Datenmengen, die beständig ausgetauscht werden. Solche Prozesse bieten eine Angriffsfläche für Unbefugte. Dies gilt sowohl für weltweite Netzwerke als auch für sogenannte cyber-physische Systeme. Das sind zum Beispiel Flughäfen, auf denen verschiedene Komponenten miteinander interagieren und kommunizieren. Dementsprechend brauchen wir Maßnahmen, die solche Systeme gegen böswillige Angriffe schützen. Dafür steht der Begriff Cybersicherheit. Sicherheit lässt sich im Englischen mit „Safety“ und „Security“ übersetzen. Safety bedeutet in diesem Kontext Betriebssicherheit. Der Begriff Security bezeichnet die Sicherheit vor gezielten Eingriffen. Gerade in den Bereichen Luft- und Raumfahrt sind beide Begriffe oft eng miteinander verwoben. Im DLR-Querschnittsprojekt liegt der Fokus auf dem Bereich „Security“ von cyber-physischen Systemen.

RADARAUFNAHME VOM HAFEN OSLO

Radarbilder werden für viele Zwecke eingesetzt, zum Beispiel für die Erstellung eines dynamischen Lagebildes, mit dem maritime Strukturen überwacht werden. Dazu müssen die verwendeten Daten jederzeit zuverlässig und vertrauenswürdig sein. Das DLR-Institut für Hochfrequenztechnik und Radarsysteme erforscht Methoden, wie Stör-Einflüsse auf Radarbilder detektiert und verringert werden können.

Auch wenn Cyberbedrohungen ein breites Spektrum von Systemen und Anwendungen betreffen, gibt es grundlegende Thematiken, die ihnen gemein sind, wie zum Beispiel die Verfälschung von Informationen oder Signalen. Wenn Signale gestört oder verändert werden, sprechen die Fachleute von „Jamming“ oder „Spoofing“. Jamming kommt aus dem Englischen und bedeutet wortwörtlich übersetzt „klemmen“. Ein Jammer (Störer) stört ein System absichtlich so lange und intensiv, bis es nicht mehr funktionsfähig ist. Spoofing (Täuschung) bedeutet ursprünglich Parodie und bezeichnet ein bewusstes, gezieltes Täuschen eines nichtsahnenden Nutzers. Die DLR-Wissenschaftlerinnen und -Wissenschaftler entwickeln Techniken, mit denen sich sowohl die Einflüsse von Jamming als auch von Spoofing reduzieren lassen. Das können spezielle Verschlüsselungsverfahren sein, die sicherstellen, dass Daten nicht manipuliert werden, aber auch Verarbeitungstechniken wie die Ortung von Störern auf Radarbildern. Das DLR-Team analysierte hierfür bekannte Angriffe und entwickelte daraus entsprechende Gegenmaßnahmen.



Rechencluster am DLR-Institut für Aerodynamik und Strömungstechnik

Schutz von Informationen

Eine aktuelle Problematik im Luftfahrt-Bereich besteht darin, dass die Kommunikation heutzutage größtenteils noch analog und unverschlüsselt abläuft. Entsprechend anfällig sind gewisse Systeme gegen böswillige Eingriffe von außen. Das Flugverkehrsmanagement ATM (Air Traffic Management), das einen sicheren und effizienten Flugverkehr gewährleistet, befindet sich im Wandel von analogen hin zu digitalen Datenlinks. Neue digitale Kommunikationsstandards, mit denen die Flugzeuge sowohl untereinander als auch mit Tower und Lotsen kommunizieren, müssen entsprechend sicher sein. Das DLR entwickelte federführend die beiden Kommunikationssysteme LDACS (L-band Digital Aeronautical Communications System) und CDACS (C-band Digital Aeronautical Communications System). Diese können Daten in Echtzeit übertragen und sichern sie gegen Angriffe und Verfälschungen mittels kryptografischer Verfahren. Gegenwärtige kryptografische Methoden, wie sie auch für sichere Verbindungen im Internet (HTTPS) verwendet werden, haben Angriffen von Quantencomputern wenig entgegenzusetzen. Solche Rechner sind in der Lage, für klassische Computer äußerst komplexe Operationen durchzuführen und bergen deshalb entsprechende Risiken. Auch wenn bislang nur wenige Prototypen existieren, werden höchstwahrscheinlich in einigen Jahren leistungsfähige Quantencomputer verfügbar sein. Die sogenannte Postquantenkryptografie entwickelt neuartige Verschlüsselungsmethoden, die Systeme robust gegen Angriffe von Quantencomputern machen. In dem Querschnittsprojekt entwirft das DLR-Team Verschlüsselungsverfahren, die resistent gegen die Angriffe mittels Quantencomputern sind. So können Kommunikationssysteme in der Luftfahrt sowie in der Satellitentechnik langfristig abgesichert und Zwischenfälle wie unautorisierte Funksprüche vermieden werden.

Schutz von Signalen

Besonders anfällig sind Flugzeuge während ihres Landeanflugs. Satellitenbasierte Landeanflugsysteme bieten ein Einfallstor für Radiostörer (Jammer), aber auch für Signaltäuscher (Spoofer). Beide stellen Sicherheitsrisiken dar, die der heutige Stand der Technik größtenteils noch nicht decken kann. Bei einem Messflug im Februar 2020 zeigte das DLR, wie sich Radiostörer auf die Bordelektronik eines kommerziellen Linienflugzeugs auswirken können: Sie legten die gesamte Satellitennavigation lahm. Wenn so etwas passiert, muss der Pilot oder die Pilotin auf Sicht weiterfliegen. Im DLR-Institut für Kommunikation und Navigation werden Antennen und Satellitenempfänger entwickelt, die Landesysteme gegen solche Angriffe stärken. Die Antennen erkennen die Richtung des Signals und können einschätzen, ob diese plausibel ist – ob es sich beispielsweise um einen Satelliten handeln kann oder einen Spoofer, der von der Erde aus sendet. So lassen sich Jamming und Spoofing minimieren und es wird verhindert, dass Schiffe am „falschen Ort auftauchen“.

In den letzten fünf Jahren haben sich Aufklärungssysteme, die ein Radar mit synthetischer Apertur (SAR) verwenden, immer weiter verbreitet. SAR-Radare gehören zur Klasse der abbildenden Radare und werden zur Fernerkundung eingesetzt. Allerdings nehmen beabsichtigte und unbeabsichtigte Störungen ihrer Sensorik zu. Das DLR-Institut für Hochfrequenztechnik und Radarsysteme beschäftigt sich bereits seit geraumer Zeit damit, wie sich solche Störsignale auf das Bildmaterial auswirken und wie sie sich eliminieren lassen. Die Forscherinnen und Forscher entwickeln Methoden, mit denen sich ursprünglich gestörte Radarbilder rekonstruieren und trotzdem noch auswerten lassen, ohne dabei die Sende- oder Empfangsvorrichtungen verändern zu müssen. Darüber hinaus beschäftigen sie sich damit, wie zukünftige Systeme aussehen, die weniger störanfällig sind.

DAS DLR-QUERSCHNITTSPROJEKT CYBERSICHERHEIT FÜR AUTONOME UND VERNETZTE SYSTEME

Beteiligte Institute und Einrichtungen:

- Institut für Flugführung
- Institut für Hochfrequenztechnik und Radarsysteme
- Institut für Kommunikation und Navigation
- Institut für den Schutz Maritimer Infrastrukturen

Laufzeit: 2019–2021

Budget: ca. sieben Millionen Euro

Vor allem die Satellitennavigation ist anfällig gegen Stör- und Täuschangriffe von außen. Im Fall von satellitenbasierten Landeanflugsystemen kann das folgenschwer sein. DLR-Fachleute arbeiten an Verfahren, um diese robuster zu machen. Nächstes Jahr soll die Technologie an Bord der DLR-Flotte getestet werden.

Bei Landeanflügen werden sensible Daten vom Flughafen an die Flugzeuge übertragen. Das Kommunikationssystem LDACS des DLR schützt gegen die Verfälschung solcher Daten und kann im Fall einer Störung der Satellitensignale die Flugzeuge sicher ans Ziel bringen.

Schutz von Systemen

Kritische Infrastrukturen wie Offshore-Windanlagen, Verkehrsleitzentralen, Schiffe und Häfen müssen besonders vor Cyberangriffen geschützt werden, denn unsere Gesellschaft ist darauf angewiesen, dass sie reibungslos funktionieren. Innerhalb des Projekts erarbeiten die Fachleute Bewertungskriterien, mit denen die Bedrohungs- sowie die Sicherheitslage eingeschätzt werden können, und entwerfen entsprechende Schutzmaßnahmen. Darunter fallen Maßnahmen, die sicherstellen, dass das Zusammenspiel der verschiedenen Systeme störungsfrei läuft – wie die Kommunikation zwischen Schiff und Hafen – aber auch Assistenz- und Beratungssysteme, die auf Angriffe hinweisen.

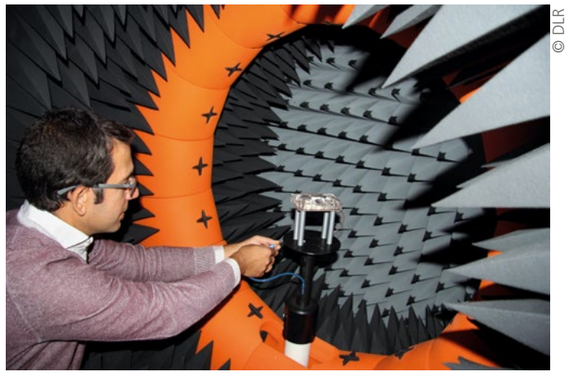
Digitalisierte Häfen oder Flughäfen beinhalten zahlreiche Schnittstellen. Sie sind mögliche Einfallstore für Hackerangriffe und bedürfen deshalb zuverlässiger Schutzmaßnahmen. Da sich der Cyberraum stetig wandelt, sollten auch die Sicherheitsanforderungen an die Systeme immer wieder angepasst werden. Innerhalb des Querschnittsprojekts baute ein DLR-Team ein exemplarisches, ganzheitliches Sicherheitsmanagement auf und überprüfte es in einem speziellen Labor, das genauso aufgebaut ist wie ein Fluglotsen-Tower.

Alle Arbeit wird gebündelt

Die Arbeiten zum Schutz von Informationen, Signalen und Systemen liefen im Querschnittsprojekt schließlich in einem gemeinsam entwickelten Landesystem sowie einer dynamischen Karte zusammen. Durch die verschiedenen Kompetenzen der Institute wurde die Sicherheit der Systeme von allen Perspektiven geprüft und entsprechend in das neue Design integriert.

Ein sicheres Landeanflugsystem für Flugzeuge

Damit Flugzeuge in Zukunft sicher autonom beziehungsweise unterstützt landen können, arbeiten die Forscherinnen und Forscher im Querschnittsprojekt an einem abgesicherten Landeanflugsystem. Besonders satellitenbasierte Systeme, wie das Ground Based Augmentation System (GBAS), das auch im DLR entwickelt wurde, sind anfällig für Cyberangriffe. Das DLR-Team konzipierte ein kryptografisches Verfahren, das robust ist gegen die Angriffe von Quantencomputern, und integrierte es sowohl in das GBAS-System als auch in das digitale Protokoll, das das Flugzeug mit der Bodenstation austauscht. Darüber hinaus härteten die Fachleute die Satellitennavigationsempfänger des Flugzeugs gegen Jamming und Spoofing ab. Aktuell bereitet das Team Messflüge für 2021 vor, in denen die Technologien getestet werden.



© DLR

Dr. Stefano Caizzone aus dem DLR-Institut für Kommunikation und Navigation in Oberpfaffenhofen testet die sogenannte 3+1 Antenne. Diese ist speziell für den Empfang von Satellitennavigationssignalen an Bord ziviler Flugzeuge gebaut und ist robust gegen Stör- wie auch Täuschsender.

Messungen an Bord eines Containerschiffs zeigten, dass Satellitensignale häufig an Häfen gestört werden. Diese Antenne kann Störsender anpeilen, aber auch ausblenden.

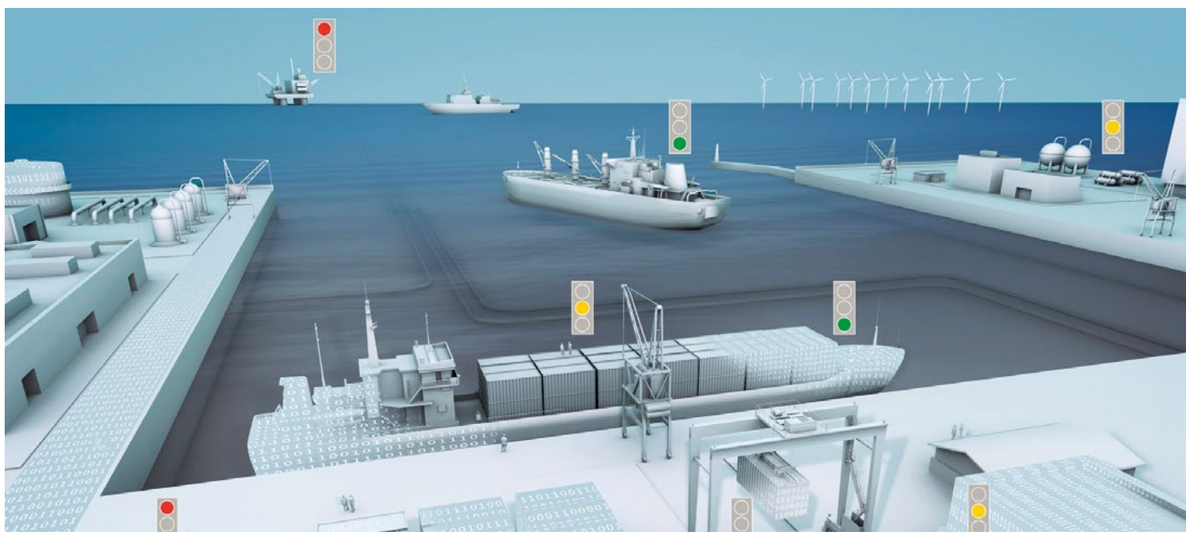
Eine dynamische Karte zeigt mögliche Gefahren

Neben dem sicheren Landeanflugsystem erstellten die Forscherinnen und Forscher eine dynamische Lagekarte mit einem integrierten Ampelsystem. Diese zeigt den Zustand aller Bestandteile einer Infrastruktur – wie ein Hafen oder ein Flughafen – in Echtzeit. Diese Lagekarte bezieht ihre Informationen aus den verschiedenen Bereichen des Querschnittsprojekts: Schifffahrt, Luftfahrt, Radaraufklärung. Grün bedeutet keine Gefahr, Gelb, dass die Infrastruktur kontrolliert werden muss, und Rot, dass diese Komponente gerade einem Angriff ausgesetzt ist. Mit diesem System können die Betroffenen schnell reagieren und die entsprechenden Gegenmaßnahmen einleiten, um weitere Infrastrukturelemente zu schützen. Eine entsprechende Karte wird bereits für den Hafen von Bremerhaven eingesetzt. Das Team arbeitet außerdem daran, eine solche Karte für Flughäfen zu entwerfen. Das abgesicherte Landeanflugsystem und die dynamische Karte sind schon vielversprechende Anfänge, damit falsche Funksprüche oder Geisterschiffe in Zukunft der Vergangenheit angehören.

Dr. Okuary Osechas arbeitet im DLR-Institut für Kommunikation und Navigation und koordiniert zusammen mit seinem Kollegen **Dr. Hannes Bartz** das Querschnittsprojekt Cybersicherheit.

QUANTENSCHLÜSSEL SICHER VERTEILEN

Moderne Kryptografiesysteme nutzen zufällig erzeugte Schlüssel, um die Informationen abzusichern. Dabei ist wichtig, dass der Schlüssel nur den beiden Kommunikationspartnern bekannt ist und nicht in die Hände von Spionen fällt. Die sogenannte Quantenschlüsselverteilung (engl. Quantum Key Distribution – QKD) sorgt dafür, dass die Schlüssel sicher verteilt werden, und verspricht dadurch Langzeitschutz gegen Cyberangriffe jeglicher Art. Das Team am DLR-Institut für Kommunikation und Navigation entwickelt zusammen mit nationalen und internationalen Partnern Systeme für satellitenbasierte Quantenschlüsselverteilung. Dabei werden die Quantenzustände über einen optischen Freistrahlkanal übertragen. Damit können große Distanzen überbrückt werden, wohingegen aktuelle faserbasierte Systeme auf wenige 100 Kilometer beschränkt sind. Satelliten können für die globale Quantenschlüsselverteilung eingesetzt werden. Die DLR-Fachleute arbeiten aktuell an einem störungsresistenten System, das für die weltweite Quantenkommunikation, insbesondere die Quantenschlüsselverteilung, eingesetzt werden kann.



Simulation einer interaktiven Karte, auf der ein Ampelsystem zeigt, inwiefern bestimmte maritime Systeme Risiken durch Cyberangriffe ausgesetzt sind