PROTECTED AREAS

DLR experts are conducting research into how autonomous and networked systems can be protected against cyberattacks

by Hannes Bartz and Okuary Osechas

Aircraft without pilots, control towers without air traffic controllers and interconnected ships: welcome to the age of networking. But each ground-breaking development also brings with it new threats. In July 2019, for instance, the navigation systems of several ships in the port of Shanghai were fooled into communicating the wrong coordinates and seemed to other ships to appear and disappear again in different locations, like ghosts. Cybersecurity threats also arise in very different areas. In a number of instances, unknown persons have been able to send unauthorised instructions to aircraft by radio. While the increasing automation of systems improves their reliability, their dependence on IT technologies leaves them vulnerable to cyberattacks. Dynamic developments invariably give rise to new weaknesses and threats. In the DLR cross-sectoral project 'Cybersecurity for Autonomous and Networked Systems', experts from four DLR institutes in the fields of security and aerospace are developing technology and methods for preventing such attacks.

What is cybersecurity?

In the modern world, vast quantities of data are constantly exchanged via global networks. This exchange of information is a clear target for unauthorised interference. Both worldwide networks and what are known as cyber-physical systems such as airports, in which different components interact and communicate with one another, are at risk. Cybersecurity is the set of active measures taken to protect such systems against malicious attacks. Particularly in aerospace, traditionally there has been a focus on safety more than security. Safety tends to refer to the protection of systems against random faults, while security usually refers to protection against deliberate tampering.

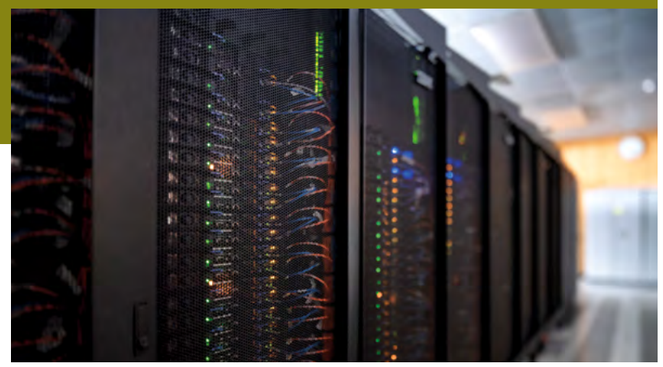
RADAR IMAGE OF OSLO HARBOUR

Radar images are used for many purposes. One example is the production of dynamic situation pictures for monitoring maritime infrastructures. For this, it is vital that the data used are reliable and trustworthy at all times. DLR's Microwaves and Radar Institute is researching methods for detecting and reducing interference in radar images.

Even though cyber threats are diverse in their approaches and their targeted systems and applications, they share a number of fundamental characteristics, such as the corruption of information or signals. Experts refer to 'jamming' or 'spoofing' if signals are disrupted or altered. A jammer intentionally disrupts a system for so long and with such severity that it can no longer function. Spoofing refers to the deliberate, targeted deception of an unsuspecting user. DLR researchers are developing techniques for reducing the impact of jamming and spoofing. These may include special encryption procedures to ensure that data cannot be manipulated, or processing techniques that allow for the rapid location of disrupters in radar images. To do this, the DLR teams have been analysing previous known attacks and developing appropriate countermeasures.

Protecting information

One current issue in the aviation sector is that communications remain largely analogue and unencrypted. As such, the system is vulnerable to malicious external interference. Air traffic management, which ensures safe, efficient air transport, is currently in the process of switching over from analogue to digital data transmission.



Computing cluster at the DLR Institute of Aerodynamics and Flow Technology

The new digital communication standards that allow aircraft to communicate with each other and with air traffic control must be secure. DLR has played a leading role in developing the L-band and C-band digital aeronautical communications systems (LDACS and CDACS) which can transmit data in real time and secure it against attacks and distortions by means of encryption.

Current encryption methods, such as those used for secure internet connections (HTTPS), will become ineffective in preventing attacks once quantum computers become a reality. Such computers are able to perform operations that would be extremely difficult for conventional computers and thus pose additional risks. Although only a few prototypes have been developed across the world so far, powerful quantum computers may become more widely available in the coming years.

The objective of post-quantum cryptography is to design new types of encryption methods that can enable systems to withstand attacks by quantum computers. As part of this cross-sectoral project, a DLR team is devising encryption methods that are suitably robust to these new challenges. Through such research, the communication systems used by aircraft and satellites are being made resistant to incidents such as unauthorised radio transmissions and secure from future threats.

Protecting signals

Aircraft are particularly vulnerable on their landing approach. Satellite-based approach systems are a window for both jammers and spoofers, posing security risks that cannot be eliminated using current technology. On a test flight in February 2020, DLR demonstrated how jammers could disrupt the onboard electronics of a commercial airliner, paralysing its entire satellite navigation system. Faced with such an attack, the pilot would have to continue flying by using legacy technology that is reliable, but less efficient. The DLR Institute of Communications and Navigation is developing antennas and satellite receivers that can help landing systems to withstand such attacks. The antennas recognise the direction from which a signal is coming – whether from above, as it would if it is coming from a satellite as it should, or below, if it is instead being emitted by a spoofer on the ground – and asses its credibility. This technique minimises the effect of jamming and spoofing and prevents ships from showing up in the wrong locations.

In the last five years, Synthetic Aperture Radar (SAR) systems have become more widespread. SAR belongs to the class of imaging radars and is used for remote sensing. However, both the unintentional and intentional disruption of SAR sensor systems is increasing. For some time now, the DLR Microwaves and Radar Institute has been investigating how such interference signals affect imaging and how the disruption that they cause might be eliminated. Researchers are developing methods that allow the original, unimpaired radar images to be reconstructed and evaluated without altering the sending or receiving devices. They are also designing future systems that are less prone to interference.

THE DLR CROSS-SECTORAL PROJECT CYBERSECURITY FOR AUTONOMOUS AND NETWORKED SYSTEMS

Institutes involved:

- Institute of Flight Guidance
- Microwaves and Radar Institute
- Institute of Communications and Navigation
- Institute for the Protection of Maritime Infrastructures

Duration: 2019–2021

Budget: approximately 7 million euros

Satellite navigation is vulnerable to interference and deceptive external attacks. This is particularly critical for satellite-based landing approach systems. DLR experts are working on procedures to make them more robust. Next year, the technology will be tested using the DLR research fleet.

During landing approaches, critical data are transmitted between the airport and the aircraft. DLR's LDACS communication system protects against the falsification of such data and, in the event of satellite signals being disrupted, can guide the aircraft safely to their destination.

Protecting systems

Critical infrastructure such as offshore wind farms, traffic control centres, ships and harbours require particularly robust protection against cyberattacks, as our society depends on their ability to function reliably. As part of the project, researchers are defining evaluation criteria to assess the security situation and its threats, and using them to devise appropriate protective measures. These include measures to ensure the continued reliable interactions between systems such as the communication between ship and harbour, and assistance and advisory systems to warn of attacks.

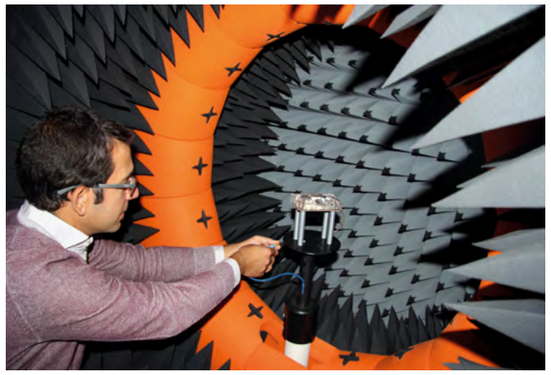
Digitalised harbours or airports comprise countless individual interfaces. This makes them particularly susceptible to attack and in need of specialised protection. As the landscape of the digital world is constantly changing, these security requirements must be continuously adapted. As part of the cross-sector project, a team from DLR is creating a demonstrative, comprehensive security management system and reviewing it in a special laboratory set up to represent an air traffic control tower.

Pooling expertise

The cross-sectoral project's work to protect information, signals and systems has now converged in a jointly developed landing approach system and a dynamic infrastructure mapping system. The broad range of expertise across the participating institutes is ensuring that the security of the new designs is evaluated from all perspectives and correctly implemented.

A secure landing approach system for aircraft

The jointly developed secure landing approach system will ensure the safe autonomous landing of future aircraft. Satellite-based systems such as the Ground-Based Augmentation System (GBAS) – developed in collaboration with DLR – are particularly vulnerable to cyberattacks. To remedy this, DLR has designed a data encryption process that is also robust against attacks by quantum computers and has integrated it into both the GBAS system and the digital protocols that aircraft exchange with ground stations. The experts also improved the resistance of the onboard satellite navigation receiver to jamming and spoofing. They are currently preparing for test flights in 2021.



© DLR

Stefano Caizzone from the DLR Institute of Communications and Navigation in Oberpfaffenhofen tests a '3+1 antenna'. This antenna is specially designed for receiving satellite navigation signals on board civil aircraft and is robust against both jamming and spoofing.

© DLR

Measurements made on board a container ship have revealed that satellite signals are particularly distorted at ports. This antenna can target an eliminate the effects of jamming transmitters.

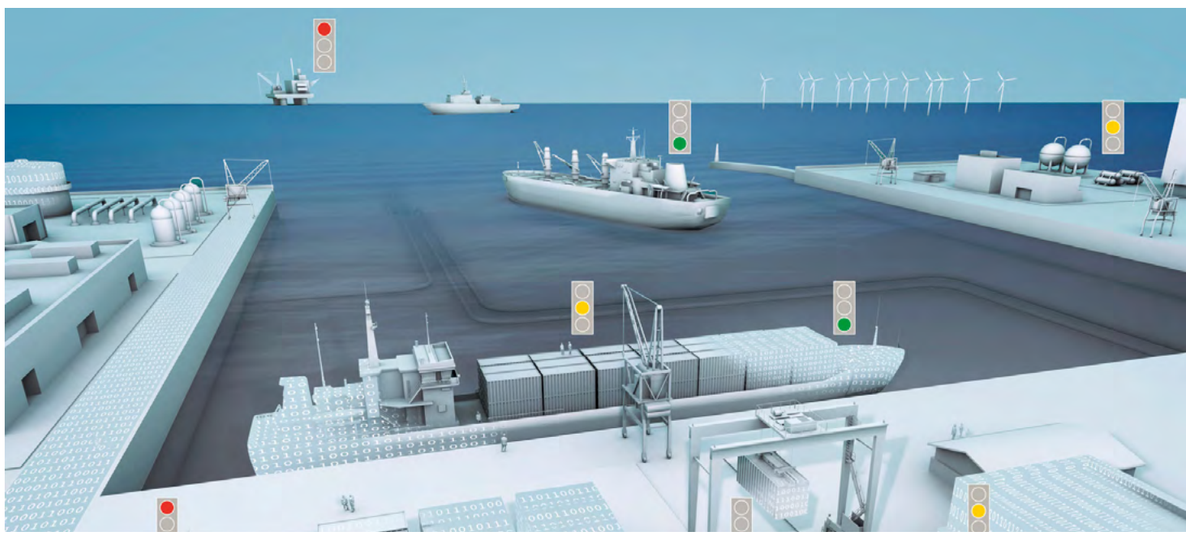
A dynamic map highlights potential hazards

In addition to the secure approach and landing system, the researchers developed a dynamic situation map with an integrated traffic light system. The map depicts the status of the entire infrastructure, such as a harbour or airport, in real time. It acquires its information from the different areas of expertise in the cross-sectoral project: shipping, aviation and radar reconnaissance. A green light means that a component in the system is in no danger, while yellow indicates that it is potentially vulnerable and needs to be inspected and red signifies that it is currently under attack. This system allows authorised personnel to respond quickly and initiate countermeasures to protect the infrastructure's other components. Bremerhaven harbour has already implemented such a map, and the team is currently working on creating a similar map for airports. In the ongoing bid to neutralise the threats of false radio transmissions and ghost ships, the secure landing approach system and dynamic map are promising beginnings.

Okuary Osechas works in the DLR Institute of Communications and Navigation and coordinates the DLR cross-sectoral project Cybersecurity for Autonomous and Networked Systems together with his colleague **Hannes Bartz.**

DISTRIBUTING QUANTUM KEYS SECURELY

Modern encryption systems use randomly generated keys to ensure the security of communications. Only users with the key can access the information, so it is vital that the key is known only to the two intended parties and does not fall into the hands of spies. Quantum key distribution ensures the secure distribution of these keys and guarantees long-term protection against any type of cyberattack. A team from the DLR Institute of Communications and Navigation is working with national and international partners to develop systems for satellite-based quantum key distribution. In this process, quantum states are transmitted via a free-space optical channel. While current fibre-based systems are limited to several hundred kilometres, this technology allows for transmission over large distances and thus makes satellites suitable for global quantum key distribution. Experts at DLR are working on a system that is robust enough for world- wide quantum communication, and quantum key distribution in particular.



Simulation of an interactive map with a traffic light system indicating the current risk of cyberattack for individual maritime systems