Cybersecurity of embedded computers systems

Jean Carlioz

AEGATS 2016
LES SALONS DE L'AVEYRON, PARIS, FRANCE / 12–14 APRIL 2016

Cybersecurity of embedded computers systems

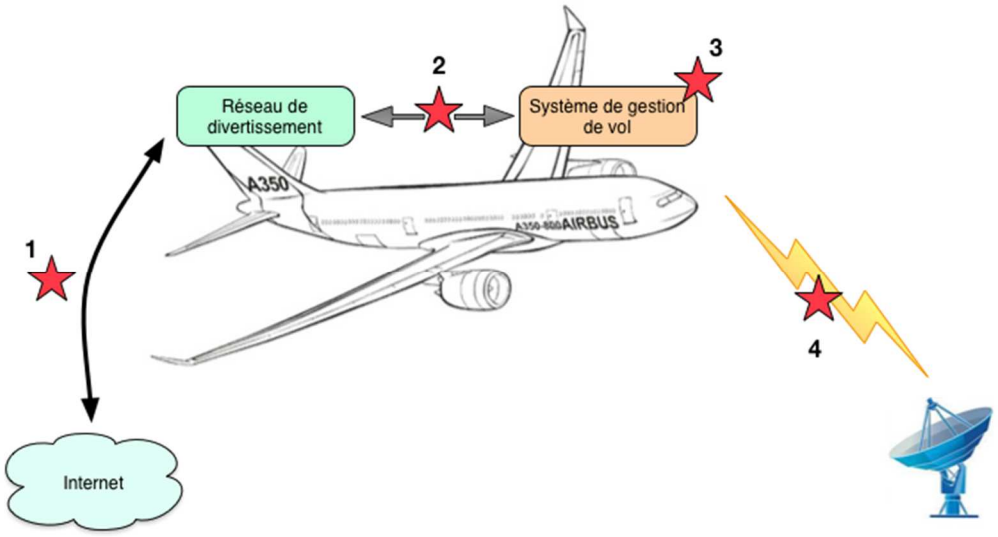
Jean Carlioz, DGAC
Directorate General, CISO
jean.carlioz@aviation-civile.gouv.fr

Several articles have recently raised the issue of computer security of commercial flights by evoking the "connected aircraft, hackers target" or "Wi-Fi on planes, an open door for hackers ? " Or "Can you hack the computer of an Airbus or a Boeing ?". The feared scenario consists in a takeover of operational aircraft software that intentionally cause an accident.

Moreover, several computer security experts have lately announced they had detected flaws in embedded systems, that exploited could lead to the aircraft's takeover by the "hacker".

This multiplication of alarming publications occurs in a context of proliferation of sophisticated computer attacks, targeting commercial enterprises to steal their sensitive information.

The world of aviation, if not offering the same exposure to the cyber threat as a public website, had however for some years its computer systems increasingly interconnected. Flight Management Computers "sealing" hitherto guaranteed by the autonomous nature of its trade (with the ground), now communicate with other systems. If this situation is not unique, it is natural that the growing number of interconnections leads observers to wonder about new vulnerabilities.



The attack points mentioned are schematically shown (red):
(1) Internet connection (2) interconnects the two aircraft systems,
(3) Flight system itself, (4) operatively connected with the ground

What is the threat?

A particularly competent "hacker" could target the "Flight Management System" (the aircraft computer system management) to disrupt the flight parameters. To succeed this attack, he should introduce a connection between the ground and the aircraft, for example by injecting a message containing false information deliberately erroneous and dangerous.

Press articles also cite a new danger: the companies now offer their passengers IT services and entertainment. These services are distributed on the plane by a network. The risk consists here on a malicious access to operational network if these two elements (entertainment and operational resources) are not separated. A passenger or a hacker from the Internet could potentially exploit this interconnection.

Likelihood of feared scenarios

If the terms of mentioned attacks are complex, some are possible. Thus, the interception and returning a

false message by ground-air liaison (*"4" in the diagram*) is technically feasible. Furthermore, injection, by this same bias, a dangerous operational message is technically described, but could not be successful, even in test patterns.

Furthermore, the scenario of an attack by a passenger who crossed the interconnexion between secure computer entertainment system and the operating system of the aircraft (*"3" in the diagram*) is serious. This interconnexion is technically a software gateway, so fallible. However, manufacturers are working to strengthen the security in order to make such an impossible scenario. But today there is no "zero risk" as long as these security measures are not deployed.

Some of the scenarios mentioned in the press are technically feasible, with significant resources, and growing interconnections of the systems make them potentially plausible.

Impact on flight safety

If the press interest in the topic of cyber threat is new, security experts have already repeatedly had to answer questions about the cyber vulnerabilities of avionics systems.

The drivers, such as controllers, are equipped and trained for their collaboration quickly detects deviation of the aircraft systems. In addition, these systems have the capacity to automatically detect such drift. If the attack occurred, and managed to "FMS" causing its drift, the pilot would immediately disengage it and follow the manual procedure. The conventional navigation means would remain available to the driver.

However, further analysis of the consequences of such an attack, that simultaneously affects multiple aircraft on approach, remains to be achieve.

Recent work by securing devices in response to the cyber threat

Manufacturers are actively working to maintain a very high level of security in their planes. For example, A380 & A350 are subject to a rigorous process that incorporates new scenario of "cyber-risk" in the update chain. In addition, a battery of audits - surrounded by precautions to ensure confidentiality - was conducted on the systems of these devices, concluding that a maximum level in the scale of protection. Those new process will retroactively be applied to older planes.

While recalling that "there is no zero risk", state agencies estimate that the recent Airbus aircrafts are now the most secure embedded complex systems in civil field.

Honeywell, producing the "FMS" (see annex), the operating system many aircraft models, integrated the attack scenarios to consolidate its product, since 2013. The product has not changed since the tests, Honeywell believes that FMS is not today more exposed.

Conclusion

Given the increasing interconnection of systems, some of the scenarios mentioned in the press would be technically possible, with significant resources.

However, even with a computer system failure, a crew is trained to keep control of the flight, according to procedures also known to air traffic controllers, navigation by conventional means.

In any case, the failure of one system alone would not impact flight safety. The air transport safety based on multiple redundancies, many backup devices and robust procedures with degraded modes which operators are well trained.

Nonetheless industrialists such as navigation services will integrate this new risk, working to limit impacts.

Annex

The components of the information "airplane" system

ADS-B

Modern aircraft, thanks to satellite positioning systems (such as GPS) know their position so much more accurate than ground control (radars having limited accuracy). The ADS-B system exploits this ability: the aircraft calculates its own position and regularly broadcasts by radio. Most modern aircraft are equipped with ADS-B (A 320-330-340-380, B-737-747-777, ...).

The ACARS

The ACARS is a digital data exchange system between an aircraft and the ground, supported by a ground network. It is used for the transmission of standard information from the floor (departure clearance, weather information, track changes, ...) or from the aircraft (technical condition, time of arrival).

The ACARS is based on radio transmissions, direct or via satellite. The "soil" network distributes the message between the radio station that received and the recipient. Thus, every company equipped with ACARS can communicate with its aircraft, anywhere in the world.

FMS

The "Flight Management System" is an embedded system that supports the strategic management of the flight (flight plan, loading ...) and its tactical management (position, embedded sensors, the crew orders). It consists of two computers (disengageable) that control the autopilot and provide information to the crew, flight parameters (Pilot Flight Director), navigation (Navigation Display), status of systems (Electronic Centralized Aircraft Monitoring), settings engines or alerts.

Only the ACARS system can address data from the ground to FMS.