CYBER SECURITY THREATS ON HELICOPTERS

Marie-Chantal Mouret

Airbus Helicopters (France)

marie-chantal.mouret@airbus.com

Abstract

Different types of events testify to the growing importance of the security field in aeronautics. Airbus Group itself considers that securing its products is one of its top priorities and some helicopters customers include cyber security threat resilience in their expression of needs. The core objective of Product Security is the insurance of the safety of flight while considering the intentional threats. Beyond the airworthiness certification perspective the security risk management aims at maintaining the mission reliability of the aircraft within its untrustworthy environment as well as at protecting the company branding. A specific process is set up in order to ensure security risk management for certification and continued airworthiness: it is based on a top-down approach based on security risk analysis which ensures the comprehensiveness of the protection in the face of all possible existing threats and the effectiveness of the selected measures to prevent undesired impacts. Specific security architecture principles and rules aim at providing adequate and optimized security design within the helicopter information system. Nevertheless the most efficient solution patterns to secure our helicopters are still under investigation as diverse criteria are to be satisfied.

What brings us to tackle cyber security threats on our helicopters?

Different types of events testify the growing importance of security in the transport field and its relevance to the helicopter as an aeronautical component.

Of course the awareness of security concern in aeronautics became very high after the physical security attack on 9/11.

But recent attempts at cyber security on commercial aviation and on cars show the increasing interest of hackers in transport means. Here are some examples:

- Flights have been cancelled as hackers have attacked the ground computers issuing flight plans (2015).

- Hackers have taken control of a Jeep car steering through its cellular communications (2015).
- Others have broken the connected Mitsubishi Outlander hybrid.
- Attempts to show an aircraft can be hijacked (ex.: Hugo Teso in 2013) were carried out. However it turned out to be not feasible.

Certification authorities highlighted risks on sensitive industries such as Aeronautics and Defense (2013). Their demands in helicopter resilience to security threats are becoming higher and higher.

In parallel the helicopter is expanding its connectivity with the open world thus making its own environment more vulnerable: the helicopter's operator wants to use wireless means for various operational uses cases on ground and in flight which implies data exchanges between untrustworthy open world and safety critical systems.

This set of factors makes cyber security a mandatory discipline on helicopters.

What do we manage the helicopter security risk for?

The core drivers of helicopter security are the maintaining of safety of flight, the insurance of operational reliability and the upholding of image of the company and customers.

The most important purpose is the insurance of the safety of flight while considering security threats. The safety process makes sure the failures and design errors do not jeopardize the safety of flight. The security process manages the risk on safety of flight coming from intentional / deliberate attacks.

In addition to the safety impacts the security risk management aims at maintain the mission reliability of the aircraft within its untrustworthy environment. In the event of security attacks the aircraft has to remain safe but also operable in both mission and maintenance phases.

These objectives are set within the scope of the helicopter itself but also regarding its support and manufacturing infrastructures.

Which process is to be set to properly manage the risk at helicopter level?

The top-down approach based on security risk analysis ensures the comprehensiveness of the protection in the face of all possible occurring threats and the effectiveness of the selected measures to prevent undesired impacts. It also contributes to minimizing overall security modifications before or after Type Certificate in case of environment or architecture evolution.

The first paragraph presents the security process related to helicopter risk management during development, operation and maintenance phases. The management of manufacturing process is not addressed in this paper.

Then the following paragraphs detail every core activity of this process.

Overall security process

In order to define, implement and validate the adequate helicopter assets protection against malicious attacks, the main activities presented in figure 2 in Appendix 1 have to be performed.

First the helicopter program directorate defines the top level security requirements applicable for this helicopter.

Then two inputs are defined:

- The environment, indicating which surrounding elements interacting with the helicopter may be sources of attacks and thus must be considered as untrustworthy.
- The functional impacts, which will be cascaded on the helicopter assets supporting the function.

At this stage, one knows where the attacks can come from and which functions deserve to be protected against these attacks.

So it is necessary to identify every potential threat scenario and then to combine attacks potentialities and impacts on helicopter assets. This is performed within the helicopter security risks assessment and it evaluates the level of associated risk. When the risks are not acceptable with regards to the security need they have to be reduced thanks to appropriate security objectives.

Then the activities of security architecture definition and validation convert these security objectives into security requirements which are allocated to specific items of the architecture. This is performed while ensuring security architecture rules are satisfied.

At this stage the development on board units implementing security barriers starts. It provides the equipment vulnerability assessment and verification reports on the security requirements.

This allows updating the helicopter security risk assessment by inserting the results of unit vulnerability analysis and it imposes to perform - if required - updates to the security architecture: this is necessary when security measures are not as effective as expected.

So the risk assessment and the architecture were preliminary ones, based on assumptions on security measures effectiveness and quality. Then after security equipment development they become substantiated and consolidated.This is performed only once the equipment security requirements have been verified and evaluated.

Helicopter security top level requirements

Helicopter security top level requirements are defined according to the targeted impacts types in the frame of the project. Safety impacts are to be addressed but beyond them, other impacts warrant coverage. Major stakes to protect against cyber aggression are the following:

- Product safety
- Product operational reliability
- Corporate image, and that of customers

Definition of the helicopter security environment

This step consists in characterizing the environment in which the helicopter operates in order to identify the sources of attacks.

The figure 1 in Appendix 1 shows the entities with which the helicopter components interact, either in development (ex.: suppliers), in operational mode (ex.: weather data provider) or in maintenance mode (ex.: Maintenance Repair Overhaul).

The helicopter information system environment is composed of the following elements definition:

- Entities in interaction with the helicopter (suppliers, passengers, Aeronautical Operational Control,..) and identification of potential threat sources.
- hackers profile,
- trustworthy/untrustworthy areas, systems and devices
- types of security attacks to be considered

Analysis of the functional impacts of security attack

The functional impact analysis identifies for all assets (functions, devices and data) the feared type of impact (corruption, loss, disclosure) and makes an assessment of the impact level (from minor to very strong).

Based on the definition of program objectives, all impacts on all valuable assets are categorized in a unique scale for all types of impacts (safety, operational reliability, image) from no impact to very strong.

Here are examples of impacts types:

- The corruption of the automatic pilot loaded software is a safety impact as it compromises the safety of flight.
- The loss of failures records is an operational impact as it causes delay on maintenance operation without affecting the safety of flight.
- The loss of In Flight Entertainment capabilities degrades the corporate image.

Helicopter security risk assessment

The security risk assessment is performed according to a specific method.

The purpose of the security risk assessment is to identify the set of security objectives that aim to reduce the risk to an acceptable level. Such security risks correspond to threat scenarios that have too high a likelihood for such associated security impact. In order to ensure the comprehensiveness of the security objectives, all possible threat scenarios have to be identified: this requires considering and combining **all possible** threat origins and causes (malicious code, remote command,…) on all assets, which may lead to several hundreds of scenarios. Adequate methods and tools contribute to manage the complexity associated to this huge amount of scenarios.

Example of a scenario: the attacker sends a remote command to an authorized tablet which generates a flooding on the helicopter Wi-Fi interface thus causing a loss of the wireless export function.

A preliminary helicopter security risk assessment is performed at the beginning of development and provides the definition of security objectives.Then after development of the elementary security measures which satisfy the objectives the helicopter security assessment is updated to reflect the verified security measures effectiveness and quality: if a security measure – once implemented – doesn’t provide the full expected security protection then the level of risk is reassessed for the threat scenarios this measure contributes to.

Security architecture definition and validation

The security architect is in charge of defining an optimized architecture capable of mitigating unacceptable security risks.

For such a purpose, it is necessary on one hand to identify all security objectives from security risks assessment and on the other hand to consider security architectures principles. Then, from the list of security objectives and the principles to follow, the security architect decides which set of security measures on which location in the architecture will satisfy the security objectives.

Example of a security objective coming from security risk assessment: the Wi-Fi communications between the helicopter and the ground are to be authenticated. Then from this security objective, the security architect performs the allocation of the objective to the relevant items: he decides which on board unit will perform the authentication and which ground items are allowed to authenticate themselves. And he selects the authentication mechanism. This allows precisely defining the security requirements for this authentication applicable to the selected onboard unit and ground devices.

Every security measure is defined, allocated to the right unit and characterized in details to make sure it provides the expected security effectiveness. In addition, security assurance level is attributed in order to ensure the adequate development design assurance in accordance with the associated impact level of the attack against which the protection covers.

Security measures development

Once security requirements are allocated to various helicopter systems components the associated security measures are developed according to design assurance which is specific to the security process.

The main point is the demonstration that the security measures are not bypassable and cannot be tampered with: this is ensured through vulnerability analysis and verification activities including tests that are specific to the security field. The point of these penetration tests procedures is to play the role of potential hackers by trying to bypass the security protections and cause an undesired impact.

Security risk assessment

After security measures development and implementation the following activities are performed in order to assess the remaining security risk:

- The security risk assessment is updated when necessary with the results of security vulnerability analyses performed at equipment level as the former security risk assessment was based on assumptions on potential vulnerabilities.
- The security architecture description is updated when necessary i.e. when the security measures don’t have the expected effectiveness.
- Security penetration tests are performed at system level to complete equipment level verifications tests.

Security procedures definition

This activity provides definition of the instructions or recommendations to be followed by operators to maintain overall helicopter security in operation, including maintenance. These procedures are of the following types:

- a complement to security technical measures. Example: if the integrity of uploaded software is not checked onboard then the maintenance operator has to perform this check on its ground data loader through a specific procedure.

- an association with security technical measures.Example: the VPN (Virtual Private Network) technical measure needs the customer to manage appropriate keys through specific procedures..

From certification till end of helicopter operational life

Management of new vulnerabilities:

This activity ensures that the helicopter information system security risk remains managed after certification during helicopter life cycle and while new vulnerabilities may be discovered. This requires performing specific monitoring of new vulnerabilities applicable to the helicopter and if the risk of potential threat scenario exploiting the vulnerability is not low then adequate protection means have to be put in place.

Which security architecture can ensure adequate and optimized design?

The core security architecture principles are the following ones:

- Border security, so that it's not necessary to implement security on every asset to be protected
- Defense in depth, so that the loss of one barrier doesn't cause any severe safety or operational damage.

Border security:

As a core driver of the security architecture is to optimize the overall design by minimizing the resources necessary for security protection, it is recommended to choose the strategy of the border security.

This means that main security measures are not implemented on all assets to be protected (ex.: safety critical units in avionics) but only on the entry points of the attack paths to the valuable assets. All assets behind this protected entry points belong to a same security domain, therefore don't require specific security protection between them.

This allows to significantly limit the amount of items on which security measures have to be implemented.

In addition to this security architecture rule it is also recommended to rationalize the number of borders, that is the number of entry points to the helicopter. For example it is advised to minimize the number of connectivity items so that associated security measures are minimized as well. This rationalization may be driven by security and is to be integrated in the general avionics architecture.

Defense in depth:

In the security risk assessment the security risks to be mitigated are identified and security objectives are set.

An adequate protection is required, which means a protection which decreases the attack likelihood level to a low level (so that residual risk is acceptable). In addition some defense in depth capability is expected through resources that are independent from the first layer of protection. This maintains protection in case of main defense failure or bypass. The maintaining of the helicopter in a secure state whereas a vulnerability is discovered at some point in time on one security layer also allows to take the necessary time to fix the problem without impacting the customer operations on the helicopter. The quality of the defense in depth has to be selected in accordance with the impact level associated to the threat scenario. It is recommended that the independence of layers be supported through physical segregation rather than logical one.

On top of these 2 fundamental principles additional security architecture rules are recommended:

- The units in the avionics domain have to have interfaces with inputs robust to any incoming data, for additional defense in depth approach.
- Authentication of devices for wireless communications in order to reduce surface of attack to the authorized devices.
- Minimization of period of time during which wireless media are on in operational mode.
- Fallback to secure state within every security barrier in case of abnormal event. The secure state may cause the loss of some connectivity functions but corresponds to a situation where the system operates again in a controlled configuration.
- Growth potential in computing performances to support the need of upgrade of security measures (cryptographic algorithms, size of keys) which has a high frequency compared to the cycle of the avionics computers.

What are the core issues to be handled in the management of cyber security on helicopters?

The helicopter security solution is expected to bring the appropriate protections to manage all security risks.

This overall objective is expected to be reached in accordance with various types of parameters:

- The security solution has to be affordable for the customer in all helicopter life phases:
  - Acquisition
  - Operation (including operational and maintenance activities).
- The security solution has to be as seamless as possible for the customer.
- The security solution has to support the threat evolution cycle that is short while the helicopter life cycle is much longer.

These factors drive the solution selections by imposing to tackle diverse questions such as:

- What is the right balance between onboard segment security protections and ground segment ones?
- Which architecture structure accommodates the most protections upgrades?
- Which design assurance activities provide the best value for effort?

Conclusion

One can see that designing helicopters capable of mitigating security attacks is a prerequisite for certification and integrating security while maintaining competitiveness and customer's easiness of operation is one of our key challenges. Providing our customers with secure platforms they can operate in a long term perspective in a security environment that moves very fast is a mandatory objective.

This imposes to consider security a core driver of the helicopter design and to integrate it from the earliest stage of its development. This also forces to deal with heterogeneous criteria all together to keep security in the helicopter manageable in terms of acquisition cost, operational constraints and sustainability.

Appendix 1 - Figures:

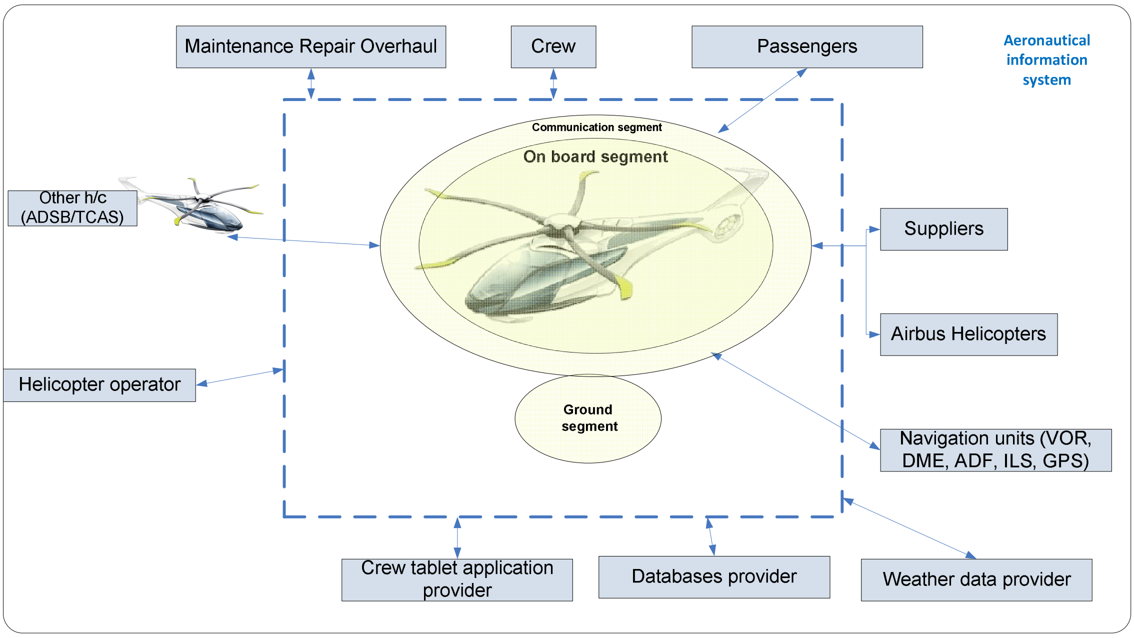

Figure 1 – Helicopter environment

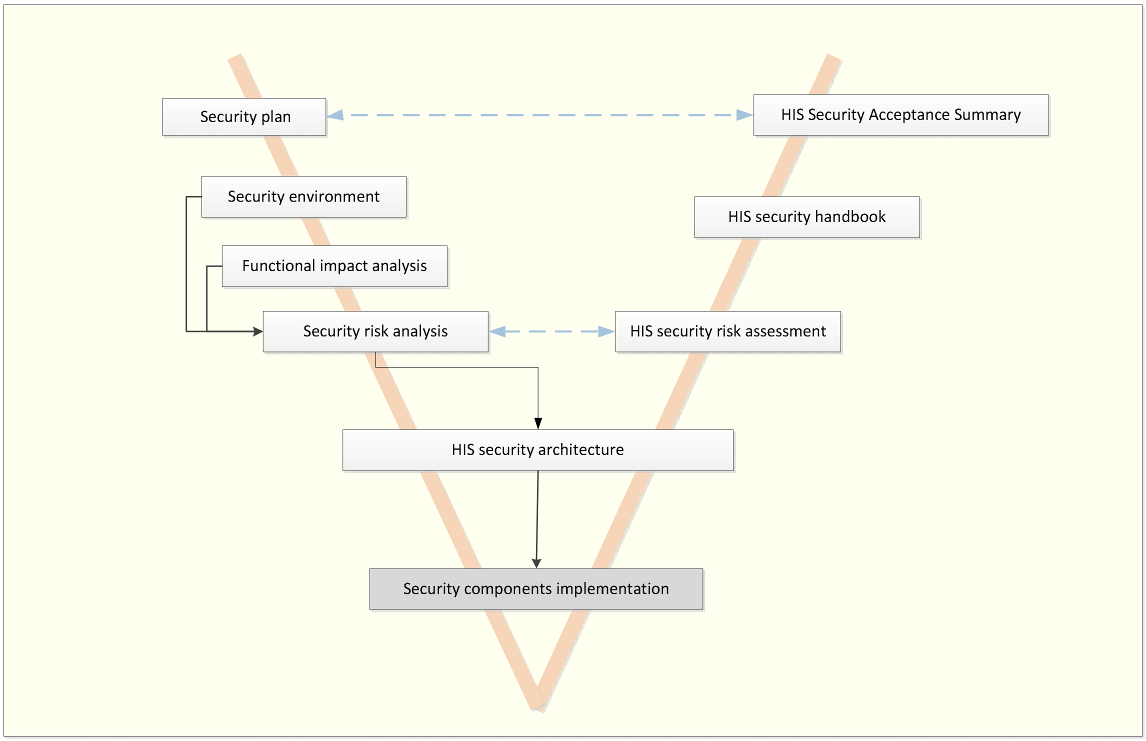
Security plan
HIS Security Acceptance Summary
Security environment
HIS security handbook
Functional impact analysis
Security risk analysis
HIS security risk assessment
HIS security architecture
Security components implementation

Figure 2: Security development process