Contact: Yoann Viaouet

Position Paper of the ASD Civil Aviation Cybersecurity Taskforce

April 2017

Content

Executive Summary 2
The need for a global cybersecurity framework: the role of ICAO 3
The need for balanced policy developments: the role of Europe 4
Rulemaking and standards-making: the need for a quick, collaborative effort 4
Information sharing 5
Research 5
Education / Training 5
Proposed Top objectives for operators and manufacturers: 6

About ASD

The AeroSpace and Defence Industries Association of Europe represents the aeronautics, space, defence and security industries in Europe in all matters of common interest with the objective of promoting and supporting the competitive development of the sector. Its membership comprises major European aerospace and defence companies as well as national associations.

Executive Summary

Civil aviation is the safest transport mode in the world, and probably also the most interconnected system of information and communication technology. Cyber-attacks are increasing in quantity and in quality and the consequences of a successful malicious cyber-attack on civil aviation operations could be severe. Points of attack span the entire industry chain and include the design, manufacturing, operation and maintenance processes of any aviation product. New technologies, extension of connectivity, use of Commercial Off The Shelf (COTS) solutions and their ever-quicker integration in the aviation industry, for example in the field of Air Traffic Management (ATM), increase the risk and impact of threats to these critical assets, whilst attackers become more numerous, adaptive and far-reaching.

Maintaining the high levels of security in civil aviation therefore urgently requires that an effective comprehensive framework addressing all aspects of the aviation system be developed. All actors should work based on a collaborative, risk-based model through a strong framework to address direct threats and at the same time increase the system's resilience against future attacks.

ASD has identified the following needs and priorities to mitigate the civil aviation cybersecurity threat:

- An end-to-end holistic vision, which describes and monitors roles and responsibilities of all stakeholders, is the only way to create a seamless cyber security risk response plan and to avoid gaps, overlaps, duplication of qualification/certification efforts or interoperability issues;

- ICAO should coordinate and aggressively pursue a comprehensive cybersecurity, cyber-safety and cyber-resilience work plan through a new dedicated group with all relevant stakeholders;

- ICAO States should develop guidelines for managing these current and future cyber-threats and vulnerabilities, and continuously update those through a comprehensive Air Transport Cybersecurity Management System;

- EASA should urgently establish the European Centre for Cyber Security in Aviation (ECCSA), announced in the EASA Cybersecurity roadmap in 2015, to ramp-up its capability to manage a major pan-European cyber crisis.

- The need for international alignment makes it necessary that civil aviation cybersecurity is positioned as a high priority on the EU diplomatic agenda: unbalanced regulatory developments from different regions of the world must clearly be avoided;

- It is not necessary to prescribe any technical solutions but rather mandate the stakeholders to demonstrate compliance with appropriate security objectives;

- A clear view of what standards are needed and what minimum expectations are placed on these standards is key: the same security requirements should be introduced into the Certification Specifications of EASA and the corresponding sections of regulations in other countries;

- There should be a 'ring fenced' budget for civil aviation cyber security research for both cost efficiency and effective implementation to improve the safe operation of the civil aviation transport system;

- EU should put an additional focus on the education of the young generations of experts, scientists and engineers who will take care of the cybersecurity of the next generation of aviation systems.

Introduction

The civil aviation system plays a crucial role in the EU economy and is known to be more and more exposed to fast evolving cyber-security threats that affect critically both safety and business continuity. In this context, the European Manufacturing Industry believes that it is now urgent to design and implement a defence system encompassing proactive, preventive, detective and reactive cybersecurity measures, to enable civil aviation to continue operations, thrive and remain competitive on the global market.

So far, many initiatives to develop and implement cybersecurity risk response strategies and pursue strategic plans for normative, regulatory, technological and procedural changes have been engaged but on a "local" basis, which miss the needed overall end-to-end and systemic vision.

Collaborative work between Authorities, Institutions, Academia, Manufacturers and Operators is needed to understand the challenges and opportunities facing the industry and coordinate the development and implementation of the ongoing and future international, European and national civil aviation cybersecurity strategies and policies. An end-to-end holistic vision, which describes and monitors roles and responsibilities of all stakeholders, is the only way to create a seamless cyber security risk response plan and to avoid gaps, overlaps, duplication of qualification/certification efforts or interoperability issues.

Moreover, constraints of the design, implementation and operation of the security measures along with the operational feedbacks and encountered security incidents shall be discussed between all the relevant stakeholders to avoid the silo effects and ensure that the solutions offered by the manufacturing industry are valued by customers, accepted by citizens and will be enforced by appropriate authorities.

Lastly, the same strong approach that fosters aviation's safety culture (clear goals, common understanding, risk-based decision making model, non-punitive reporting structures) must be applied as much as possible to securing cyber systems across Civil Aviation.

The need for a global cybersecurity framework: the role of ICAO

A better clarity is needed in the allocation of roles and responsibilities as regards cybersecurity, and the International Civil Aviation Organisation (ICAO), the UN aviation agency, has a leading role to play in delivering this leadership in collaboration with all relevant stakeholders.

The European aviation manufacturing Industry would like ICAO to create a group to work with and across most of the existing ICAO committees and the ICAO States. A top-level body is necessary to cover all aspects of civil aviation security, be it information systems, procedures and processes, or information network security architecture and the related physical security.

For this purpose, the International Coordinating Council of Aerospace Industries Association (ICCAIA) called upon ICAO to set up such as group during the 39th ICAO Assembly, in its working paper 236: "Coordinating Security Work". It was proposed that this group should lead, coordinate and aggressively pursue a comprehensive cybersecurity, cyber-safety and cyber-resilience work plan and governance structure with all relevant stakeholders. In addition to these tasks, the group should understand and provide visibility on the extent to which the activities of the various initiatives could contribute to the achievement of the global cyber security strategy, and identify inconsistencies between these initiatives and the strategy being developed.

Additional efforts should also be made to increase global awareness of cyber-threats and vulnerabilities in aviation, and ICAO States should collectively develop guidelines for managing these current and future cyber-threats and vulnerabilities. The continuous improvement of the Industry's cyber security posture could be ensured through a comprehensive Air Transport Cybersecurity Management System.

The need for balanced policy developments: the role of Europe

ASD members believe that it is crucial for regulators to recognise that a local response to a global threat is insufficient and that a concerted effort from all is necessary to address this issue. This means that unbalanced developments from different regions of the world must be avoided, so as to preserve stakeholders' capability to converge on a common regulatory basis and ensure international alignment.

As no region of the world should impose its vision over the others, the European aviation manufacturing industry believes that it is necessary to position civil aviation cybersecurity as a high priority on the EU diplomatic agenda. The European Commission (DG MOVE) as well as the European External Action Service (EEAS), in charge of the cybersecurity dialogue on behalf of the European Union, should ensure that European interests and specificities are considered and promoted on a global level.

It is proposed to agree with the US on the objectives and on the implementation means so as to ensure commonality between US, EU and other National Aviation Authorities to avoid duplicating design qualification/certification efforts. To this extent, ASD believes that EASA need to continue and sustain its involvement in the international Civil Aviation cybersecurity scene, for example in the US Advisory and Rulemaking Advisory Committee (ARAC) meetings: this also calls for EASA to be sufficiently equipped to deal with cybersecurity, starting with the much needed set-up of a collaboration platform.

EASA has made a first step in approaching the FAA to combine forces and set common regulations. The European aviation industry hopes that this proposal is accepted and that a hand is extended from these major authorities to the other national authorities of countries with significant aviation bases such as Canada and Brazil.

Rulemaking and standards-making: the need for a quick, collaborative effort

Through rulemaking, the European Commission and especially EASA are key enablers in establishing a clear view of what standards are needed and what minimum expectations are placed on these standards. This will allow the industry to satisfy these requirements through the development of industry standards with the support of standardisation bodies. Stakeholders should be required to demonstrate compliance with appropriate security objectives, instead of being prescribed technical solutions that would require numerous updates as technology is quickly evolving.

In the spirit of the international cooperation discussed above, the same security requirements should be introduced into the Certification Specifications of EASA and the corresponding sections of regulations in other countries. The Acceptable Means of Compliance and equivalent Advisory Circulars should be similarly harmonised to allow solutions to be used internationally.

As cybersecurity is a relatively new, yet critical subject, it is also preferable to introduce the most crucial rules as soon as possible rather than releasing a complete package at a later stage. In order to establish a first iteration of regulation with appropriate guidance, EASA – with its international partners – should indicate the priority of the topics and the target dates for each. This would help steer the industry committees in providing the relevant standards to phase in security into aviation with maximum effect, and to resolve potential differences in approaches to standardisation.

Additionally, industry would like a commitment that EASA will continue to contribute its expertise to standard-making activities to optimise the process by early communication of minimum expectations such that standards can be considered acceptable as AMCs when released.

Information sharing

Industry would like states to collaborate with other national cyber security organisations and anti-terrorist organisations to facilitate the efficient communication of cyber security threat information and enable these to be addressed in a coordinated manner, especially during crisis. Information sharing policies must be encouraged by ICAO and by the EU, especially regarding the threats and incidents, and there should also be a focus on harmonising cybersecurity events reporting schemes: various CERTs (Computer Emergency Response Teams) are being created around the world and convergence is needed (e.g. European Commission's NIS directive versus EASA initiatives).

In the EASA Cybersecurity Roadmap, one of enablers is the EU Centre for Cybersecurity in Aviation (ECCSA), which provides the risk landscape in partnership with Industry and EU Institutions and in collaboration with the CERT-EU. A solid legal framework, starting with the timely adoption of the new EASA basic regulation, will enable a reinforced cooperation between Member States, European Community, EASA and Operators to achieve efficient sharing of information and intelligence on existing or imminent threats: this shows the importance of involving all European Institutions in this debate.

Research

Civil aviation cybersecurity research and development activities are currently fragmented across national and EU funding sources. Different advisory bodies also exist, such as the new EU cyberPPP European Cyber Security Organisation (ECSO) for the overall cybersecurity issues, or the ACARE Strategic Research & Innovation Agenda for aviation issues. These different perspectives must be coherent and complementary: this is the reason why civil aviation cybersecurity must be fully integrated in the EU Research agenda in order to increase efforts to develop technologies and competencies at European level.

A more coordinated research and development work programme needs to be implemented with short-term flexible research activities to react to the ever changing "threat" evolution and more long term critical infrastructure activities. The Air Transport domain is critical by nature, and the EU research agenda should fully acknowledge civil aviation cybersecurity research as a key priority, and address it effectively. This EU commitment should serve for development activities to improve the safe operation of the civil aviation transport system, whilst research and development activities for business continuity could remain within the existing funding instruments. As part of this strategic vision and master plan, EASA needs to be involved to ensure there is a good link between science, innovation development, deployment and policy.

Education / Training

Europe should put an additional focus on the education of the young generations of scientists, engineers and entrepreneurs who will take care of the security of the next generation of aviation systems. For example, the need for aviation product security experts, which are very different from IT Security experts, is rapidly increasing and might be the source of dramatic disruptions in the near future.

European Authorities should facilitate and support the ramp-up of future human resources to populate, for example, the aviation CERT, in addition to the recruiting and training efforts already carried out by industry.

Proposed Top objectives for operators and manufacturers:

At the core of the approach described in this paper shall be the principle of continuous improvement of the Industry's cyber security posture through a comprehensive Cyber Security Management System. As an example and to illustrate concrete proposals by the Industry, top high level cybersecurity objectives have been identified:

- Identify critical assets (systems, operations, business…etc.);
- Define roles, responsibilities and processes regarding cybersecurity risk management;
- Define administration and maintenance policies of cyber protections;
- Deploy training programs and awareness sessions;
- Protect Network and Information Systems;
- Regularly assess residual risks through audits of operational procedures,, penetration testing and code reviews;
- Ensure COTS vulnerabilities management and mitigation;
- Deploy cybersecurity monitoring capabilities and cyber incident management;
- Prepare cybersecurity crisis management and short term recovery;
- Secure External networks and remote sites connection;
- Maintain a cartography of systems and networks;
- Secure software deliveries and supply chain (e.g. through the use of digital signature);
- Establish risk-based development processes for software & hardware.

These cybersecurity objectives are recognized as best practices and should allow the aviation industry to raise its level of resilience against cyber-attacks, if they are applied across all stakeholders.

****

Signed by Jan Pie, ASD Secretary General, on 21 April 2017