Council of the
European Union

Brussels, 11 September 2018
(OR. en)

11842/1/18
REV 1

AVIATION 108

'I/A' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee (Part 2)/Council
No. Cion doc.:	WK 9879/2018
Subject:	ICAO - Coordination for the 13th Air Navigation Conference (9 - 19 October, Montréal) – Endorsement

1. In preparation for the EU coordination activities for the 13th ICAO Air Navigation Conference (hereinafter 'ANC') (9-19 October 2018), the Commission services have submitted a second batch of 5 ~~European~~ Working Papers and 4 Information Papers. The following papers have already been endorsed by the ECAC Directors General for Civil Aviation:

   - WP Implementing search and rescue (SAR) processes
   - IP Considerations about Cybersecurity in Aviation
   - IP Emissions from supersonic aeroplanes
   - Joint WP System-of-systems notion of cybersecurity in aviation
   - Joint WP Challenges with the implementation of the concept of acceptable level of safety performance (AloSP)

In addition, the other papers of this batch are co-sponsored by the EU, but they have been shared with the ECAC/EU Ad-hoc European Coordination Group **and the ECAC Directors General for Civil Aviation** for coordination, and full transparency has been ensured. These papers are:

- Joint WP on Aviation Safety Implementation Assistance Partnership (ASIAP)
- Joint WP on strengthening regional safety oversight organizations (RSOOs)
- Joint IP regional safety oversight organizations (RSOOs): Examples of achievements and developments
- Joint IP on the third edition of the Nextgen-SESAR state of harmonisation report

2. On 7 September 2018, the Aviation Working Party examined all the above-mentioned papers. Delegations expressed their support for them and the actions recommended to the ANC.

3. In light of the above, COREPER is invited:

– to approve the text of the ~~Commission~~ Working Papers and Information Papers as set out in annex to this note and to endorse the actions recommended to the ANC contained in them;

– to forward them to the COUNCIL for approval in one of its upcoming sessions, so that the above-mentioned papers can be submitted to ICAO with a view to the upcoming Air Navigation Conference (Montréal, 9-19 October 2018).

International Civil Aviation Organization

INFORMATION PAPER

AN-Conf/13-WP/xxxx
../../18
(Information Paper)
English, Arabic, Chinese, French, Spanish and Russian only[1]

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE B

Agenda Item	6:	Organizational safety issues
	6.1	Strategic plan
	6.1.1:	Vision and overview of the Global Aviation Safety Plan (GASP), 2020-2022 edition
	6.1.2:	Enabling safety performance monitoring; goals, targets and indicators in the 2020-2022 edition of the GASP
	6.1.3:	Global Aviation Safety Oversight System (GASOS)
Agenda Item	6.2	Implementation of safety management
	6.2.1:	State safety programmes (SSPs)
	6.2.2:	Safety management systems
	6.2.3:	Developing safety intelligence
Agenda Item	6.3	Monitoring and oversight
	6.3.1:	The evolution of the Universal Safety Oversight Audit Programme (USOAP) continuous monitoring approach (CMA)
	6.3.2	Support and the USOAP CMA Online Framework (OLF)
Agenda Item	7:	Operational safety risks
	7.1:	Facilitation of data-driven decision-making in support of safety intelligence to support safety risk management
	7.2:	Operational safety risks at the global, regional and national levels, and the role of RSOOs and RASGs in achieving the GASP goals
	7.3:	Other implementation issues
Agenda Item	8:	Emerging safety issues
	8.1:	Measures to proactively address emerging issues;
	8.2:	Emerging safety issues

[1] Language versions provided by State/Organization

REGIONAL SAFETY OVERSIGHT ORGANIZATIONS (RSOOs):
Examples of achievements and developments

Presented by Interstate Aviation Committee (IAC), on behalf of AAMAC, ACSA, ACSAC, ASSA-AC, BAGASOO, CASSOA, CASSOS, the European Union (EU)[2], ECCAA, IAC, iSASO, PASO and SRVSOP

EXECUTIVE SUMMARY

This paper complements and supports the working paper "Strengthening Regional Safety Oversight Organizations" by providing examples of developments and achievements of some RSOOs.

1. INTRODUCTION

1.1 Today about 17 initiatives of regional cooperation are launched or in preparation, including institutionalised RSOOs, ICAO led-projects and Cooperative Inspectorate Scheme. 13 RSOOs are functioning already covering more than 130 states around the world. They are acting in different legal, economical and procedural frameworks but are sharing the common objective to strengthen the safety oversight performance of their Member States. The following provides 6 examples of RSOO achievements and on-going developments.

2. DISCUSSION

2.1.1 IAC

The Interstate Aviation Committee (IAC), known also as MAK, was founded in 1991 by 12 newly independent states of the former Soviet Union. Being the oldest organisation of such a kind, combining the RSOO and RAIO functionalities the IAC proved to be an effective instrument in the flight safety assurance system in the region. Today the IAC is acting within the frame of agreements with 78 states and 19 international organisations (including ICAO, EASA, IATA, and etc.). The sphere of competences of the IAC delegated by States of the Agreement on Civil aviation and airspace use in 1991 covered the certification of aircraft, systems, engines, aerodromes and equipment, development of the common legislation, standards and guidance material, developments in the area of the ATC systems harmonisation, aviation medicine, aviation security, staff training, investigation of air accidents.

Within the past 25 years the more than 150 aircraft and engines types, and more than 102 aerodromes have been certified by the IAC. More than 800 air accidents have been investigated. The IAC created the system of aviation rules AR harmonised with the FAA and EASA systems. Within the ICAO-MAK project (ICAO/IAC Project RER/01/901), being one of the most stable and effective one since 2001, a batch of the template legislation and guidance material, model Aviation Code, 14 sets of OPS rules templates have been designed and more than 9500 specialists participated at training courses, contributing to State's abilities to comply with the ICAO SARPs significantly.

[2] In the ICAO framework, EASA (the European Aviation Safety Agency) may act as a Regional Safety Oversight Organisation and is a member of the RSOO Cooperative Platform.

2.1.2 ACSA

ACSA was created as a regional Central American integration organization within COCESNA's framework (ACSA-ICCAE & ACNA) to advise and assist the Central American States in aviation safety and security matters since 2000. ACSA has been continuously improving itself and assisting the States in improving their ICAO Effective Implementation (EI) in the Central American Region. As a result, the current average of EI for the Central America Region is 85.56%.

ACSA has formally developed and established a Regional Rulemaking Process intended to attain the harmonization and standardization of Regulations, and training programs for the safety inspectors of the region. In this regard, ACSA has developed a total of 23 regulations, 20 of them are written in Spanish and English and 9 of them have been approved for regional implementation. As a result, a project for a regional license Regulation and implementation process is currently ongoing. In terms of Guidance Material for the different areas, the process of revision of these documents has just started this year and is expected to be completed by the first quarter of 2019. At the moment, we have a total of 11 Joint Implementation Procedures in English and Spanish.

The Agency is actively participating in the issuance process of AOCs for air operators in the region, including the operational approval for RVSM, AWO, PBN, as well as OCs for airports, training and approved maintenance organizations. Similarly, surveillance activities requested by the Member States are within our scope. As part of our products, the Agency has also developed and provided an important IT web tool for the States of the Region named Regional Data Management Aviation System (SIAR, for its acronym in Spanish) to improve the State's information, database, processes and aeronautical registry. Some of the different modules included in this system are:

- the licensing module for aeronautical technical personnel;
- the test module for theoretical examination of all applicants for licenses and ratings;
- the activities module to carry out the certification processes;
- the oversight module to be used by inspectors for scheduling, completion of checklists, oversight reporting and follow up;
- the module for the aircraft registration, which has been serving the Civil Aviation Authorities and their staff for over 15 years to comply with the certification and oversight obligations.

Finally, through COCESNA, ACSA offers over 80 aviation courses in all the different aeronautical fields.

2.1.3 ACSAC (COSCAP-UEMOA)

The "Agence Communautaire de supervision de la sécurité et de la sûreté de l'aviation civile des Etats membres de l'UEMOA" (ACSAC) was created on October 24, 2013 by an additional Act of the Presidents of the WAEMU Member States, in the normal evolution of the COSCAP-UEMOA Project set up in 2003 and whose activities have started in 2005, following the signing of a Memorandum of Understanding between the UEMOA Commission and ICAO. The primary objective of ACSAC is to promote the development of safe and efficient civil aviation that contributes to the establishment and maintenance of a uniform and high level of safety and security and to promote the protection of the environment in the Member States.

Pending the operationalization of ACSAC, the COSCAP-UEMOA project is a transitional body that performs missions assigned to ACSAC on behalf of Member States. The COSCAP-UEMOA project has developed some technical regulations in the PEL, OPS, AIR and AGA domains, with associated guidance documents. A common law on civil aviation adopted in 2013 forms the basis of these regulations.

Thanks to the technical activities of the COSCAP-UEMOA Member States, the average level of effective implementation (EI) has increased from 46% in 2012 to 64% in 2017. Three (3) Member States have received the certificate of the President of the Council for exemplary commitments and progress in aviation safety in 2015 and 2016. Another State is nominated to receive the certificate of the President of the Council in 2018. Five (5) airports have received their aerodrome certificates. Certification activities for three (3) other aerodromes are underway. It is expected that ACSAC will begin operations effectively by January 2019; and the Agency is supposed to be financially autonomous after 2021.

2.1.4 EASA

The European Aviation Safety Agency (EASA) is a regulatory agency of the European Union. Founded in 2002, covering 32 states with more than 800 employees and the budget over 160 M. EUR, EASA is the largest organisation of such a kind nowadays. Its main tasks include the following;

- assisting the European Commission in the development of EU rules in the field of aviation safety, air navigation and environment 'hard law', and developing material to ensure their correct application 'soft law' (certification specifications, acceptable means of compliance, guidance material);
- certification of aeronautical products,
- issuing approvals to design, production, maintenance, training and air navigation services organisations as well as FSTD qualifications;
- issuing authorisations for third country operators;
- conducting inspections, verification of compliance with the EU safety rules by the authorities of the Member States and other investigations;
- safety management on the level of the EU through the European Plan for Aviation Safety;
- assisting Member States to carry out their tasks ascribed to them by the international conventions;
- cooperating with Member States on security matters related to civil aviation;
- other areas such as safety analysis, research, safety promotion and technical assistance to other RSOOs and Stares.

Among the core features of the EU safety system is the mutual, automatic recognition of all certificates and approvals issued either by EASA or the Member States and the clear division of competences between EASA and the MS in performing safety oversight tasks. In 2017 EASA was audited by ICAO under the USOAP-CMA and its rate of effective implementation is 97.46%. The new founding act of EASA, so-called 'Basic Regulation' which is expected to enter into force in 2018 will extend the remit of EASA to new fields including drones, ground handling implementation of the Single European Sky and certain aspects of aviation security.

2.1.5 SRVSOP

The Regional Cooperation System on Safety Oversight in Latin America (SRVSOP) originated as COSCAP-LAM in 1995 and has been operating as an RSOO since 2003, following the signing of a Memorandum of Understanding between the Latin American Civil Aviation Commission (LACAC) and ICAO. The main objective of the SRVSOP is to establish and operate a regional safety oversight system in the South American (SAM) Region with the required technical, logistical and administrative support.

The SRVSOP has developed 35 Regulations in OPS, AIR, PEL, ANS and AGA as part of the Latin American Regulations Project; 10 inspector's manuals, 30 Advisory Circulars and has a catalogue of 30 courses available for on demand-on site provision for its member States.

Based on a harmonized regulatory framework and its resulting standardization, key achievements include: Multinational recognition of approved maintenance organization, training center and medical center certificates; 82.73% Average Level of Effective Implementation; 4 member States awarded with the Council President Certificate for exemplary commitments and progress on aviation safety in the last 2 years; and a 15 year, 37 Million USD direct benefit for member States, as measured by the latest Cost/Benefit Study.

2.1.6 EAC-CASSOA

On 18th April 2007 EAC Council of Ministers approved the establishment of the East African Community Civil Aviation Safety and Security Oversight Agency (EAC-CASSOA) as an autonomous self-accounting institution of the EAC. CASSOA is mandated by EAC Partner States to assist them in their undertaking to make air transport services safe, efficient and profitable while adopting common policies for the development of civil air transport in the region. The Agency is established by two legal instruments, the Protocol Establishing CASSOA and the CASSOA Act. Since 15th March, 2010 CASSOA Headquarters is hosted by the Republic of Uganda having moved from the East African Community Headquarters in Arusha, through a Headquarter Agreement signed between CASSOA and Uganda. The EAC CASSOA Membership is determined by being a party to the EAC Treaty and acceding to the Protocol. Republics of Burundi, Kenya, Rwanda, South Sudan, United Republic of Tanzania, and Uganda are the current members of CASSOA having signed or acceded to the Protocol and Treaty.

The following are functions that CASSOA carries out for the EAC Partner States:

- Harmonising operating regulations to ensure that they meet international standards and recommended practices;
- Developing standardised procedures for licensing, approving, certificating and supervising civil aviation activities; and
- Providing guidance and assistance to Partner States including putting in place measures for resource sharing particularly for the technical personnel.

CASSOA Operations are enhanced by the great support received from Partner States.
CASSOA has successfully carried out the following activities:

- Development, Review and Amendment of Model EAC Primary Civil Aviation Act and Aircraft Accident and Incident Investigation Act;
- Development, Review and Amendment of Model EAC Civil Aviation Regulations Development, Review and Amendment of Technical Guidance Materials;
- Technical Assistance to the Partner States in preparation for ICAO Safety Audits and development of Corrective Action Plans;
- Pooling of resources such as sharing of Inspectors;
- Enhanced Capacity building through Inspector Training;
- Regional Road Map for implementation of State Safety Programmes;
- EAC Examinations System; and
- Stakeholders engagement through regular Regional Aviation Symposia.

The Agency has initiated a number of projects in the EAC region that include Centre for Aviation Medicine, ECCAIRS Installation and Implementation in Partner States and Automatic Validation of PEL.

3. CONCLUSION

3.1 The RSOO model has proved in multiple examples and after years of consistent development effort how it can provide added value, through its ability to provide effective support to States, to drive both harmonisation of aviation safety and increased safety oversight capabilities, while fostering resource sharing and cost savings.

— END —

International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/xxxx
../../18

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE B

Agenda Item 6.2 Implementation of safety management
6.2.1: State safety programmes (SSPs)

CHALLENGES WITH THE IMPLEMENTATION OF THE CONCEPT OF ACCEPTABLE LEVEL OF SAFETY PERFORMANCE

(Presented by Australia, , by Austria on behalf of the European Union[1] and its Member States[2], the other Member States of the European Civil Aviation Conference[3] and by EUROCONTROL, Brazil, Cameroon, Canada, Colombia, Dominican Republic, New Zealand, Saudi Arabia, Singapore, South Africa and International Federation of Air Traffic Controllers' Associations (IFATCA))

EXECUTIVE SUMMARY

Annex 19 requires States to establish the acceptable level of safety performance (ALoSP) to be achieved through their State Safety Programme. This paper presents the challenges faced by States in implementing ALoSP and calls for a review of the ALoSP concept.

Action: The Conference is invited to:

(a) Note the challenges faced by States in implementing ALoSP; and

(b) Request ICAO to review the ALoSP concept, taking into consideration the experience of States that have sought to implement ALoSP.

[1] In the European Union, State obligations are discharged to a large extent on the basis of EU law and as such States refer to EU legislation in their State safety programmes

[2] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[3] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Republic of Moldova, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Turkey and Ukraine.

1. INTRODUCTION

1.1 Standard 3.4.2.1 of Annex 19 requires States to establish the acceptable level of safety performance (ALoSP) to be achieved through their State Safety Programme (SSP).

1.2 ALoSP is defined[4] in the Safety Management Manual (SMM) as *"the minimum level of safety performance of civil aviation in a State, as defined in its State safety programme, or of a service provider, as defined in its safety management system, expressed in terms of safety performance targets and safety performance indicators."*. Annex 19 further describes how an ALoSP can be achieved in the note accompanying Standard 3.2.4.1: "An acceptable level of safety performance for the State can be achieved through the implementation and maintenance of the SSP as well as safety performance indicators and targets showing that safety is effectively managed and built on the foundation of implementation of existing safety-related SARPs."

2. DISCUSSION

2.1 The purpose of the ALoSP appears to be clear from the descriptions in Annex 19 and the SMM. After defining its safety objectives, safety performance indicators and the targets associated with these indicators, States should make a determination on the minimum overall level of safety performance that would be considered to be acceptable to the State. It should be noted that the ALoSP relates to the safety performance of the whole system, rather than of individual safety performance indicators. This is illustrated by the flowchart in Figure 1 below, which can be found in the advance unedited 4th Edition of the Safety Management Manual.

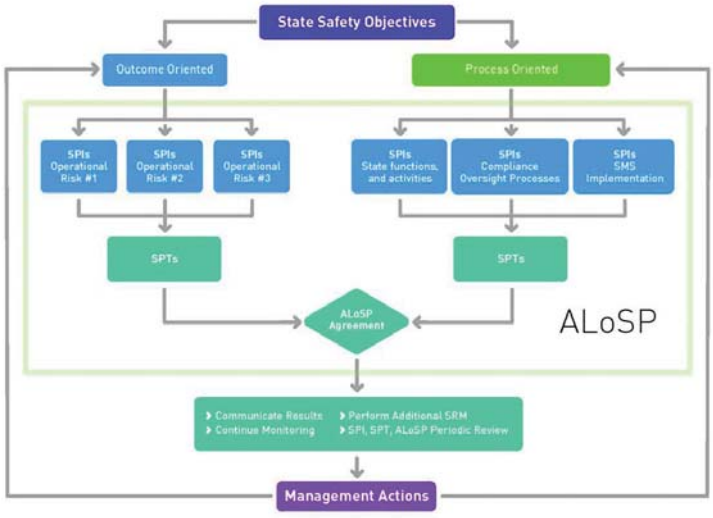


Figure 1 : Acceptable Level of Safety Performance

[4] In the advance unedited 4th Edition of the SMM, the term ALoSP is used only in relation only to States, and is defined as "*the level of safety performance agreed by State authorities to be achieved for the civil aviation system in a State, as defined in its State safety programme, expressed in terms of safety performance targets and safety performance indicators.*"

2.2 The States co-sponsoring this paper, among others, have found that while the purpose of the ALoSP may be clear, *how* it is to be implemented is not clear and may be challenging in practice.

2.3 The use of the word "acceptable" in the term "acceptable level of safety performance" suggests that there are two possible categories that aviation safety performance may fall into: acceptable safety performance (i.e., within the bounds of the ALoSP), or unacceptable safety performance (i.e., outside the bounds of the ALoSP). This would appear to require the State to develop criteria to determine whether the safety performance of the State, as a whole, is "acceptable" or "unacceptable".

2.4 Consider the ALoSP that encompasses the 6 safety performance indicators (SPIs) in Figure 1 above. While it may be possible to determine whether performance of a single indicator falls within or outside the 'acceptable' range (for example by assessing whether the target or trigger levels for that indicator were met or exceeded), it is significantly more difficult to assess whether the safety performance of a State as a whole has been 'acceptable'. How an ALoSP is to be expressed in terms of safety performance targets and safety performance indicators requires more clarification. For example, given that ALoSP is expressed in terms of targets and indicators, would the inability to meet the safety performance target for a single SPI be considered not meeting the ALoSP? How many SPIs would need to show unsatisfactory outcomes for the State to conclude that it does not meet its ALoSP? Should a smaller subset of more critical safety performance indicators be selected to represent the ALoSP? If so, should these SPIs be weighted and how does the State determine which areas carry a heavier or lesser weighting? Should the determination of whether the safety performance of the State has been acceptable take into consideration mitigating circumstances that may be outside of the control of the State?

2.5 The determination of what would constitute a level of safety performance that is acceptable can also be complicated by public expectations as well as the local cultural and political context. In order to develop a more straightforward criteria for an acceptable level of safety performance, some States may distill its safety performance into a single indicator and target of the highest consequence, expressed in terms of number of accidents or fatalities. States that have done so face non-safety complications, such as political sensitivity in having to express an 'acceptable' accident rate.

2.6 The States co-sponsoring this paper have taken different approaches to address this issue. Some have taken the approach of determining whether it has achieved an acceptable level of safety performance in more dynamic and subjective manner, by periodically considering the State's safety performance through a management review process. The review is informed by its suite of safety performance indicators, whether targets were met, whether trigger values were exceeded, and whether mitigating actions put in place were successful in arresting the safety concerns. The approach to determining its ALoSP is therefore described more as a process, rather than as a specific pre-defined desired outcome. While this approach addresses the issue of how the State manages its acceptable level of safety performance, the fundamental question remains unanswered: what is the State's acceptable level of safety performance?

2.7 It is clear from the challenges faced by States in meeting the Annex 19 Standard on ALoSP that there needs to be greater clarity on the concept of ALoSP, particularly in relation to how it should be implemented in practice. One consideration could be to avoid the use of the word 'acceptable' given its sensitivity. The experience of States that have embarked on their SSP implementation would be useful in the review of the ALoSP concept.

3. CONCLUSION

3.1 States that have embarked on their SSP implementation have encountered challenges with implementing the concept of ALoSP. While the purpose of ALoSP may be clear, the way to implement it

is not. With more States expected to implement SSP going forward, it is important to revisit and review the ALoSP concept, taking into consideration the experience of States that have sought to implement it.

3.2 In light of the above, the Conference is invited to agree to the following recommendations:

Recommendation 6.2.1/X Challenges with the Implementation of the Concept of Acceptable Level of Safety Performance

The Conference is invited to:

a) Note the challenges faced by States in implementing ALoSP; and

b) Request ICAO to review the ALoSP concept, taking into consideration the experience of States that have sought to implement ALoSP.

— END —

International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/xxxx
../../17
(Information Paper)
English

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 1: Air navigation global strategy
1.1: Vision and overview of the sixth edition of the GANP

THIRD EDITION OF THE NEXTGEN-SESAR STATE OF HARMONISATION REPORT

(Presented by the United States and the European Union)

SUMMARY

This paper provides an overview and informs the Conference of the publication of the 3rd Edition of the NextGen-SESAR State of Harmonisation Report in support of global ICAO and industry standardisation efforts. It invites to broaden this cooperation with other States and regional modernisation programmes as well as ICAO to consider support in further building on these collaborative efforts.

1. INTRODUCTION

1.1 The U.S. and Europe are modernising their ATM systems through the NextGen and SESAR programmes respectively that develop new capabilities introducing new enabling technologies and operational procedures. Specifically, these modernisation efforts are enabling a move from a ground-based ATM system, using radar and voice communications, to an integrated air-ground aviation and ATM system using satellite-based navigation and digital data communications. The goals on each side of the Atlantic are to improve overall aviation and ATM system performance, particularly in the areas of flight efficiency and the environment, while also meeting expected demands for increased capacity and continuing to maintain the highest levels of safety.

1.2 This third edition of the NextGen-SESAR State of Harmonisation document builds on the two earlier editions published in 2014 and 2016. It provides a summary of the current state of progress towards securing harmonisation and interoperability between the two modernisation programmes, and by incorporating deployment encompasses the full aviation and ATM modernisation lifecycle view. The

(2 pages)
3. AN-Conf13_COM A_FAA-EU WP_IP_SOHP_Consolidated final.docx

document serves as an outline for consideration of the current issues at stake and the challenges ahead. It demonstrates that differences are recognised and actions are taken to address them where necessary to ensure harmonisation and interoperability.

2. DISCUSSION

2.1 The NextGen-SESAR State of Harmonisation reports provides a high level summary of the current state of progress towards achieving the necessary level of harmonisation and global interoperability between NextGen and SESAR.

2.2 More broadly, the publication reflects the current and planned collaboration efforts by the U.S. and the EU to harmonise and secure the modernisation of ATM not just across the Atlantic but globally in support of the International Civil Aviation Organisation (ICAO) Global Air Navigation Plan (GANP) and its Aviation System Block Upgrade (ASBU) programme.

2.3 Both NextGen and SESAR recognise the need to safely integrate the air and ground components of their respective aviation and ATM systems. This requires greater predictability and efficiency in the planning and execution of flight trajectories and the seamless and timely sharing of accurate information. The U.S.-EU harmonisation work aims to ensure that modernisation in air navigation systems worldwide supports a high-performing aviation system over time, based on global cooperation leading to seamless operations and safe and efficient practices for the airspace users and the travelling public.

2.4 NextGen and SESAR have together made significant progress in several critical areas since the publication of the first edition of the State of Harmonisation in 2014 and second edition in 2016. This third edition provides an update on each of these areas and reflects the broadening scope of the Memorandum of Cooperation, the scope of which was expanded in December 2017 to include all aspects of the ATM modernisation lifecycle, from planning to development and deployment.

3. CONCLUSION

3.1 Ultimately, the collaboration between the U.S. and Europe is not just about achieving transatlantic interoperable standards but to support the broader goal of achieving global harmonisation and interoperability as articulated in the ICAO GANP and ASBUs.

3.2 For that reason, much of the collaboration work described in this document directly supports global ICAO and industry standardisation efforts and as such provides for our common interest to use available mechanisms to broadening this cooperation with other States and regional modernisation programmes of a similar nature.

3.3 Equally, we invite ICAO to consider their support in further building on these collaborative efforts by requesting them to develop consensus proposals on specific elements of the GANP/ASBU´s.

3.4 The U.S. and the E.U invite you to review the report at *www.faa.gov and www.sesarju.eu.*

— END —

International Civil Aviation Organization

AN-Conf/13-WP/..

WORKING PAPER

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 4: Implementing the global air navigation system and the role of planning and implementation regional groups PIRGS
4.4: Implementing search and rescue (SAR) processes and procedures

IMPLEMENTING SEARCH AND RESCUE (SAR) PROCESSES

(Presented by Austria on behalf of the European Union and its Member States[1] and the other Member States of the European Civil Aviation Conference[2] and by EUROCONTROL)

EXECUTIVE SUMMARY

This paper presents the last amendment of Annex 6 with implementation of new Standards in support of the Global Aeronautical Distress and Safety System (GADSS) and their consequences in terms of SAR effectiveness. It highlights that the new Standards if improving the situation for accidents over water, provide less accuracy than the previous automatic ELTs in case of an accident over terrain especially in mountainous areas. And urges for a review of Annex 6 so as to include a performance based Standard for adequate crash localisation capability to ensure a more accurate localization of the wreckage and survivors after an accident occurring over terrain.

Action: The Conference is invited to agree to the Recommendation 4.4/x: Search And Rescue (SAR) and the Global Aeronautical Distress and Safety System (GADSS) in paragraph 3.1.

1. INTRODUCTION

1.1 SAR processes are effective if the location of an accident site is determined with accuracy. The implementation of new Standards relating to the location of an aeroplane in distress in support of the Global Aeronautical Distress and Safety System (GADSS) will

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.
[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Moldova, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Turkey and Ukraine.

significantly improve the capability to search for and locate an aircraft after an accident occurring above water.

1.2 This new Standard has replaced the Standard for Automatic Emergency Locator Transmitter (ELT), which has been shown to be relatively ineffective in case of an aircraft accident into water. However, an automatic ELT remains a highly effective means to precisely locate survivors after an accident occurring over terrain, even when the new means to locate an aeroplane in distress which is still in-flight are activated. Annex 6, Part I should be amended with a performance based Standard to precisely locate survivors, which allows the same or better level of performance, reliability and interoperability than ELT during SAR operations.

2. DISCUSSION

2.1 Post Flight Localization in the GADSS Concept

2.1.1 One of the main components of the GADSS concept is Post Flight Localization. When an accident occurs, a phase immediately begins at the end of flight where the rescue of possible survivors has the immediate and highest priority. When technically feasible, and in particular when the aircraft is not in water, accurate aircraft position information allowing to determine accurately the point of end of flight was historically provided by means of the Post Flight Localization function of an ELT (including homing signal) to guide SAR services on site. To assist in the localization of survivors after an accident, the post flight localization function specified a number of requirements for ELTs included in previous ICAO Annex 6 provisions.

2.2 Amendment of Annex 6

2.2.1 Annex 6 was amended in 2016 with new Standards for Location of Aeroplane in Distress resulting from the GADSS concept. At the same time, the Standard for the installation of an Automatic ELT was downgraded to a Recommendation status. The new Standard for the location of an aeroplane in distress mandates the transmission of sufficient information to determine the position of the aeroplane once a minute when in-distress and still in-flight. Based on the results of the work of an International WG led by the BEA in the scope of the AF447 Rio-Paris safety investigation, this one-minute interval transmission may permit location of an aeroplane wreckage within 6 NM from the last reported position in 95% of the cases. This new Annex 6 Standard covers the issue raised by AF447 and MH370 but is less demanding than the previous Standard concerning ELTs to precisely locate survivors after an accident on ground. With such amendments, the Annex 6 Standard for Post Flight Localization, which required an automatic ELT no longer exists. The capability to locate the wreckage and survivors, with very high accuracy when the aircraft is not in water, is significantly diminished. The performance of SAR depends largely on the organization of SAR services and preparations undertaken before any SAR operations take place but the crucial issue is to accurately determine the location of the end point of the flight and allow efficient consecutive SAR operations

2.2.2 These Annex 6 amendments, with the removal of the automatic ELT Standard, were proposed by the Air Navigation Commission in 2015 in the aftermath of the MH370 disappearance, during the final review after a Letter to States. The focus was on developing new provisions to prevent cases such as the MH370 disappearance.

2.2.3 EASA submitted WP/12 to the last Flight Operations Panel (FLTOPSP/WG/5 at Montréal from 7 to 11 May 2018) with the same aim to amend Annex 6, Part I. It was also

considered by EASA that the means to locate an aeroplane in distress may improve the likelihood that an alert is transmitted (e.g. when the ELT antenna is destroyed during the accident). However, in the case of survivable accidents, its 6 NM accuracy is insufficient to ensure timely assistance to survivors whereas the Automatic ELT could provide a much more accurate location. Removing the carriage requirement for Automatic ELTs reduces the probability that occupants surviving a crash are rescued in a timely manner, unless another system on-board the aircraft offers adequate performance for search and rescue purposes.

2.3 Analysis of past events

2.3.1 It is often thought that ELTs do not work during a public transport accident sequence. It should be remembered that these ELTs were designed to allow SAR services to find the site of an accident with survivors. These ELTs do not work, as per design, in non-survivable high impact force accidents. Nevertheless, ELTs have proved their usefulness, as illustrated in the table below. In addition, ELT integral/internal antennas authorize the transmission of the 406 MHz signal and homing even if the cable to the external antenna is broken. This type of antenna has shown the robustness of the ELT on the MH17 event over Ukraine.

2.3.2 A list of accidents for which Accident Investigation Authorities issued a number of Safety Recommendations addressed to ICAO for the installation of automatic ELTs or for which ELT activation assisted in finding the accident site is provided herewith. The ELTs are designed to precisely locate survivors by combining satellite based localization and a ground homing capability. This capability could not be replaced by a system transmitting a signal once a minute while in-flight and providing a position within 6 NM. This 6 NM precision will not be satisfactory enough in mountainous areas.

Aircraft type	Registration	Operator	Location	Date	Fatal	Survivors	Information on accident and ELT activation
Airbus A320	F-GGED	Air Inter	Mont Saint Odile (France)	20/01 /1992	87	9	9 survivors found in mountains 4 hours after the crash. 6 lives could have been saved if rescue had been on site in 30 minutes (2 lives in 2 hours). Crash site located ~1 Km from last reported point. Search area was 21 km². No ELT installed.
Avro-146 RJ85	CP2933	LaMia	9 NM from Medellin airport (Colombia)	26/11 /2016	71	6	Fuel exhaustion, 10 NM from the airport. Heavy fog prevented air SAR. ELT detected and located.
Boeing 737-800	TC-JGE	Turkish Airlines	1.5 km from Schiphol airport (Netherland)	25/02 /2009	9	120	ELT detected and located.
Boeing 777-28EER	HL7742	Asiana Airlines	San Francisco airport (US)	06/07 /2013	3	214	ELT detected and located.
Boeing 777-2H6ER	9M-MRD	Malaysia Airlines	Over Ukraine	17/07 /2014	298		ELT detected and located. The ELT was triggered during the in-flight break-

							up sequence and on-ground later on thanks to the ELT internal antenna.

2.4 Increased survivability of ELTs and MEOSAR detection capabilities

2.4.1 Cospas-Sarsat is implementing a new MEOSAR (Medium Earth Orbit for SAR) system based on the use of search and rescue transponders on new GPS, GLONASS, and GALILEO satellites and accompanied by a new ground segment. This new MEOSAR system provides near-instantaneous detection of ELTs and significantly improves the timeliness and accuracy of alerts provided by ELTs. Improved specifications for new generation ELTs are currently being developed by the joint EUROCAE/RTCA WG (ED-62B/DO-204B). Thanks to NASA studies and trials, the specifications include increased survivability of ELTs during an impact sequence. The specifications permitted the development of new ELT(DT), compliant with the location of an aeroplane in distress Standards, with improved crash survivability, homing and integral/internal antenna. The EUROCAE WG has already published the specifications document for Criteria to Detect In-Flight Aircraft Distress Events to Trigger Transmission of Flight Information (ED-237). This document is already referenced by Annex 6 to start the in-distress sequence of the flight.

3. CONCLUSION AND RECOMMENDATION

The new Annex 6 Standard for the location of an aeroplane in distress covers the issue raised by AF447 and MH370 but provides a lower accuracy than the previous Standard on ELTs to precisely locate survivors after an accident occurring over terrain..

Annex 6 Part I should then be reviewed to include a performance based Standard for adequate crash localisation capability to ensure a more accurate localization of the wreckage and survivors after an accident occurring over terrain in support of effective and efficient SAR operations.

Recommendation 4.4: Search And Rescue (SAR) and the Global Aeronautical Distress and Safety System (GADSS)

a) That ICAO reviews aircraft equipment related Standards, in order to ensure that aeroplanes are equipped with robust and automatic means to accurately determine the location of the end of flight point for an effective SAR response following an accident over terrain.

— END —

International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/xxxx
xx/xx/18

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE B

Agenda Item 7: Operational safety risks
7.3: Other Implementation Issues

Aviation Safety Implementation Assistance Partnership (ASIAP)

Presented by the United Kingdom, on behalf of:

Canada, China, France, Japan, Korea (Republic of), Malaysia, Russian Federation, Singapore, South Africa, Togo, United States, the European Union (EU)[1], Airports Council International (ACI), African Civil Aviation Commission (AFCAC), Airbus, Boeing, Civil Air Navigation Services Organization (CANSO), , International Air Transport Association (IATA), World Bank

EXECUTIVE SUMMARY

One of ICAO's strategic objectives is to ensure a continuous improvement in global aviation safety in close collaboration with the aviation community. The rapid growth in air transport in recent years has resulted in ICAO needing to play a key role in achieving this objective. This paper presents information about the Aviation Safety Implementation Assistance Partnership (ASIAP) and calls on States to support this initiative which facilitates coordination and collaboration on technical assistance activities, in order to further advance aviation safety implementation assistance capacity in the aviation community.

Action: The Conference is invited to agree to Recommendations 7.3/x – Other Implementation Issues, in Paragraph 3.1.

Strategic Objectives:	This working paper relates to the Safety and Air Navigation Capacity and Efficiency Strategic Objectives.
Financial implications:	Impact for the aviation community: The continuous sharing of information and coordination on assistance projects planned by the Partners avoids duplication of efforts and maximizes the effectiveness and efficiency of assistance programmes provided by the Partners. This will benefit all stakeholders involved, as the Partners will be able to manage resources more sustainably and decrease the costs of the projects' delivery. There is also further need for voluntary contributions to supplement the ICAO programme budget for implementation of technical assistance projects.

[1] *The EU body involved in the work of ASIAP is the European Aviation Safety Agency (EASA).*

	Impact for ICAO (*relative to the current Regular Programme Budget resource levels*): Additional resources and budget are required particularly IT resources to further develop the Project Database and other electronic tools, as required.
References:	Assembly Resolution, A37-16, *The Safety Fund (SAFE)* Assembly Resolution A39-14, *Regional cooperation and assistance to resolve safety deficiencies, establishing priorities and setting measurable targets* Assembly Resolution A39-16, *Consolidated statement of ICAO policies on technical cooperation and technical assistance* Assembly Resolution A39-23, *No Country Left Behind (NCLB) Initiative* Assembly Resolution A39-26, *Resource Mobilization* Doc 10004, *2017-2019 Global Aviation Safety Plan*

1. INTRODUCTION

1.1 Recent rapid growth in air transport has resulted in the need for ICAO to play a key role in working with stakeholders in support of implementing their safety oversight obligations. The Aviation Safety Implementation Assistance Partnership (ASIAP) was established during ICAO's High-Level Safety Conference (HLSC) in February 2015 to complement the Global Aviation Safety Plan (GASP) and Universal Safety Oversight Audit Programme (USOAP). ASIAP's main priority is to promote coordination and cooperation amongst key stakeholders to further advance aviation safety implementation assistance capacity in the aviation community.

1.2 High importance is placed on continuous collaboration and partnership for safety assistance activities in order to facilitate global aviation safety objectives. In light of this, ASIAP is determined to achieve the following objectives: technical assistance and cooperation (information sharing, prioritisation of needs); resource mobilisation; collaboration and partnerships; coordinating efforts; encouraging States to prioritise aviation in national policies; and promoting further support to Regional Safety Oversight Organisations (RSOOs), as appropriate.

1.3 In line with the UN Sustainable Development Goals, ICAO has established mechanisms for technical cooperation facilitation such as No Country Left Behind (NCLB) initiative, Resource Mobilization, the Safety Fund (SAFE), and ICAO Programme for Aviation Volunteers (IPAV). ICAO continues to innovate in this area, with proposals such as the Civil Aviation Safety Inspector (CASI) database and the Global Aviation Safety Oversight System (GASOS), however for the established mechanisms, there remains a need for voluntary contributions to supplement the ICAO programme budget in this area. There is a significant gap between the demands for assistance and the resources available. In order to bridge that gap, it is important for States to engage at Governmental and Ministerial levels to raise the level of importance of aviation and to provide support to ASIAP and ICAO in order to implement effective technical assistance.

1.4 Despite the overall success of recent technical assistance projects and the on-going collaboration of stakeholders, ASIAP is still facing some challenges and improved coordination and prioritisation of activities is required.

2. DISCUSSION

Scope of ASIAP Activities

2.1 The main activities of ASIAP include: the continuous sharing of assistance information (reporting on ongoing Projects and Project Outcomes) and making this available on ICAO's website; the collaboration on particular assistance activities, and periodic coordination meetings to further share information and discuss priorities. ASIAP provides communication channels for discussion amongst

Partners to facilitate the provision of assistance to States, and at the same time strengthen the partnership to further increase its reach and effectiveness.

Functions

2.2 The objectives of ASIAP are achieved through the active participation of its Partners in the following activities, which are coordinated by ICAO:

- identifying priority States for the provision and coordination of assistance activities, including States with Significant Safety Concerns;
- expanding coordination and collaboration of assistance activities to include RSOOs;
- exchanging information and views on the improvement of, and collaboration on, assistance activities for States and Regional Organizations that have challenges in rectifying safety deficiencies;
- developing and promoting the use of performance indicators and metrics to ensure efficient and effective assistance implementation and optimal use of resources;
- developing a platform to increase the overall assistance effectiveness and transparency; and
- encouraging prioritizing aviation safety in State national policies, strategies and plans.

Ongoing Activities and Accomplishments

2.3 The ASIAP Prioritisation Tool (https://www.icao.int/safety/ASIAP/Pages/ASIAP-APP.aspx) has been developed to help identify States that should be prioritised for technical assistance. The Tool uses a methodology developed by ASIAP using real-time data sourced from the:

- ICAO Universal Safety Oversight Audit Programme (USOAP);
- Integrated Safety Trend Analysis and the Reporting System (iSTARS), including Safety Margins App; and
- World Bank Worldwide Governance Indicators (WGI).

2.4 An ASIAP Working Group on Technical Assistance/Cooperation (Project) Outcome Indicators (POIs) was established to develop a set of indicators to guide and determine the level of success of the assistance provided by ASIAP Partners. The aim is to use the POIs at the start and end of a project, and at any time in-between when considered appropriate to measure progress on the actions delivered. The initial indicators that have been proposed are SMART: specific to the objective it is supposed to measure, measurable (either quantitatively or qualitatively), available at an acceptable cost, relevant to the information needs of managers, and time-bound. The POIs will be used and shared on a voluntary basis. The results will include information available on the CMA-OLF, iSTARS and UN SDG and should be compared to the baseline result established at the beginning of the project. The European Aviation Safety Agency (EASA) has advised that they are applying the POIs for both their State and Regional Projects. ICAO has recently applied the POIs to completed projects.

2.5 A web-based Projects Database is being developed (address to be added) and the Partners have been asked to enter at least one project in the database. Going forward, it is anticipated that all relevant projects will be included in the database. To date, Canada, France, Singapore, South Africa, the United Kingdom, EASA and ICAO and have made submissions into the database. The Projects Database is an important tool to coordinate technical assistance activities in order to avoid further duplication of effort and overlap in activities.

3. CONCLUSION

3.1 In light of the foregoing, the Conference is invited to agree to the following recommendation:

Recommendation 7.3/x – Other Implementation Issues

That the Conference:

a) Acknowledge the importance of coordinating and collaborating on the development and implementation of technical assistance activities;

b) Acknowledge the work done by ASIAP and encourage ASIAP Partners to further develop cooperation;

c) Urge the Partners to strive for greater commitment to, and participation in, the ASIAP Programme, and invite other States and International Organisations that can provide technical assistance to States to join ASIAP;

d) Recommend that Partners and other stakeholders providing technical assistance (including States, RSOOs, International Organisations, industry and financial institutions), coordinate their technical assistance activities and make use of the online Project Database (update with website address) in order to reduce duplication of activities and effort;

e) Encourage the Partners to apply the POIs to their projects and review the measurable results in coordination with each other;

f) Urge the Partners, including ICAO, States, International Organisations, industry and financial institutions to provide funding to support technical assistance activities;

g) Request ICAO to continue to develop the Prioritisation of States and Areas of Technical Assistance criteria in order to achieve appropriate and transparent prioritisation.

— END —

International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/xxxx
../../18

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues
5.4: Cyber resilience

SYSTEM-OF-SYSTEMS NOTION OF CYBERSECURITY IN AVIATION

(Presented by Canada, by Austria on behalf of the European Union and its Member States[1], and the other Member States of the European Civil Aviation Conference[2], by EUROCONTROL and by Singapore. Co-sponsored by Australia and New Zealand)

EXECUTIVE SUMMARY

This paper will briefly introduce the concept of a system-of-systems, and establishes why such an approach would be suitable in the context of addressing cybersecurity considerations in civil aviation. This paper will also introduce the notion of security-by-design, and how the integration of this concept within the aviation system will improve its resilience.

Action:
The Conference is invited to agree to the recommendations in paragraph 3.

1. INTRODUCTION

1.1 The availability of accurate information and the correct functioning of safety-critical systems are pre-requisites for a safe and secure civil aviation system as the sector encounters further digitalization. The aviation system is highly integrated and information travels globally. Therefore, cybersecurity initiatives in the aviation sector must take a holistic and end-to-end approach.

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Republic of Moldova, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Turkey and Ukraine.

(4 pages)

1.2 A holistic, end-to-end approach can only be successful if aviation is understood as a "System-of-Systems", for which all members of the aviation community share responsibility. The aviation system is made up of a variety of networks and devices that are becoming increasingly connected and mutually dependent for the exchange of digital data and information, while aviation stakeholders such as States, aircraft and aerodrome operators, air navigation service providers (ANSPs) and others have come to rely on interconnected and interoperating information and communications technology (ICT) systems for their day-to-day operations.

1.3 Developments such as system-wide information management (SWIM), the introduction of remotely piloted aircraft systems (RPAS) and the emergence of future airspace users and stakeholders that are not yet operational further reinforce this interdependency. The aviation system of the future thus requires more concerted design and less individual evolution to maintain its resilience against cyber interference.

1.4 The evolution towards interconnected and interoperating information systems mentioned above also brings new vulnerabilities. Cyber-related events can impact aviation on many levels and can jeopardize the performance of the air navigation system and endanger the overall safety of the sector. These events can influence information exchanges between stakeholders, directly affecting safety, security, capacity and efficiency with potentially severe repercussions.

2. DISCUSSION

2.1 **Aviation as a system-of-systems (SoS)**– in the aviation sector, many stakeholders, both direct and indirect, play a role in the functioning and maintenance of individual sub-systems and the system as a whole – with the understanding that a system can be comprised of products, people and processes. Each of these sub-systems draw directly from other sub-systems in order for them to function smoothly and efficiently; conversely, each of these sub-systems also has a significant impact on the others when it is unable to function correctly.

2.2 These sub-systems today are designed, integrated, operated and managed independently of each other, and evolve at their individual paces, leading to an overall evolutionary process that is challenging to predict and pin down deterministically. Since aviation stakeholders have a total system responsibility for the overall product, the consideration of aviation as a SoS is all the more important. Responsibility for the functioning of the aviation system therefore includes both direct stakeholders, such as aircraft and aerodrome owners/operators and ANSPs, as well as indirect stakeholders, such as States and equipment manufacturers / designers.

2.3 Given that these sub-systems serve individual functions that are chained together to achieve common objectives (e.g. communications between air traffic control and pilots, or location tracking data between aircraft operation control centres and aircraft), compromising any of these sub-systems would adversely affect the overall functionality of the entire chain of sub-systems. As such, cybersecurity risk management will need to be addressed using a holistic approach in order to reduce the reachability of threat actors to core functionality.

2.4 **Cybersecurity: an ongoing, evolutionary consideration** - given the evolutionary nature of SoS described above, cybersecurity must similarly be an ongoing consideration among the many stakeholders in the aviation SoS. It is also imperative that the aviation SoS maintains its required cybersecurity conditions by means of sufficient flexibility and adaptability when its components permanently interact in a variety of manners with each other (e.g. aircraft interacting with different air navigation service providers as they transit through different Flight Information Regions).

2.5 Therefore, the development and maintenance of such cyber resilience across the SoS require continued coordination among all stakeholders (see paragraph 2.2), in order to maintain the desired flexibility and adaptability needed for the aviation SoS to function correctly.

2.6 An important challenge to address in pursuit of this objective is the concept of "composability" – the ability to integrate multiple elements (components for systems, or subsystems for SoS) into bigger entities securely. The key challenge here is the departure from the safety paradigm, in which the integration of elements focused primarily upon their functionality and interactions across common interfaces. From the cybersecurity perspective, the integration of individual elements also requires careful consideration of how cybersecurity postures of each element contributes to the overall cybersecurity state. A key question that will arise in this pursuit includes how to support States and regions (and other individual stakeholders) in their development journeys such that the SoS can be effectively protected from cybersecurity attacks, despite the inevitable variance that will exist between sub-systems.

2.7 In achieving the above goal, the integration of individual sub-systems will require careful consideration and integration of native security environments for each sub-system, to the extent that a holistic and cyber resilient environment emerges. Uncoordinated approaches to cybersecurity could either lead to undetected vulnerabilities in protection; overlaps in perceived system defences are just as dangerous, since that scenario would still potentially result in a viable attack surface for the aviation SoS.

2.8 Therefore, a globally coordinated approach to managing system interactions is essential, and core to that objective is a common view of how these systems and sub-systems interact.

2.9 **Integrating security-by-design for aviation systems** – in order for the aviation SoS to achieve its desired level of cyber resilience, it is important for cybersecurity considerations to be incorporated from the beginning of system development, as opposed to being considered retroactively. This would also allow for interfacing considerations between sub-systems to be taken into account, such that these interactions would also take place in a secure and efficient manner.

2.10 Most current security standards focus on mitigating measures taken and implemented *within* the organisational context – there is a pressing need to adjust the focus of such measures to include and account for measures that must be taken from the inter-organisational perspective as well. This allows for the assurance of overall SoS security, over and above security arising from an amalgamation of sub-systems which are individually secured.

2.11 Without appropriate management, uncoordinated cybersecurity approaches of aviation sub-systems can pose a risk to the system as a whole. This lack of coordination also potentially stems from insufficient communication between sub-system managers and other relevant stakeholders during the development and design of cybersecurity approaches.

2.12 Through multiple layers of coordination (e.g. between States as managers of domestic aviation systems, managers of sub-systems within domestic aviation systems, etc.) across different levels of sub-systems, as well as ensuring that individual sub-systems are effectively protected in their own right, States would be contributing to an aviation SoS that maintains defence-in-depth as a natural outcome of such work.

2.13 **Future work** – Such work in incorporating security-by-design as part of initial system design should not replace the best practices honed by the aviation community through many decades of experience in developing aviation systems and working on cybersecurity challenges. By incorporating such principles alongside and complementary to the traditional focus on system redundancy as well as the emphasis on maximising ease of access to operational data and systems, stakeholders will further strengthen the aviation SoS in its cyber resilience policies, while maintaining operational effectiveness.

2.14 As part of the variety of operational concepts and solutions being discussed at various aviation fora today, it is important for States and industry to take the above considerations into account through the development and design process. By extension, the community may also evolve its collective work to further identify representative sub-systems and research to which extent its results – based upon the measures taken and the practices used – can be transferred to other sub-systems to improve cyber resilience across the board.

2.15 Similarly, following success in this arena, the aviation community may consider working to initiate the further development of increasingly larger sub-systems, which take information security into consideration during their initial design phase. As such work progresses and matures, stakeholders may begin to collectively explore whether there exist suitable and trusted candidates to be tasked with responsibility in developing and maintaining such systems which are secure-by-design, and the feasibility of such processes in the aviation system of the future.

2.16 Through continued investment and dedication of efforts in the area of system cyber resilience, the aviation community will contribute effectively to the safe and efficient operation of the aviation ecosystem ("SoS") well into the future.

3. CONCLUSION

3.1 The Conference is invited to agree on the following recommendations:

That the Conference:

a) Urge ICAO and States to acknowledge that the cyber resilience of the aviation system depends on continued coordination among all relevant stakeholders.

b) Request ICAO to acknowledge the concept of SoS, requiring the necessity of collaboration and coordination among managers of sub-systems, in particular when developing, integrating, operating and maintaining subsystems that are "secure by design".

c) Urge ICAO to develop a framework that requires and guides States to implement measures to mitigate the cyber threat and risk to civil aviation systems. This may result in the development of SARPs for several affected ICAO Annexes.

d) Recognize the concepts contained in Information Paper: "*Considerations about Cybersecurity in Aviation*".

— END —

International Civil Aviation Organization

AN-Conf/13-WP/xxxx
../../18

WORKING PAPER

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE B

Agenda Item	**6:**	**Organizational safety issues**
	6.1	**Strategic plan**
	6.1.1:	**Vision and overview of the Global Aviation Safety Plan (GASP), 2020-2022 edition**
	6.1.2:	**Enabling safety performance monitoring; goals, targets and indicators in the 2020-2022 edition of the GASP**
	6.1.3:	**Global Aviation Safety Oversight System (GASOS)**
Agenda Item	**6.2**	**Implementation of safety management**
	6.2.1:	**State safety programmes (SSPs)**
	6.2.2:	**Safety management systems**
	6.2.3:	**Developing safety intelligence**
Agenda Item	**6.3**	**Monitoring and oversight**
	6.3.1:	**The evolution of the Universal Safety Oversight Audit Programme (USOAP) continuous monitoring approach (CMA)**
	6.3.2	**Support and the USOAP CMA Online Framework (OLF)**
Agenda Item	**7:**	**Operational safety risks**
	7.1:	**Facilitation of data-driven decision-making in support of safety intelligence to support safety risk management**
	7.2:	**Operational safety risks at the global, regional and national levels, and the role of RSOOs and RASGs in achieving the GASP goals**
	7.3:	**Other implementation issues**
Agenda Item	**8:**	**Emerging safety issues**
	8.1:	**Measures to proactively address emerging issues;**
	8.2:	**Emerging safety issues**

STRENGTHENING REGIONAL SAFETY OVERSIGHT ORGANIZATIONS (RSOOs)

Presented by Interstate Aviation Committee (IAC), on behalf of:

Autorités Africaines et Malagauche de l'Aviation Civil (AAMAC)
Agencia Centroamericana para la Seguridad Aeronáutica (ACSA),
Agence Communautaire de Supervision de la Sécurité et de la Sureté de l'Aviation Civile (ACSAC)
Agence de Supervision de la Sécurité Aérienne en Afrique Centrale (ASSA-AC)
Banjul Accord Group Aviation Safety Oversight Organization (BAGASOO)
East African Community Civil Aviation Safety and Security Agency (CASSOA)
Civil Aviation Safety and Security Oversight System (CASSOS)
The European Union (EU)[1],
Eastern Caribbean Civil Aviation Authority (ECCAA)
Interstate Aviation Committee (IAC),
Interim Southern African Development Community Aviation Safety Organization (iSASO),
Pacific Aviation Safety Office (PASO)
Regional Safety Oversight Cooperation System (SRVSOP)

EXECUTIVE SUMMARY

This paper discusses the current role of Regional Safety Oversight Organizations, the challenges they are facing and the need for both States and ICAO to continue supporting their strengthening by implementing the Global strategy and action plan for the improvement of RSOOs and the establishment of a global system for the provision of safety oversight, with the aim that RSOOs become an essential component of the future Global Aviation Safety Oversight System (GASOS).

1. INTRODUCTION, BACKGROUND

1.1 The traditional model of aviation safety oversight foresees that all safety oversight functions are performed directly by a State's Civil Aviation Authority (CAA). Today the implementation of a new paradigm for safety oversight has become essential, because of several factors, most of which are already influencing today's aviation system:

1.1.1 The world of aviation is undergoing rapid changes and becoming more complex, while air traffic is predicted to double within the next 15 years. It will require significant additional resources to ensure the aviation safety system remains stable;

1.1.2 The aircraft ownership, registration and user business models are changing, thereby affecting the safety oversight systems. They need to adapt to the future demands of a rapidly expanding aviation industry, of new technologies and new systems such as RPAS.

[1] In the ICAO framework, EASA (the European Aviation Safety Agency) may act as a Regional Safety Oversight Organisation and is a member of the RSOO Cooperative Platform.

1.1.3 Different regulatory systems, overlapping auditing and re-certification programmes require a rethink of current safety oversight systems in order to simplify the system for better resource management, to resolve current inefficiencies and to cater for future challenges in the frame of constant growth of the civil aviation industry;

1.2 The harmonisation of safety regulations at a regional level and a more effective management of safety oversight resources may be a solution to meet these growing challenges. In this context the development of regional cooperation has been a priority for many States in the last fifteen years, while being actively promoted by ICAO and by Industry.

1.3 RSOOs are well placed to address those challenges with the mandate given to them through regionalisation of certain oversight functions and the technical support they can provide to their Member States. ICAO has strongly promoted the role of RSOOs in Assembly Resolution A39-14 and provided guidance for their establishment in Doc 9734 Part B.

1.4 The 2017 RSOO Forum endorsed the Global strategy and action plan for the improvement of RSOOs and the establishment of a global system for the provision of safety oversight. As part of the implementation of this strategy:

1.4.1 The RSOO Cooperative Platform was set up to facilitate the sharing of experience between RSOOs, their interfacing with ICAO as well as and the coordination of technical assistance, with the overall objective to help strengthening RSOOs.

1.4.2 The development of GASOS (Global Aviation Safety Oversight System) was initiated by ICAO, with the double objective of a) strengthening State safety oversight capabilities by providing them with a system for the delegation of safety oversight functions to recognized Safety Oversight Organizations (SOOs) and of b) strengthening existing SOOs.

2. DISCUSSION: RSOO ACHIEVEMENTS AND CHALLENGES

2.1 Today about 17 initiatives of regional cooperation are launched or in preparation, including institutionalised RSOOs, ICAO led-projects and Cooperative Inspectorate Scheme. 13 RSOOs are functioning already covering more than 130 states around the world. They are acting in different legal, economical and procedural frameworks but are sharing the common objective to strengthen the safety oversight performance of their Member States. Examples of achievements and on-going developments for some RSOOs are provided in the separate Information Paper "RSOOs – Examples of achievements and developments".

2.2 It is recognized however that many RSOOs are facing challenges that are preventing them to contribute to the full extent possible to the reinforcement of the safety oversight capacity of their Member States. The main challenges have been exposed in the RSOO evaluation that was completed by ICAO in November 2017 and relate to :

- their legal framework,
- their organizational structure, resources and technical capacities
- their funding mechanism

- their management processes and systems

2.3 The current actions of ICAO aimed at supporting RSOOs and strengthening of their recognition within the ICAO system should be commended. ICAO should continue efforts to ensure the appropriate participation in the technical work of ICAO, for instance, by establishing the status of RSOO observer in the Air Navigation Commission, similar to the current status of the Observer of a Contracting State.[2]

2.4 In order for all RSOOs to be able to contribute effectively to reinforced global safety oversight capabilities and to achieving GASP objectives, it is necessary that both States and ICAO continue the efforts undertaken to establish well performing RSOOs. In particular through GASOS recognition RSOOs will be strengthened both by the independent assessment activities and associated improvement incentives, making them more effective and efficient in supporting their member States.

3. RECOMMENDED ACTIONS

The Conference is invited to:

a) Acknowledge that RSOOs have an important role to play in carrying out safety oversight functions on behalf of their Member States and, within the GASP framework, in addressing safety issues at regional level.

b) Recommend that States further support the strengthening of RSOOs by engaging actively in the establishment of their RSOO, by securing adequate, sustainable RSOO funding mechanisms, and by further delegating safety oversight functions to the RSOO.

c) Recommend that ICAO further supports the strengthening of RSOOs and their recognition within the ICAO safety system by facilitating access to technical support, facilitating the sharing of experience and knowledge between RSOO through the RSOO Cooperative Platform, establishing GASOS and by reinforcing the direct cooperation between ICAO and RSOOs in the framework of the GASP.

d) Recommend that ICAO ensures adequate recognition of RSOOs within the ICAO safety system

e) Recommend that RSOOs continue to engage in the RSOO Cooperative Platform and that they engage actively in the establishment of the future Global Aviation Safety Oversight System by supporting its implementation and, where applicable, by taking steps towards their own recognition as a competent Safety Oversight Organization.

4. REFERENCES

ICAO Resolution A39-14 on Regional cooperation and assistance to resolve safety deficiencies, establishing priorities and setting measurable targets

ICAO Document 10004 – 2017-2019 Global Aviation Safety Plan

Forum on Regional Safety Oversight Organizations (RSOOs) for Global Aviation Safety 22-24 March 2017, Ezulwini, Swaziland, Report

[2] ICAO Doc 8229, Rules of Procedure for the Air Navigation Commission

Global strategy and action plan for the improvement of Regional Safety Oversight Organizations (RSOOs) and the establishment of global system for the provision of safety oversight - ICAO

5. **RSOO OVERVIEW**

RSOO	Member States	Functional Areas (active/foreseen)
AAMAC	Benin, Burkina Faso, Cameroon, Chad, Central African Republic, Comoros, Congo, Cote d'Ivoire, Gabon, Guinee Bissau, Equatorial Guinea, Madagascar, Mali, Mauritania, Niger, Senegal	PEL, OPS, AIR, AGA, ANS, SMS
ACSA	Belize, Guatemala, El Salvador, Costa Rica, Nicaragua, Honduras	PEL, OPS, AIR, AGA, ANS, SMS, AIG, AVSEC
ACSAC	Benin, Burkina Faso, Côte d'Ivoire, Guinee Bissau, Mali, Niger, Senegal, Togo	PEL, OPS, AIR
ASSA-AC	Cameroon, Central African Republic, Congo, Gabon, Equatorial Guinea, Chad	PEL, OPS, AIR, AGA, SMS
BAGASOO	Cabo Verde, Gambia, Ghana, Guinea, Liberia, Nigeria, Sierra Leone	PEL, OPS, AIR, AIG, ANS, SMS
CASSOA	Burundi, Kenya, Rwanda, South Sudan, Tanzania, Uganda	PEL, OPS, AIR, AGA, ANS, SMS, AVSEC
CASSOS	Barbados, Guyana, Haiti, Jamaica, Suriname, Trinidad and Tobago, The OECS: Antigua and Barbuda, Dominica, Grenada, Montserrat, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and Grenadines, Anguilla, British Virgin Islands	PEL, OPS, AIR, AGA, ANS, SMS, AIG, AVSEC, ENV/CORSIA
EASA	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta. Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom	PEL, OPS, AIR, AGA, ANS, SMS, ENV/CORSIA
ECCAA	Antigua and Barbuda, Dominica, Grenada, Montserrat, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and Grenadines, Anguilla, British Virgin Islands	PEL, OPS, AIR (TBC)
IAC	Azerbaijan, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Uzbekistan, Russian Federation, Tajikistan, Turkmenistan, Ukraine	PEL, OPS, AIR, AGA, ANS, SMS, AIG, AVSEC
iSASO	Angola, Botswana, Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia, Zimbabwe	TBC
PASO	Cook Islands, Kiribati, Nauru, Niue, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, Vanuatu	PEL, OPS, AIR, AGA, ANS, AVSEC
SRVSOP	Argentina, Bolivia, Brazil, Chile, Colombia, Cuba, Ecuador, Panama, Paraguay, Peru, Uruguay, Venezuela	PEL, OPS, AIR, AGA, ANS

— END —

International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/xxxx
../../18
(Information Paper)
English only

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues
5.4: Cyber resilience

Considerations about Cybersecurity in Aviation

(Presented by Austria on behalf of the European Union and its Member States[1], the other Member States of the European Civil Aviation Conference[2]; and by EUROCONTROL)

SUMMARY

This paper supports the AN-Conf/13-WP/xxxx on cybersecurity by expanding on concepts intended to be used to improve the situation of Cybersecurity in Aviation. It will touch on notions like aviation being a System-of-Systems, which should be designed with Security-by-Design in mind. It will also touch on rationales why any organisation should manage not only their individual cybersecurity risks, products and services by means of an Information Security Management System (ISMS), but also why this should be done in a concerted way.

The paper also addresses the notions of dependability, confidence and trust, from which it derives concepts for Digital or technical Trust, Trustworthiness and Operating Conditions for cybersecurity, why they are needed and which benefits they provide.

The paper further touches on the differences between Information Sharing and the notion of Reporting and Notification.

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Republic of Moldova, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Turkey and Ukraine.

(15 pages)
8. AN-Conf13_COM A_EU-ECAC-ECTL WP_IP_CYBER_Consolidated final.docx

1. INTRODUCTION

1.1 The availability of correct information and the correct functioning of safety-critical information systems are pre-requisites for a safe and secure civil aviation as the sector encounters further digitalization. The aviation system is highly interconnected and information travels globally. Therefore, a holistic and end-to-end approach must be taken to cyber security initiatives in the aviation sector. These will only be successful if aviation is understood as a "System-of-Systems", for which all members of the aviation community are accountable and share responsibilities. The aviation system in the future thus requires more concerted design and less individual evolution to maintain its resilience against cyber interference.

1.2 To avoid confusion with other terminology, this paper will use the term "cyber security" interchangeably with "information security". The latter is also perceived as the more accurate term, as the ultimate objective of protection is information and those systems and interfaces processing, exchanging, or storing information.

1.3 This paper supports the European working paper AN-Conf/13-WP/xxxx and introduces into the different concepts in a more detailed manner. It starts with a discussion about the "System-of-Systems" notion, including fundamental design principles like "Secure-by-Design".

1.4 It further addresses some objectives and characteristics of Information Security Management Systems in general as well as its extensions with respect to the "System-of-System" approach, as required for the aviation sector.

1.5 This paper also elaborates on the notion of Dependability, Trust, and Confidence. Trust generally reflects the level of anticipation that another party behaves as legitimately expected, while confidence is about the level of control and scrutiny, of facts and evidences, which can be considered in the assessment of expected behaviour of another party (or system). In the aviation sector, trust - in addition to confidence - in each partner is paramount. *Digital* or *Technical Trust* and *Trustworthiness* are two related concepts which will be addressed in this context. Further, the information security environment is constantly changing, a concept allowing implementation of cybersecurity measures at different times and adaptation of diverging trustworthiness levels will thus be required. One reason: it will be highly unlikely that all aviation will be able to establish to the same level of trustworthiness at the same point in time. This paper will describe an adaptation of the existing concept of Operating Conditions, as it can be applied to cyber security.

1.6 Sharing information for long term trend and systemic weakness analyses purposes differs from Information Sharing for operational purposes. However, they are linked to the extent that lessons learnt from operational occurrences should be used to initiate changes targeted to reduce risks. Regulatory update processes are one vehicle to achieve improvements. Within organisations Computer Security Incident Response Teams (CSIRT) or Cyber Security Centres (CSC) are usually tasked to support operational Information and Communication Technology (ICT) entities in securing their services and systems.

2. DISCUSSION

2.1 **System-of-Systems** – Before entering into the discussion of *Systems-of-Systems* it should be emphasised that in the context of this paper a *System* consists of Products, People and Processes. This means that the term *System* should be broadly interpreted and is not limited to technical equipment!

A description of a System-of-System (SoS) reads like this: "*A system of systems (SoS) brings together a set of systems for a task that none of the systems can accomplish on its own. Each constituent system keeps*

its own management, goals, and resources while coordinating within the SoS and adapting to meet SoS goals."[3].

That's not much different from the description of a system itself. This is quite natural, as a SoS is a System in itself. So, in the context of ICAO, what distinguishes a SoS from a "*System*"? There are a few characteristics, which allow for a distinction (Maier, 1998[4]):

- **Operational independence of elements:** The elements that make up a system of systems are in turn fully self-sufficient systems. These systems can also be independently operated and used. You can also leave a system-of-systems network to join another System of Systems.

- **Managerial independence of elements:** The subsystems of a SoS can not only work independently of each other, they are usually also developed and procured separately. Their lifecycle is independent of the system-of-system lifecycle model. However, from the security perspective a SoS can only be protected by shared management of risks by all SoS elements.

- **Evolutionary Development:** A completely developed System of Systems does not exist! Its development and existence is evolutionary. Over the entire lifecycle, functions - and thus subsystems - are added, removed or changed on the basis of operational experience. From an information security perspective this creates the challenge of composability: Under which conditions can changes to the SoS composition avoid degradations in the effectiveness of protection of the SoS?

- **Emergent behaviour:** Emergence is the more or less spontaneous formation of new qualities or functions of a system as a result of the interaction of its elements. Emergence can be observed well in nature, for example in the swarm behaviour. A large bird or fish swarm are good examples of this. The individual individuals of such a swarm know only the position and direction of movement of their immediate neighbours. By emergence, however, the movement of the entire swarm appears to an outside observer as if it were centrally controlled. Transferred to a system of systems, this means that the composition of the subsystems creates certain properties and services for the user that can no longer be uniquely assigned to subsystems.

- **Geographical distribution of elements:** The geographical extent and distribution of subsystems of a SoS is often very large. "Size" is certainly a fuzzy and relative concept, but in terms of a SoS, it means that its subsystems, due to their spatial distance from one another, can essentially exchange only information, and not significant amounts of mass, matter or energy.

Systems-of-Systems can be classified into the following categories (Maier 1998; Dahmann and Baldwin 2008[5]; DUS(AT) 2008[6]; Dahmann, Lane, and Rebovich 2008[7]):

[3] ISO/IEC/IEEE 15288 Annex G (ISO, 2015), Systems and software engineering -- System life cycle processes
[4] Maier, M.W. 1998. "Architecting Principles for Systems-of-Systems". Systems Engineering.
[5] Dahmann, J., and K. Baldwin. 2008. "Understanding the Current State of US Defense Systems of Systems and the Implications for Systems Engineering." Paper presented at IEEE Systems Conference, 7-10 April, Montreal, Canada.
[6] DUS(AT). 2008. Systems Engineering Guide for Systems of Systems," version 1.0. Washington, DC, USA: Deputy Under Secretary of Defense for Acquisition and Technology (DUS(AT))/U.S. Department of Defense (DoD).
[7] Dahmann, J.S., J.A. Lane, and G. Rebovich. 2008. "Systems Engineering for Capabilities." CROSSTALK: The Journal of Defense Software Engineering. (November 2008): 4-9.

- **Virtual:** Virtual SoS lack a central management authority and a centrally agreed upon purpose for the system-of-systems. Large-scale behaviour emerges—and may be desirable—but this type of SoS must rely upon relatively invisible mechanisms to maintain it.

- **Collaborative:** In collaborative SoS the constituent systems interact more or less voluntarily to fulfil agreed upon central purposes. The Internet is a collaborative system. The Internet Engineering Task Force works out standards but has no power to enforce them. The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards.

- **Acknowledged:** Acknowledged SoS have recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment approaches. Changes in the systems are based on collaboration between the SoS and the system.

- **Directed:** Directed SoS are those in which the integrated system-of-systems is built and managed to fulfil specific purposes. It is centrally managed during long-term operation to continue to fulfil those purposes, as well as any new ones the system owners might wish to address. The constituent systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose.

In the context of ICAO the aviation community will establish multiple types of sub-SoS. However, on the ICAO level aviation can be considered to be at best a SoS of the ***Acknowledged*** category.

In the context of information security of a System-of-System, a consideration mentioned above needs to be highlighted: ***Composability***. It describes the challenges of integrating multiple elements (components for systems, or subsystems for SoS) into bigger entities. Systems integration based upon the functionality of its individual elements is focused upon the individual properties of these elements. Interface definitions and functional specifications determine the conditions under which such integration can take place (e.g. compatible definitions for network interfaces or information formatting; frequency of exchange; physical layout; etc.). Physical or logical performance properties may create further conditions for integration (e.g. heat dissipation; duty-cycle; Gflops; MTTF; Severity of safety effects; etc.). In essence, if determined that integration is possible, the individual properties of each element are maintained. An example: In the figure below System A and System B are integrated and form the resulting System AB. Interfaces and functional properties expose their combined characteristics to their environment, unless they are now internal to the new system (e.g. individual external interfaces may become combined internal interfaces).

However, when it comes to the integration in the information security context, as shown in the next figure, the limitation to specified functionality and performance is no longer adequate. The integration under consideration of the information security context includes additionally the integration of the Security Environment (SE) of each element. Not only is each individual SE largely unknown (its space is simply too vast, we only know about individual spots that have been investigated), the resulting SE is almost totally unknown – including the consequences of their integration. To be able to make any assessment of the SE,

an extra step of assurance actions is required, which are dedicated to the resulting combined environment called Refutation.

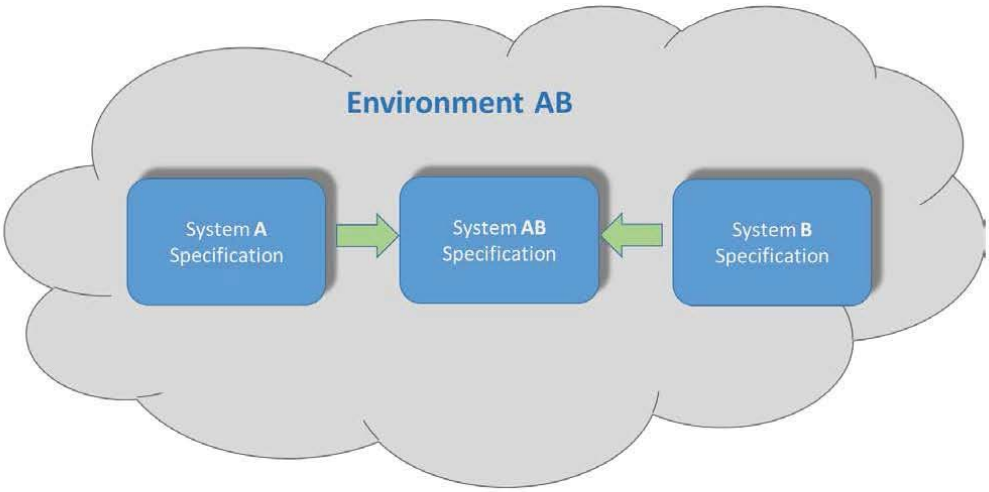
Refutation is introduced by Eurocae/RTCA ED-203A / DO-356A and used in the sense of demonstrating the absence of problematic behaviours, as in refuting the allegation of vulnerabilities. Hence, information security refutation is demonstrating the absence of information security problems.

An example: In the figure below System A, including its (information security) environment, and System B, also including its (information security) environment are integrated and form the resulting System AB, including its combined (information security) environment. Like in the example before, Interfaces and functional properties expose their combined characteristics to their environment, unless they are now internal to the new system (e.g. individual external interfaces may become combined internal interfaces). However, no statement can be made about the combined environment, until Refutation actions have been performed.

Examples for refutation actions are security penetration testing and may include fuzzing tests. As a generalization, when a set of requirements are generated in response to a negative requirement/objective – specifying the absence of specific behaviours – then even though a set of requirements are correct and complete and are properly developed, this does not mean that the resulting assurance actions necessarily provides confidence in the absence of specific undesired behaviours beyond what is called process assurance.

ED-203A / DO-356A continue in stating, "*Refutation activities act as an independent set of assurance activities beyond those assurance activities driven from the formalized analysis and requirements. Any time system complexity precludes exhaustive testing that an unwanted behaviour never occurs, refutation can be used to formally demonstrate that an unwanted behaviour has been precluded to an acceptable level of confidence*".

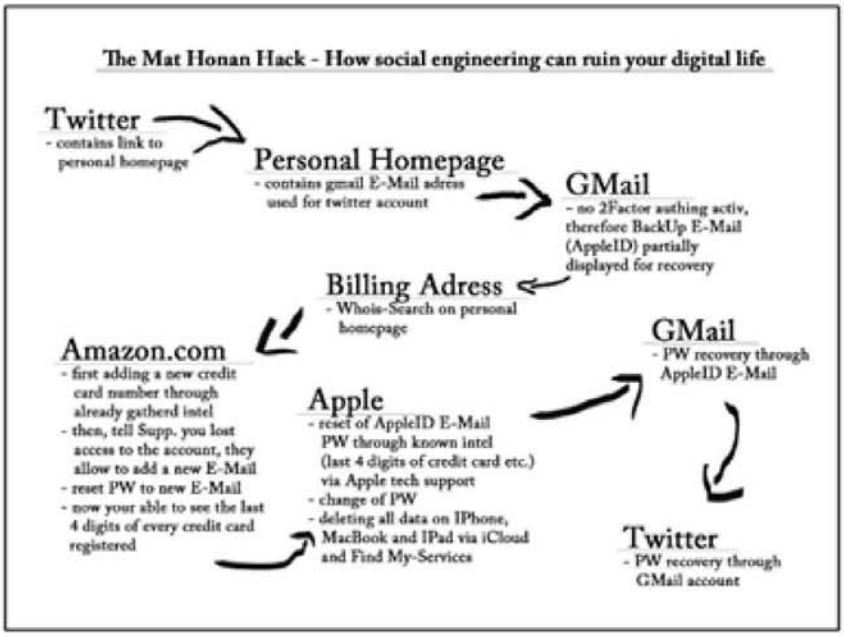
For integrations like the one in the figure below applying refutation for key areas seems to be straightforward. However, the above mentioned exhaustive refutation effort may increase overwhelmingly, as the complexity of the SoS – ultimately like the global aviation system - increases. The task of the community is thus to identify representative subsystems and research to which extent and by which margin



of error its results – based upon the measures taken and the practices used – can be transferred to other subsystems. An example: SESAR is developing coherent approaches for its constituents, resulting in a significant degree of compatibility among them. It may be conceivable that refutation results of one constituent system will also be applicable to other constituent systems, and thus do not require a full repetition there. Another task is to initiate the development of larger subsystems, which consider information security during their initial design phase (see "Secure-by-Design"). This will allow for the evolution of the aviation system to higher levels of resilience and maturity against unauthorised or unlawful electronic interference by adverse (intentional) or negligent (unintentional) actors.

An example for such global, collaborative SoS is The Internet. Organisations are individually trying to protect themselves against information security threats. Unfortunately, their approach is not sufficient, as one prominent case demonstrated in 2012: an editor of the Wired Magazine, Mat Honan, explains in the "HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING" article[8], how "*IN THE SPACE of one hour, my entire digital life was destroyed*". A malicious hacker, interested in his Twitter account, took advantage of the uncoordinated information security approaches taken by Internet Giants like Google, Apple, or Amazon, and eventually gained access to his Twitter account.

The lessons learnt from this case are that not only gaps in the approaches will create dangerous loopholes, uncoordinated overlaps may be equally dangerous for the effectiveness of protection or a larger System-of-Systems.



2.2 **Secure-by-Design** – In engineering, this means that systems – in the broad sense as mentioned above – when they are designed and integrated into SoS, are securable, secure and remain secure during their whole life-cycle. Adverse practices are taken for granted and care is taken to minimize their

[8] https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

impacts. However, in the past, and unfortunately probably for many years to come, information security has been and will be considered by some as an add-on to systems.

The aviation system that we use today has been designed during many decades, using a threat model relying upon presumptions such as attackers having inferior technological, or financial capabilities and little or no knowledge of the system. An insider threat was not included in the model for a very long time and only less than a decade ago information security threats have been internationally recognised by the aviation community as part of the ICAO Beijing Convention of 2010 (though only indirectly). However in the meantime the world has evolved, developing new information system technologies that aviation is heavily relying upon, however without reconsidering its threat model. A new model should now include the fact that technological capabilities have increased with the development of e.g. Software Defined Radios which allow interception and generation of messages on analogue channels at no extra cost for bespoke components. At the same time, the benefits of using commercial technologies in aviation helped also reducing the effort for potential adversaries to interfere with the system.

A *common* understanding of the term "secure" is that no interference with a system could change its intended or expected behaviour or performance. While this seems simple from a concept perspective, it is more difficult in its application as it can encompass many complex interactions, in particular in a SoS environment.

Many of the core functions of the aviation system are shared among multiple stakeholders. Knowing about those functions and their security needs is essential to the functional and architectural design of the system. As a general rule, the Secure-by-design principles will rely upon three pillars which are reflecting the most common risk assessment and management methodologies.

- 1st pillar - reflects the fundamental principles of the architecture: how components relate to each other and the nature of their interfaces. It deals with dependencies and reduction of complexity, with composition of systems and with trust. But it will also consider the evolution of the system without jeopardising its security capabilities.

- 2nd pillar - deals with the information security needs of functions across federated aviation systems, and the design and effectiveness of information security measures applied. Ensuring to meet those needs continually, requires trans-organisational risk management. Sharing the results of risk assessments among providers of functions are giving the key elements to the definition and application of mitigations. However, the design of information security measures should consider an approach which prevents to oppose security principles (e.g. "secure fail") with safety principles (e.g. "safe fail").

- 3rd pillar - contributes to the initial and continuing security of a system. A system and in particular a SoS will evolve throughout its lifetime. For example, an aircraft will be operating for approximately 30 years without any fundamental change in its information system architecture. One retrofit during lifetime is the maximum to be expected, implying that the maintenance of the security status of the aircraft would require an agility which has to be integrated into the design. But retrofitting has also its challenge to avoid transforming a system able to sustain the security objectives, into a system which is not. The reliability of processes to maintain the level of security of a system at its best, is also an essential element of the third pillar.

Experience has shown that when these principles were applied to the design of a system, development time and effort often rose in comparison to typical "time to market"-driven commercial development practices. This economic discrepancy has resulted in various proposals for using untrustworthy components to create trustworthy systems, with unsatisfactory results. However, regulation has been influencing positively the

safety level of flights so far, and the future will prove to be even safer with a novel engineering approach integrating information security across the aviation system, embracing the "Secure by Design" paradigm relying upon the 3 pillars above.

2.3 **Information Security Management Systems** – Existing concepts of Information Security Management Systems (ISMS) are inherently limited to individual organisations. Two of the most prominent standards for ISMS are ISO 27001, or NIST Special Publication 800-39, but other standards also exist. Their scope is to: "*...specify the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization*". In addition they also include requirements related to the assessment and treatment of risks, as they pertain to an individual organisation.

The risk management process itself is very well established in aviation. However, there are a number of reasons, why the introduction of an ISMS is a fundamental deviation from the way the aviation community is used to conducting business. One key reason is the difference between the treatment of so-called "*software bugs*" in the traditional risk management process and the one of "*vulnerabilities*" in the ISMS.

For the former, safety and quality assurance requirements require measures for the identification and remediation of software design and implementation errors, commensurate with the level of safety risk they may create or contribute to. As soon as all those measures have been taken, all tests completed and passed without deficiencies, the software will only be modified again if unexpected behaviour can be traced down to software deficiencies.

For vulnerabilities this will be quite different. Just like software bugs, all known vulnerabilities will have to be eliminated with scrutiny commensurate with the level of safety risk they may create or contribute to. The security environment, which is defined as "*… the external security context in which an asset performs*

its function" changes constantly, independently and outside of the influence of the aviation community: new threats emerge, new ways to interfere with existing functionalities are discovered, and new vulnerabilities are either reported to manufacturers and/or recorded with public vulnerability databases (https://cve.mitre.org/) and scored. This means new vulnerabilities will become known in multiple ways:

- Unexpected behaviour
- Reporting/Publication by third parties, e.g. of standards or commercial implementations
- Research of own implementations, e.g. in response to new publications

Although the majority of vulnerabilities do not apply to the safety critical or airspace operational systems, the aviation community will have to observe very closely these types of information, regardless where they are published. Vulnerability management includes, inter alia, the identification of vulnerabilities and resulting risks, and the definition of actions to be taken to remedy the effects commensurate with those risks until a fix has been developed and deployed. This type of activity is well established for "IT" (Information Technology) systems but has not been widely introduced into the "OT" (Operational Technology) systems management environment.

As civil aviation is such a tightly interwoven System-of-Systems, comprising of interconnected products, people, and processes, including connections with military systems, the limitation to the perspective of an individual organisation is insufficient. Thus civil aviation will have to introduce ISMSs with the notion of a shared, trans-organisational management of cyber security, allowing the coordination of measures throughout the sector, taking into account the fact that information is shared within the entire aviation system, and that the same systems are common to many actors in the sector. Some high-level ISMS subjects reaching beyond the boundaries of individual organisations are Information Security Policies, Asset Management, Communications Security, Cryptography, Supplier relationships, and Information Security incident management. Such management systems, preferably aligned or integrated with existing aviation risk management systems, assist both individual organisations and the sector as a whole to better prepare and respond to information security threats.

2.4 **Dependability, Trust, and Confidence** – In the paper "Basic Concepts and Taxonomy of Dependable and Secure Computing"[9], Avizienis et al. propose definitions relating to dependability as well as an associated taxonomy. These terms will be important in order to understand, what needs to be established by technical, organisational or operational means to enable recipients of information to place "trust" or "confidence" into it and the organisation submitting it.

*The **Dependability** of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable*. It can be said that the dependability of a system should suffice for the dependence being placed on that system. In other words, **dependence** of e.g. System A on System B represents the extent to which system A's dependability is affected by that of System B. An example is a flight crew of an airplane (= System A) depending on the information provided by an ATC Centre (= System B).

***Trust** is the anticipation of one entity in the evaluation of the expected behaviour of another entity.* An example is that an originating system does not deliberately provide false information.

***Confidence** is about the level of control and scrutiny, which one entity can factor into the evaluation of the expected behaviour of another entity.* An example is the process of initial aircraft certification, where

[9] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr - Basic Concepts and Taxonomy of Dependable and Secure Computing: IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1, JANUARY-MARCH 2004.

assurance processes, inter alia, allow for a level of scrutiny of the development and integration process commensurate with the airworthiness requirements. It creates the level of confidence with the Certification Authority permitting it to issue the Type Certificate.

There are three levels of confidence/trust when communicating information from one originating system to another receiving system:

a) The confidence that the information is from the alleged originator and that it has not be tampered with. This could be considered as "Digital Trust" or "Technical Trust", as it has to rely only on technical measures of the communication link to assure that confidence. Digital Trust is auditable, as it allows the verification that technical standards are complied with;

b) The confidence that the infrastructure of a peer organisation (i.e. a "*system*") is resilient against unauthorised or unlawful electronic interference commensurate with the expected service delivery. This could be considered as "Organisational Trust", as it has to rely on organisational measures and technical measures put in place by that organisation. This results in the ability of one organisation to depend upon another organisation. Organisational Trust is auditable, as it allows the verification that process and technical standards are complied with;

c) The trust that the originator of information provides uncompromised information. This could be considered as "Societal Trust", as it relies on only on the anticipation of an expected behaviour. Societal Trust is not auditable.

Discussion of Case a): The common challenge for both areas of confidence (verification of alleged originator; verification of integrity of information) will be the system (organisation including its technical infrastructure) which guarantees the validity of the identity of the originator, expressed by an electronic identification (Digital Certificate) used for the electronic signature of the information exchanged. More information about this mechanism can be found in section 2.6.

Discussion of Case b): The challenge for this area of confidence is with the system (organisation) which approves and oversees (e.g. by audits and inspections) the operation of another system (organisation including its technical infrastructure). It guarantees that the system operates at a particular level of trustworthiness, with respect to the protection of the system against unauthorised or unlawful electronic interference, potentially creating or contributing to a risk of compromised information. More information about this mechanism can be found in section 2.7.

Discussion of Case c): In cases where no controls or scrutiny can be exercised by the aviation community, systems (organisations) may have to trust blindly. On the other hand, past experience in many areas may contribute to the evaluation of a significant level of trust, despite the lack of any hard evidence.

The next three paragraphs will address the two first cases, for which the international aviation community will have to establish standards and recommended practices.

2.5 **Digital or Technical Trust** – A study by Gartner, Inc, about Digital Trust states that it "…underpins every digital interaction by measuring and quantifying the expectation that an entity is who or what it claims to be and that it will behave in an expected manner." This has a few consequences which those, exchanging information of any kind by means of technical systems, will have to bear:

- Every party wishing to be part of a trusted information exchange will need to have a digital identity;
- The level of trust in that party is strongly dependent upon the level of scrutiny of its real identity, being a measure for the assurance of its validity;

- The level of trust in all parties is strongly dependent upon the technology used for the digital identity. Technologies, which are not Quantum-computing resistant, will undermine trust levels;
- Only exchanges between parties having such digital identity will be considered trustworthy;
- Setting-up an information exchange will require the verification of the validity of digital identities (authentication);
- Establishment of an information exchange requires consent by all participating parties (authorisation);

However, the benefits are:

- The integrity of each information exchange can be verified;
- The confidentiality of each information exchange can be assured, if required.

Digital or Technical Trust relies upon cryptographic methods to establish these benefits between parties of the aviation community. And it keeps adversaries out of the communication for the majority of risks. In all clarity it is to be stated that ***all*** Radio Frequency (RF) communication, such as the one by Satellite or VHF, is susceptible to electromagnetic interference, which may not impair the integrity or authenticity of the communication, but which will jeopardise its availability. Thus, Digital or technical Trust is not the Silver Bullet against all technical communication threats.

There are considerations which link Digital or technical Trust to Organisational and Societal Trust. They concern the first three bullets above and are related to the scrutiny of the verification of the real identity as well as to the organisations and systems operated issuing and maintaining the validity of the digital identities.

In all societies, identities of individuals are established and maintained by States, starting with birth certificates and ending with a death certificate. There are equivalents for organisations, which differ slightly between types of organisations and States. As long as communication takes place between individuals or organisations, the level of scrutiny of the validity of the real identity is largely in the hands of state authorities or delegated organisations, and as such subject to Societal Trust. As soon as communication takes place between technical systems, e.g. autonomous command and control communication or uploading of software into a system supplied by its manufacturer, concepts need to be established providing similar levels of validity of the digital identities used. For example, individuals could act as "device sponsors", to act on behalf of a device whenever a digital identity is to be established or maintained.

Organisations establishing digital identities operate information systems to perform their duties. The level of trustworthiness (see next section) of these information systems is largely dependent upon how well they have been designed, developed, integrated, operated and maintained and how secure integration, operation and maintenance is. In particular for digital identities the process of their decommissioning is equally important. If these systems enjoy a high level of trustworthiness, their digital identities will benefit from it. However, if they fail to be highly trustworthy, the digital identities they established suffer from lower levels of trust, regardless of the level of scrutiny put into their establishment.

A global trust framework will thus be necessary to enable resilient and trustful information exchange between parties of the aviation community. It shall not only define elements of Digital or Technical Trust, but will also have to include those for Organisational Trust, considering the variability of the possibilities of Societal Trust from a global perspective.

2.6 **Trustworthiness** – In civil aviation, a strong framework of confidence has been built over decades. Trustworthiness is a formal concept by which one organisation - or a system it operates - can rely on the cyber security properties of another organisation - or a system it operates. It can thus be considered as one possible instantiation of *Organisational Trust*. As trust is never absolute, the concept proposes multiple levels of Trustworthiness, which should depend upon the impact (e.g. safety or service continuity, such as expeditious flow of traffic in a region) it will have upon the relying party.

When discussing how trust can be established among organisation, NIST SP 800-39 states: "*Organizations are becoming increasingly reliant on information system services and information provided by external organizations as well as partnerships to accomplish missions and business functions. This reliance results in the need for trust relationships among organizations. In many cases, trust relationships with external organizations, while generating greater productivity and cost efficiencies, can also bring greater risk to organizations. This risk is addressed by the risk management strategies established by organizations that take into account the strategic goals and objectives of organizations*".

And it continues "*Two factors affecting the trustworthiness of information systems are:*

- *Security functionality (i.e., the security features/functions employed within the system); and*
- *Security assurance (i.e., the grounds for confidence that the security functionality is effective in its application).*"

In aviation there is precedence for these concepts: Design Assurance is required for all aircraft development and integration and provides confidence about the airworthiness. ***Validation*** activities ensure that the *right functionality* has been put in place while ***Verification*** activities ensure that the *functionalities* have been put in place *correctly*. Confidence is based upon these assurance actions, and that they have been performed yielding acceptable results. Those actions have been designed to address – and be commensurate with – the severity of impact of safety risks. Higher levels of severity of impact will thus need higher levels of scrutiny in the development process.

Security assurance has to go yet one step further, as the right functionality being put in place correctly is only a necessary, but not a sufficient condition. Even after adequate scrutiny with respect to known vulnerabilities the potential for the existence of unknown vulnerabilities, or the misuse of intended functionality, still exist. Traditional airworthiness related assurance actions cannot make any statement about this potential. By extending those actions with ***Refutation*** actions, this potential can be evaluated and scored and remedial actions be derived.

Based upon those two factors, a similar concept is proposed for information security properties. It is designed to reflect the effectiveness of protection against cyber threats. Multiple levels of Trustworthiness, attributed to an organisation and the systems it operates, could be defined. Each level would be defined by combining

a) the implementation of security measures against identified information security risks with

b) the assurance that they have been architected and implemented commensurate with the risks they are intended to mitigate.

When two organisations connect their systems and operations thereof the trustworthiness level allows them to evaluate how much confidence each organisation can place into the peering organisation in contributing to its own protection – and then either take measures to compensate shortcomings or help the peering organisation to increase their level of trustworthiness. The latter may be the more cost-effective solution, in particular in complex interconnection arrangements.

In essence, confidence in (a) is primarily about the absence of development errors and vulnerabilities and (b) in organisations adequately protecting civil aviation is what will prepare the future of safe flight. The Trustworthiness concept should be integrated into ISMS, which in turn should be aligned or integrated with existing management systems.

2.7 **Operating Conditions for Cybersecurity** – Aviation is a global operation which constantly evolves. Changes are initiated permanently on organisational, local, national, regional and even global level. Further, transitioning globally to a safe and secure aviation sector will not happen overnight. Thus, special care has to be taken that all constituents of the aviation system migrate in a concerted way through increasing states of cyber security while maintaining seamless interoperability.

So, Trustworthiness Levels provide for one factor of the ability of a third party to evaluate the risk of a communication connection with an organisation and a system it operates. Another factor is about the residual risk that organisation exposes to the third party after applying its security measures. Trans-Organisational Risk Management standards complement these two factors for the final information security evaluation. There are a few limitations associated to this evaluation. First of all, this is a static snapshot in time. However, the dynamics of the evolution of individual organisations and systems they operate, belonging to the globally interoperable, secure infra-structure needs to be covered. Secondly, it requires criteria against which the acceptability of the connection between two organisations can be determined. For every connection between peers it will be essential that Trustworthiness Levels will be compatible among them, consequently requiring the definition of matching pairs. Certain pair combinations of Trustworthiness Levels will be permissible to connect, as they will meet cyber security objectives with acceptable risk levels. Other combinations may fail to meet the objectives.

Two levels of speed of evolution of connections between peers need to be distinguished: the one between organisations which connect their ground systems, and the one between air- or space-based vehicles and ground-based systems, between which the connections transition at a fast pace. Their key discriminator is the speed by which their cyber security condition evolves.

Slow evolution: On the one hand, ground systems in general – and ATM/ANS systems in particular - evolve on a comparatively slow pace. Changes in their operating conditions are largely determined by changes either of their own cyber security situation or the one of the systems they are connected to. This allows for a closely coordinated adaptation of cyber security properties – including associated roles and responsibilities – such that all connected parties meet the overall cyber security requirements. Thus, acceptable Operating Conditions could be established by proper pairing of Trustworthiness Levels between connecting organisations and systems. As a side effect, it will create incentives to reach agreements between interconnected organisations about the conditions for matching, yet differing Trustworthiness Levels, ultimately leading to economically balanced approaches. When functionalities change, leading to changed operating risks, Trustworthiness levels may have to be adapted. Also, changes in the notion of the acceptability of risks may be another factor requiring Trustworthiness levels to be adjusted. Previously acceptable pair combinations may no longer be acceptable, leading to modifications to security measure functionalities or assurance requirements by either or both peers.

Fast evolution: On the other hand, aircraft are migrating from one location to another at a comparatively high pace, while being connected dynamically to a large number of peers during a short period of time. The challenge here is, that aircraft or ground systems will not be in a one single or matching state of cyber security at any given day. There will be always individual differences due to the differences in the speed of evolution. Those connections could be established by proper pairing of Trustworthiness Levels between connecting systems. However, due to the comparatively high pace, matching Trustworthiness Levels need to be pre-coordinated and maintained a priori as part of organisational approval and aircraft certification

processes. To keep them acceptably secure for operation, the consideration of this evolution on either side will be required.

An example may shed some light of the concept: In the existing concept of Operating Conditions, horizontal separation requirements applicable within one airspace are mandated. A certain equipage of ground and aircraft systems with certain (functional and assurance) properties are needed to meet respective requirements. These properties create matching functional and safety levels, allowing for safe operation. Thus, the existing concept of Operating Conditions could serve as a blue print for cyber security. Adequately paired Trustworthiness Levels between ATM/ANS and aircraft systems would allow for safe and secure airspace use.

2.8 **Information Sharing** – A global ISMS framework could also assist in creating a more coherent information sharing mechanism for cyber security risks. The Information Technology (IT) world has created the concept of a *Cyber Security Centre*, which "handles" information about cyber security incidents, including collecting and maintaining databases of incidents, threats and vulnerabilities, and provides analyses and guidance on successful practices about how to counter the actual incident to its constituencies. These tasks are associated with Information Sharing.

Internationally, Computer Emergency Response Teams (CERTs) and CSIRTs have created a community, called Forum for Incident Response and Security Teams (FIRST). This forum could serve the civil aviation community as a template for a nucleus, for further expansion of its collaboration. While FIRST does not share operational information itself, it enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams. However, this approach will not suffice due to the inter-connectedness of the civil aviation community. It will need a concerted approach towards a global, operational information sharing mechanism with the objective of not only reacting to incidents, but also being increasingly resilient to future attacks. One example: In dealing with the discovery of new vulnerabilities, the information collected by CSIRTs will allow for a the anticipation of emerging risks, consequently allowing community members to take preventive measures to limit detrimental effects on civil aviation. In summary, this objective aims at improving the awareness about cyber-threats. Once aviation CSIRTs coordinate among each other and their respective members, internationally aligned defensive measures against cyber threats will be possible.

Further, cyber security threats exist beyond civil aviation, e.g. in other transport sectors but also non-transport related sectors. They often share technologies and implementations, hence threats and vulnerabilities. It is therefore fundamental to share policies, intelligence information, and best practices with organizations from these sectors. An approach to cyber security in civil aviation should thus benefit from other national or regional cross-sectorial approaches and experiences. Close communication with governmental entities engaged in cyber security of other sectors will enhance the benefits for Civil Aviation Authorities of Contracting States.

2.9 **Reporting and Notification** – While industry has developed models of voluntary information sharing, States often rely on mandatory reporting or notification. There are a number of differences between the two models, which sometimes create sharp discriminations. One example highlights a difference in information handling: Information Sharing uses the so called Traffic Light Protocol (TLP), which determines "*how widely originators want their information to be circulated beyond the immediate recipient.*" It is at the originators discretion to share or not to share – and when to share – information. States often combine principles of Information Classification to identify sharable information for a particular group of recipients with the need-to-know principle, to determine who will be the ultimate recipient.

ICAO Annex 13 requires Contracting States to establish mandatory and voluntary reporting systems. The objective of mandatory incident reporting systems is to "*facilitate collection of information on actual or potential safety deficiencies*". To capture also other deficiencies, which the mandatory reporting system does not capture, the voluntary reporting system "*shall be non-punitive and afford protection to the sources of the information*". The collected information is then analysed to determine patterns or systemic deficiencies. From this knowledge preventive actions can be derived. Obviously, this is a longer term process, which has no immediate operational impact. Further to that, ICAO requirements relating to the implementation of safety management systems (SMS) require that aviation service providers develop and maintain a formal process for effectively collecting, recording, acting on and generating feedback about hazards in operations, based on a combination of reactive, proactive and predictive methods of safety data collection.

A similar approach is taken by some regional or national regulations for other areas of commercial services. Taking European Union as an example, the Directive on security of network and information systems (NIS-Directive)[10] requires operators of essential services to notify their competent authority about "significant incidents". Similar objectives as for safety incident reporting schemes apply. However, the NIS-D also introduces a network of Computer Security Incident Response Teams (CSIRTs), which is established to "*contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation*". On the national level CSIRTs will collaborate with the Operators of Essential Services to detect cyber security events and to minimise the impact of cyber security incidents.

— END —

[10] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the UnionOJ OJ L 194, 19.7.2016, p. 1–30

International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/xxxx
../../18
(Information Paper)
English only

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5 : Emerging issues
5.5 : Other emerging issues impacting the global air navigation system including unmanned aircraft systems (drones), and supersonic and commercial space operations

EMISSIONS FROM SUPERSONIC AEROPLANES

(Presented by Austria on behalf of the European Union and its Member States[1], the other Member States of the European Civil Aviation Conference[2]; and by EUROCONTROL)

EXECUTIVE SUMMARY

This paper presents the European views on civil supersonic aeroplane projects. While the Committee on Aviation Environmental Protection (CAEP) is developing environmental standards and recommended practices (SARPs) for supersonic aeroplanes, AN-Conf/13-WP/13 invites ICAO and regulators to engage their regulatory mechanisms to ensure that the necessary policies are in place before supersonic operations become regular again. However, the environmental impact of this type of aviation remains a major concern in Europe and a challenge that must be overcome before considering their introduction into the global air navigation system.

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Republic of Moldova, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Turkey and Ukraine.

INTRODUCTION

1. Considering that supersonic aeroplane projects could come to fruition as early as 2022, the ICAO's Committee on Aviation Environmental Protection (CAEP) is in the process of developing environmental standards and recommended practices (SARPs) that are intended to enable supersonic aeroplane flights in ICAO Member States. The Authors of this paper welcome this effort forming part of challenges for the introduction of future supersonic aeroplanes in global aviation.

2. While the standard setting process is ongoing, AN-Conf/13-WP/13 right now invites regulators to implement their respective regulatory mechanisms to ensure that the necessary policies are in place before supersonic aircraft operations become regular again.

3. The Authors of this paper would like to share their opinion on the standard setting challenges to be overcome and, more broadly, on the public acceptability of supersonic aeroplane projects.

NOISE OF SUPERSONIC AEROPLANES

4. In September 1968, the Sixteenth Session of the ICAO Assembly adopted Resolution A16-3 which is based on two main recitals: (i) the problem of aircraft noise in the vicinity of many of the world's airports is so acute that public reaction is growing to the point of causing serious concern and requiring an urgent solution, (ii) the introduction of new aeroplane types could increase and aggravate this noise unless measures are taken to improve the situation.

5. Standards and Recommended Practices (SARPs) relating to aircraft noise were first adopted in 1971 pursuant to the provisions of Article 37 of the Convention on International Civil Aviation (Chicago, 1944). They were developed in the light of the subsonic aircraft fleet in service to improve their environmental footprint and thus improve the public acceptability of air transport. These first SARPs set noise levels not to be exceeded that reflect the level of aircraft technology being planned at that time. Since then, the standard development has been following technological improvements and gradually more stringent limits for newly designed aircraft have been established. These new limits are therefore implicitly associated with aircraft noise levels that the public now agrees to accept.

6. The Authors of this paper consider that supersonic aeroplane projects should not be noisier than current and future subsonic aircraft in landing and take-off (LTO) operations. Indeed, over the past 50 years, the aviation sector has made considerable efforts to reduce noise pollution around airports. Granting less stringent noise limits would be a step backwards and would run the risk of extending dissatisfaction to all air transport. Beyond that, aviation's "license to grow" as a whole would be at stake if less stringent noise limits would be put in place for supersonic aeroplanes. Social acceptance of air transport and its development are linked to noise limits in force, which must be maintained whatever the aircraft type. The standard setting process cannot, therefore, be entirely separated from the political reality. In fact, CAEP receives its remit from the Council and Assembly and has a clear political direction from Assembly Resolution A39-1 to "take due account of the problems which the operation of supersonic aircraft may create for the public". Political realities and non-technical factors therefore have and will rightly continue to set the context within which the technical work of CAEP is conducted.

7. Early evidence available indicates that supersonic aeroplane projects will not be able to meet current noise limits of subsonic aeroplanes due to criteria that designers have set themselves while detailed information on HISAC (environmentally-friendly HIgh Speed AirCraft) preliminary study presented at the ICAO/CAEP/WG1/LTO Workshop#5, in Washington, 30 April to 4 May 2018, indicate that it could be possible to design a supersonic aeroplane that meets maximum permitted noise levels for subsonic aeroplanes, even with conventional engines. The Authors of this paper are of the opinion that internationally agreed environmental certification Standards are essential for the sustainable development of the aviation sector. Past development of subsonic noise standards has been effective at ensuring public acceptability of subsonic aircraft operations as one element contributing to the balanced approach to noise management. Therefore, the adoption of standards that would allow higher noise levels than subsonic aircraft does not guarantee the public acceptability of supersonic aeroplane projects in Europe. Such a situation would inevitably call into question the purpose of ICAO standards.

8. At the 39th ICAO Assembly, the importance of ensuring that no unacceptable situation for the public is created by sonic boom from civil supersonic aeroplanes in commercial service was reaffirmed[3].

9. With regard to sonic booms that would be perceived on the ground when the aircraft reaches and also maintains a supersonic speed over populated lands, pursuant to 39th Assembly Resolution A39-1, ICAO is attempting to reach international agreement on the definition of the expression "unacceptable situations for the public" and the establishment of the corresponding limits. Technical evidence shows that during the acceleration phases sonic boom levels will be of the same magnitude as those previously produced by Concorde in cruise. Such sonic boom levels led to the prohibition to fly at supersonic speeds over inhabited territories. As regards the cruise phase, the Authors of this paper consider that perception of sonic booms in populated areas would constitute a new form of nuisance, whatever their intensity.

10. Currently there are no civil supersonic aeroplanes operating commercially anymore and new market opportunities for supersonic aeroplanes must be assessed in light of their scope, quantity and effects on the environment. In this context, the European RUMBLE program contributes to the CAEP work. According to the CAEP work program, assessment of sonic boom public acceptance is expected by 2025, since it requires a low boom demonstrator aeroplane.

EMISSIONS AND CLIMATE IMPACT OF SUPERSONIC AEROPLANES

11. The provisions of Annex 16, Volume II, Chapter 3 applicable to supersonic aeroplanes emissions are outdated and need to be revised to avoid certifying a new product to this regulation and to provide an incentive to fit aeroplanes with best available environmental technology.

12. As for CO_2 emissions, since ICAO adopted a global Standard limiting emissions of subsonic jet aeroplanes, it seems to be essential to also subject supersonic aeroplanes to a standard, particularly as this new class of aircraft will have significantly increased fuel burn and therefore CO_2 emissions on both a per aircraft and per passenger basis, compared to existing aircraft. The absence of a Standard would place supersonic aeroplanes in a situation of unfair competition.

13. In addition, the full climate impact of supersonic air transport is likely to be different to subsonic aircraft, due to the higher altitudes at which these aircraft would operate. This includes impacts of particulates and NOx on stratospheric ozone depletion and ultraviolet radiation. The science of these effects is not well understood but represents an additional climate impact compared to subsonic aircraft.

[3] Assembly Resolution A39-1 Appendix G.

14. The Authors of this paper consider that the set of supersonic Standards under development should provide a consistent regulatory framework for environmentally friendly civil supersonic airplanes.

CONCLUSION

15. The environmental impact of civil supersonic aeroplane projects remains a major concern. The adoption of certification standards that would allow higher noise levels than those for current and future subsonic aeroplanes does not guarantee the public acceptability of supersonic aeroplane projects in Europe. The Authors of this paper consider that the environmental impact must be addressed holistically for noise and emissions before considering the introduction of supersonic aeroplane projects into the global air navigation system.

16. In doing so, ICAO cannot divorce itself from the political context. The political realities outlined above have and will rightly continue to set the context within which the technical work of CAEP is conducted.

— END —