

PROTECTION OF INFORMATION FROM SAFETY DATA COLLECTION SYSTEMS

Silverio Espinola

Marcus Costa

Daniel Maurino

Formatted: Spanish (Spain-Modern
Sort)

This article addresses the importance of protecting information from safety data collection and processing systems (SDCPS) in order to improve aviation safety. The article summarises the situation in international civil aviation regarding the protection of such information and describes action undertaken by ICAO on the subject.

BACKGROUND

International civil aviation's outstanding safety record is primarily due to three key factors: a) the dedication to safety by aviation organizations and their staff; b) a continuous learning process, based on the development and free exchange of safety information; and c) the ability to turn errors into preventive actions. It has long been recognized that endeavours aimed at improving contemporary civil aviation safety must build upon empirical data. There are several sources of such data available to civil aviation. In combination, they provide the basis for a solid understanding of the strengths and weaknesses of aviation operations.

For years, information from accident and incident investigations formed the backbone of activities aimed at improvements in equipment design, maintenance procedures, flight crew training, air traffic control systems, airport design and functions, weather support services, and other safety-critical aspects of the air transportation system. In recent years, the availability of technological means has led to an accelerated development of safety data collection, processing and exchange systems (hereafter referred to in the article, in combination with accident and incident investigation and reporting, as *safety data collection and processing systems or SDCPS*). SDCPS form the pillars of a safety management system (SMS), and generate information that is used to implement corrective safety actions and proactive long-term strategies.

A key difference within SDCPS concerns the human performance data each captures. Accidents and serious incidents are rare occurrences, often reflecting the linking of circumstantial factors. As a result, it is often difficult to uncover unsafe operational practices in time to deal with them appropriately, using information from the investigation of accidents and serious incidents exclusively. Furthermore, because accidents and incidents are failures of the aviation system, human performance data accessed through accident and incident investigations inevitably reflects unsuccessful system and human performance (i.e., *unmitigated* operational errors).

On the other hand, any typical aviation operation - just like any other human activity - involves frequent and minor but, most important, inconsequential errors (selecting wrong frequencies, dialling wrong altitudes, acknowledging incorrect read-backs, mishandling switches and levers, and so forth). Some errors are due to natural limitations in human performance, others are fostered by systemic shortcomings; most are a combination of both. The fact nevertheless remains that these frequent and minor errors contain the same damaging potential as rare and major errors captured through accident and incident investigations. However, such damaging potential is neutralized because: a) operational personnel employ successful coping strategies; and b) specific system defences fulfil their role and act as containment net. Emerging SDCPS capture successful coping strategies and well-performing systems defences. Simply put, they largely capture what works well in aviation operations.

From a systems safety perspective, in order to develop countermeasures to operational errors, it is essential to complement the lessons from failures accessed through accident and incident investigations with information about successful strategies and defences accessed through emerging SDCPS. These latter can be grouped into three broad categories, depending on the method employed to collect the safety data: a) self-reporting; b) electronic capture; or c) direct observation. These systems are, with few exceptions, voluntary and, without exception, confidential and non-punitive. Furthermore, because they constantly collect data on a daily basis, emerging SDCPS generate a great volume of information to support safety actions and long-term strategies.

Industry attempts to collect safety data through self-reporting safety data collections systems include, among others, examples such as the Aviation Safety Action Programme (ASAP). Flight data analysis (FDA) programmes such as the Flight Operations Quality Assurance (FOQA) Programme is an example of a safety data collection system based on electronic capture of safety data. Lastly, the Line Operations Safety Audit (LOSA) and the Normal Operations Safety Survey (NOSS) are examples of SDCPS that capture safety data through direct observations of flight crews or air traffic controllers respectively by expert, especially trained observers. All these systems permit recording successful system and human performance (i.e., *mitigated* operational errors), and they lead to more complete conclusions to develop countermeasures to human error.

THE INTERNATIONAL SITUATION

SDCPS have allowed civil aviation to gain a deeper understanding of operational errors: why they happen, what can be done to minimize their occurrence, and how to contain their negative impact on safety. It remains undisputed that the majority of operational errors in aviation are inadvertent: well-trained, well-intentioned people make errors while maintaining, operating, or controlling well-designed equipment. For those rare situations where errors are a result of willful acts, substance abuse, sabotage or violations, enforcement systems in place ensure that the chain of accountability remains unbroken. This dual approach, combining enhanced understanding of inadvertent operational errors with appropriate enforcement of rules in cases of misconduct, has served civil aviation well in terms of safety, while ensuring that there are no harbours for violators.

Recent years, however, have shown a trend in civil aviation when dealing with operational errors leading to occurrences, in that information from SDCPS has been used for disciplinary and enforcement purposes, as well as admitted as evidence in judicial proceedings. These proceedings have also resulted in criminal charges being brought against individuals involved in such occurrences. Bringing criminal charges into aviation occurrences resulting from inadvertent operational errors may hinder the development and free exchange of safety information which is essential to improve aviation safety, with a potential adverse effect on it.

A number of initiatives within the international civil aviation community have attempted to address the protection of SDCPS. However, given the sensitivity of the question at hand, a framework that provides unity of purpose and consistency among civil aviation's efforts is essential. Efforts to ensure the protection of safety information must strike a very delicate balance of interests between the need to protect safety information, and the responsibility to administer justice. A cautious approach should be taken in this regard to avoid making proposals which might be incompatible with laws pertaining to the administration of justice in Contracting States.

Within ICAO, a number of provisions addressed the protection of certain sources of safety information. These included:

- Assembly Resolution A33-17; *Non-disclosure of certain accident and incident records*, that urges States to examine and if necessary adjust their laws, regulations and policies to protect certain accident and incident records in compliance with paragraph 5.12 of Annex 13, and instructs ICAO to develop guidance materials to support States in this respect;
- Assembly Resolution A33-16, *ICAO Global Aviation Safety Plan (GASP)*, that instructs ICAO to participate in efforts by States to improve safety information reporting and exchange, with due consideration to protection of privileged information; urges States to examine and, if necessary, adjust relevant legislation; and instructs ICAO to provide guidance materials to support States in this respect;
- Assembly Resolution A31-10, *Improving accident prevention in civil aviation*, that urges States to implement voluntary and non-punitive reporting systems;
- Annex 13 — *Aircraft Accident and Incident Investigation*, paragraph 5.12, that establishes that statements from persons, communications between persons that were involved in the operation of the aircraft, medical and private information, cockpit voice recordings and transcripts, and opinions expressed in the analysis of information shall not be made available for purposes other than accident and incident investigation, unless the appropriate authority for the administration of justice in the State determines that their disclosure outweighs the adverse domestic and international impact such action may have on that or any future investigations;
- Annex 13, paragraph 8.3, that establishes that voluntary incident reporting systems shall be non-punitive and sources of information shall be protected; and
- Annex 6 — *Operation of Aircraft*, paragraph 3.2.4, that establishes that flight data analysis programmes shall be non-punitive and shall contain safeguards to protect source(s) of data.

The provisions in Assembly Resolution A33-17 and Annex 13, paragraph 5.12, address the protection of information from certain accident and incident records listed in Annex 13, paragraph 5.12, in particular, the provisions related to the cockpit voice recorder and their transcripts. The provisions in Assembly Resolution A33-16, Assembly Resolution A31-10, Annex 13, paragraph 8.3 and Annex 6, paragraph 3.2.4, address self-reporting and electronic safety data collection systems. ICAO provisions do not address direct observation safety data collection systems.

ICAO provisions protecting certain accident and incident records are explicit regarding their admissibility in judicial proceedings. The same explicit protection is not evident for information from emerging SDCPS. In the absence of explicit wording such as in Annex 13, 5.12, information from safety data collection systems is protected by agreements within operators or service providers. The legal protection afforded to the information from SDCPS by such agreements, within different judicial systems in Contracting States, is difficult to ascertain.

Few States have promulgated national legislation protecting the information from self-reporting safety and electronic safety data collection systems. In some States, legal reform may be required to accommodate such legislation. The protection of the information from direct observation safety data collection systems is not presently addressed by legislation in any State. It can therefore be concluded that the fact that current ICAO provisions, as well as international and national legislations do not sufficiently address the protection of the information from SDCPS other than accident and incident records, may result in inadequate protection being provided to such information in the national legislation of many States, and that developments dictate the need to generate legal guidance that encompasses the protection of all relevant SDCPS. Such legal guidance should be the product of international consensus, and compatible with the cautious approach already discussed

ACTION BY ICAO

The 35th Session of the Assembly considered the subject of the protection of sources and free flow of safety information and adopted Resolution A35-17: Protecting information from safety data collection and processing systems in order to improve aviation safety. This Resolution instructed the Council “to develop appropriate legal guidance that will assist States to enact national laws and regulations to protect information gathered from all relevant safety data collection and processing systems, while allowing for the proper administration of justice in the State.”

As a first step in developing the legal guidance called for in Assembly Resolution A35-17, ICAO requested some States to provide examples of their relevant laws and regulations relating to the protection of information from SDCPS. Subsequently, ICAO conducted an analysis of the material received from States, seeking common threads and conceptual points from the laws and regulations provided. The legal guidance that resulted takes the form of a series of principles that have been distilled from such laws and regulations.

Consideration was given to the most effective means of disseminating this legal guidance. As the guidance material primarily relates to two chapters of Annex 13 — *Aircraft Accident and Incident Investigation*, it was believed that an Attachment to Annex 13 would be an appropriate location. As a consequence, Notes were proposed to be added to Chapters 5 and 8 of Annex 13, with a further Note added to paragraph 3.2.4 of Annex 6 — *Operation of Aircraft, Part I — International Commercial Air Transport — Aeroplanes*, referring to the legal guidance contained in new Attachment E to Annex 13.

THE LEGAL GUIDANCE

The guidance is aimed at assisting States enact national laws and regulations to protect information gathered from SDCPS, while allowing for the proper administration of justice. The objective is to prevent the inappropriate use of information collected solely for the purpose of improving aviation safety.

Bearing in mind that States should be allowed the flexibility to draft their laws and regulations in accordance with their national policies and practices, the legal guidance takes the form of a series of principles that can be adapted to meet the particular needs of the State enacting laws and regulations to protect safety information. A brief outline of the guidance follows.

The legal guidance includes **general principles** stating that:

- The sole purpose of protecting safety information from inappropriate use is to ensure its continued availability so that proper and timely preventive actions can be taken and aviation safety improved;
- It is not the purpose of protecting safety information to interfere with the proper administration of justice in States;
- National laws and regulations protecting safety information should ensure that a balance is struck between the need for the protection of safety information in order to improve aviation safety, and the need for the proper administration of justice;
- National laws and regulations protecting safety information should prevent its inappropriate use, and
- Providing protection to qualified safety information under specified conditions is part of a State's safety responsibilities.

The guidance includes **principles of protection**, as follows:

- Safety information should qualify for protection from inappropriate use according to specified conditions that should include, but not necessarily be limited to: the collection of information was for explicit safety purposes and the disclosure of the information would inhibit its continued availability;
- The protection should be specific for each SDCPS, based upon the nature of the safety information it contains;
- A formal procedure should be established to provide protection to qualified safety information, in accordance with specified conditions;
- Safety information should not be used in a way different from the purposes for which it was collected; and
- The use of safety information in disciplinary, civil, administrative and criminal proceedings should be carried out only under suitable safeguards provided by national law.

The guidance provides that exceptions to the protection of safety information should only be granted by national laws and regulations when:

- there is evidence that the occurrence was caused by an act considered, in accordance with the law, to be conduct with intent to cause damage, or conduct with knowledge that damage would probably result, equivalent to reckless conduct, gross negligence or wilful misconduct;
- an appropriate authority considers that circumstances reasonably indicate that the occurrence may have been caused by conduct with intent to cause damage, or conduct with knowledge that damage would probably result, equivalent to reckless conduct, gross negligence or willful misconduct; or
- a review by an appropriate authority determines that the release of the safety information is necessary for the proper administration of justice, and that its release outweighs the adverse domestic and international impact such release may have on the future availability of safety information.

The guidance also addresses the subject of **public disclosure**, proposing that, subject to the principles of protection and exception outlined above, any person seeking disclosure of safety information should justify its release. Formal criteria for disclosure of safety information should be established and should include, but not necessarily be limited to, the following:

- disclosure of the safety information is necessary to correct conditions that compromise safety and/or to change policies and regulations;
- disclosure of the safety information does not inhibit its future availability in order to improve safety;
- disclosure of relevant personal information included in the safety information complies with applicable privacy laws; and
- disclosure of the safety information is made in a de-identified, summarized or aggregate form.

The guidance discusses the **responsibility of the custodian of safety information**, proposing that each SDCPS should have a designated custodian. It is the responsibility of the custodian of safety information to apply all possible protection regarding the disclosure of the information, unless:

- the custodian of the safety information has the consent of the originator of the information for disclosure; or
- the custodian of the safety information is satisfied that the release of the safety information is in accordance with the principles of exception.

Lastly, the guidance discusses the protection of recorded information, and considering that ambient workplace recordings required by legislation, such as cockpit voice recorders (CVRs), may be perceived as constituting an invasion of privacy for operational personnel that other professions are not exposed to, proposes that:

- subject to the principles of protection and exception above, national laws and regulations should consider ambient workplace recordings required by legislation as privileged protected information, i.e. information deserving enhanced protection; and national laws and regulations should provide specific measures of protection to such recordings as to their confidentiality and access by the public. Such specific measures of protection of workplace recordings required by legislation may include the issuance of orders of non-public disclosure.

— END —