In Service Safety at Boeing

Simon Lie
Technical Fellow, Air Safety Investigation
Boeing Commercial Airplanes

Simon Lie is an Technical Fellow and Senior Air Safety Investigator for Boeing Commercial Airplanes. He has been with Boeing since 1989.

Simon received his SB and SM degrees from MIT where his graduate work focused on impact damage and residual strength of composite sandwich structures. At Boeing, Simon has worked in a number of areas including flight line engineering, structural loads analysis, avionics design and, most recently, accident investigation. Simon joined Boeing's accident investigation department in 2000 and has since led the company's involvement in more than 20 major investigations.

In addition to his engineering and aviation background, Simon also has experience as a firefighter and emergency medical technician which provides a different insight into emergency operations and incident command.

Introduction

With the publication of ICAO Annex 19 in 2013, talk about Safety Management Systems (SMS) has become common place in the commercial aviation industry and is the theme of ISASI's 45th annual seminar in Adelaide, Australia.

The basic tenets and theories of safety in commercial aviation have of course been around for years. SMS provides a framework to catalog the various activities and best practices, and may also be considered a common taxonomy that can be used to document, monitor and measure safety efforts.

Commercial aviation is a highly cooperative industry with many participants who together have produced the safest form of transportation in the history of the world. Each participants has a part to play in keeping the global air transportation system safe. Some of these roles are obvious, such as the role of air traffic services in keeping airplane separated, while some are less obvious. An airframe manufacturer has an obvious role to play in the initial engineering design and manufacture of the airplane. What may be less obvious is the role manufacturers play in helping ensure the safety of in-service fleets.

This paper describes the Boeing In-Service Safety Process from the perspective of Safety Management Systems. Boeing's Safety Process has been developed over the five decades the company has been producing and supporting commercial airplanes. Although our in-service safety process predates the publication of the ICAO SMS Manual, there is a very good fit between the two. Both set out to accomplish the same ends in much the same manner.

SMS Overview

ICAO's SMS framework has four components covering twelve elements. Each SMS component is important and cannot function effectively in insolation from the others. It is not my intention to review each of these elements in detail, but I do want to list them here as certain elements will be referred to later when describing the Boeing Safety Process.

This paper is focused on three elements: 2.1 Hazard Identification, 2.2 Safety Risk Assessment and Mitigation, and 4.2 Safety Communication as they apply within Boeing, particularly in our support of in-service fleets. The effective application of these elements to the in-service fleet requires interaction and cooperation between manufacturers, operators and regulators.

Table 1: ICAO SMS Components and Elements

1. Safety policy and objectives
   - 1.1. Management commitment and responsibility
   - 1.2. Safety accountability
   - 1.3. Appointment of key safety personnel
   - 1.4. Coordination of emergency response planning
   - 1.5. SMS documentation
2. Safety risk management
   - **2.1. Hazard identification**
   - **2.2. Safety risk assessment and mitigation**
3. Safety assurance
   - 3.1. Safety performance monitoring and measurement
   - 3.2. The management of change
   - 3.3. Continuous improvement of the SMS
4. Safety promotion
   - 4.1. Training and education
   - **4.2. Safety communication**

In the spirit of the ICAO Annexes, we begin with some definitions.

Safety and Airworthiness

Safety and airworthiness are related but distinct concepts. Fortunately, Annex 19 provides a definition of "Safety".

> *The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level.*

In short, safety means acceptable risk, that is, the absence of undue risk. But what is acceptable risk? The risk of an undesirable outcome has two factors – the severity and probability. Acceptability lies in the balance between the two. Referring to the ICAO SMS Manual:

> *It is important to note that the acceptability of safety performance is often influenced by domestic and international norms and culture. As long as safety risks are kept under an appropriate level of control, a system as open and dynamic as aviation can still be managed to maintain the appropriate balance between production and protection.*[1]

Aviation authorities define a specific relationship between severity and probability to set the level of acceptability, setting the border between safe and unsafe. For example, probability of a catastrophic accident must be no more than extremely improbable, typically defined as 10^{-9} per flight or flight hour.

Annex 8 is devoted to "Airworthiness," although the term does not appear in the definitions section. Section 3.2.1 of Annex 8 reads as follows.

> *A Certificate of Airworthiness shall be issued by a Contracting State on the basis of satisfactory evidence that the aircraft complies with the design aspects of the appropriate airworthiness requirements.*

In short, airworthiness means the aircraft complies with requirements[2]. Of course, the requirements themselves were developed to ensure safety, so the concepts of safety and airworthiness are closely related.

- Safety = acceptable risk
- Airworthy = compliance with requirements and conformity with approved design

Keeping these definitions separate will become important because an undesired event may be a safety issue without being an airworthiness issue and vice-versa[3].

Product Life Cycle

[1] ICAO Doc 9859, Safety Management Manual (SMM), section 2.1.2

[2] Two similar terms are used at Boeing, compliance and conformity, but with different meanings. Both terms relate to "Type Design", which is the definition of a particular model airplane as described by engineering drawings and other supporting documents. The type design *complies* with the applicable airworthiness requirements and regulations. A specific serial number airplane that is manufactured *conforms* to the type design.

[3] Consider an information placard that is designed and certified with dark gray letters on a white background, but was manufactured with black letters on a while background. That issue could be an airworthiness issue (it does not conform to the approved design), but may not be a safety issue (does not create undue risk). A related concept is the FAA's Equivalent Level of Safety (ELOS) doctrine described in FAA Order 8110.112.

Broadly speaking, there are 4 stages in the life cycle of an airplane:

- Design
- Production
- Validation
- In-Service (including maintenance and modification)

While the steps are listed in generally chronological order, the flow through each step is not always linear or orderly, as when design enhancements or new features are added to existing models. We will now review how safety is ensured during each step in the life cycle.

Safety during Design

During the design portion of the life cycle, the safety focus is on identification of the correct requirements and compliance to those requirements. Some of these requirements are imposed by commercial aviation regulators, such as FARs published by the FAA[4], CSs published by EASA[5] or CASRs published by CASA[6]. All of these regulations are instances of States fulfilling their obligations under ICAO Annex 8. Other requirements include Boeing-specific requirements which go above and beyond the minimum acceptable levels set by the government regulators. The body-of-knowledge which comprises these requirements benefits from lessons learned over many decades[7].

Boeing's design phase ensures safety in three steps: identifying and documenting the correct requirements, designing the airplane in accordance with those requirements, and validating that the requirements have been met. During the Design phase, many analyses are performed, including a Functional Hazard Assessment (FHA), Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). Collectively, this work is often referred to as the Safety Analysis.

The FHA contains of a list of the types of failures which might affect a system and the resulting severity of the associated consequence. For example, in the design of a landing gear system, we might determine that failure of the landing gear to retract after take-off has only minor consequences in specific circumstances.

The FMEA lists each component of the system and different ways it might fail (e.g. a wire might fail as an open circuit, might short to ground or might short to a power source). That's the "Failure Modes" part of the work. The "Effects" analysis looks at the consequence of the particular failure mode at the airplane level taking into account multiple factors such as system redundancy, degraded functionality, and increased crew workload.

Finally, the FTA considers the failures or combinations of failures needed to result in the different failure modes and predicts the probability of each such failure. If the probability is inappropriate for the severity (in other words, if the risk is unacceptable), then a change is made to mitigate that risk. Hazards that are identified might be mitigated by one or more of several methods including the following (methods higher on the list are generally preferred, but may not always be possible):

[4] FARs are Federal Aviation Regulations published by the US Federal Aviation Administration
[5] CSs are Certification Specifications published by the European Aviation Safety Agency.
[6] CASRs are Civil Aviation Safety Regulations published by the Australia Civil Aviation Safety Authority.
[7] An excellent website describing safety lessons learned and how regulations have evolved is maintained by the US FAA at: http://lessonslearned.faa.gov

- Eliminate hazards from design
- Incorporate safety devices
- Provide warnings devices
- Develop procedures and training avoid the situation

Returning to the SMS Framework and the three specific elements identified earlier: The FMEA described above, together with the FHA are the chief means by which hazards are identified (Element 2.1 Hazard Identification). The FHA determines the severity of a hazard while the FTA determines the probability, thereby determining the risk (Element 2.2 Safety risk assessment and mitigation). Collectively the safety analysis documents communicate the safety actions taken (Element 4.2 Safety communication).

While the safety analyses currently in use during the design phase were developed to meet certification requirements predating SMS, they serve to accomplish the same goals set forth in ICAO Annex 19.

Safety during Production

Once a design is complete, production can begin. The key to safety assurance during production[8] is quality, while the key to quality is consistent conformity to the approved type design. Long before we began thinking in terms of safety management systems, an entire industry was developed that is devoted to quality improvements through consistency.

At its core, our quality system minimizes and detects inconsistent or non-conforming parts or processes. On occasion however, a manufacturing error may go undetected. Alternately, and perhaps more commonly, a change made to a process or tool may have an unintended consequence that is not apparent until well after the change is made. Similarly, our suppliers have their own quality systems performing much the same role. Should a supplier escapement occur, Boeing is notified that potentially non-conforming material or parts may have been delivered or that new information shows that a part may not function properly. In all of these situations, the non-conformance is documented and evaluated to determine if a formal review by the in-service safety process (described later) is required.

Safety during Validation

In addition to being a manufacturer of airplanes, Boeing is also an operator. We fly our airplanes on test flights both during initial certification and also as part of the production process for each airplane we build.

This part of our operations is most like those of an airline, except that many of our test flights exercise safety systems that will never be needed in the life of the airplane -- or possibly even in the life of the fleet.

Prior to each test flight, a formal review take place during which the proposed testing and potential outcomes are discussed, the associated hazards are identified, and any necessary mitigations are decided upon.

[8] In this context safety assurance during production refers to the risks related to the use of finished airplanes or services in commercial aviation. This is distinct from worker safety which we also hold dear at Boeing and manage separately under our “Go for Zero” program.

For some tests which are considered high-risk (e.g. flutter testing early in the flight test program), risk mitigation can include steps such as using only minimum crew equipped with parachutes and an egress route. Our commercial airplanes do not have egress routes as part of the basic design, so flight test specific mechanisms must be designed and built for this purpose. Of course, these mechanisms must then have their own safety analysis as part of their design and manufacture.

In some cases, an event occurs during flight test which may have broader implications for the in-service fleet. For this reason, each technical log entry is evaluated against the same criteria applied to in-service events (described in the next section). Events meeting any of the criteria are evaluated for safety implications using the same process as for in-service event. In other words, Boeing flight test operations are viewed as any other in-service operation, albeit ones that deliberately explores the corners of the flight envelope.

In-Service Safety

The Boeing In-service safety process has evolved over the past few decades and it built around the same principles which appear in the SMS elements: hazard identification, risk assessment and mitigation, and safety communication. The safety process itself can be characterized by the following steps.

- Issue Identification
- Safety Decision
- Issue Resolution

A diagram of the process is shown in Figure 1. The above-listed steps occur left-to-right, along with the ICAO Annex 19 SMS equivalent.

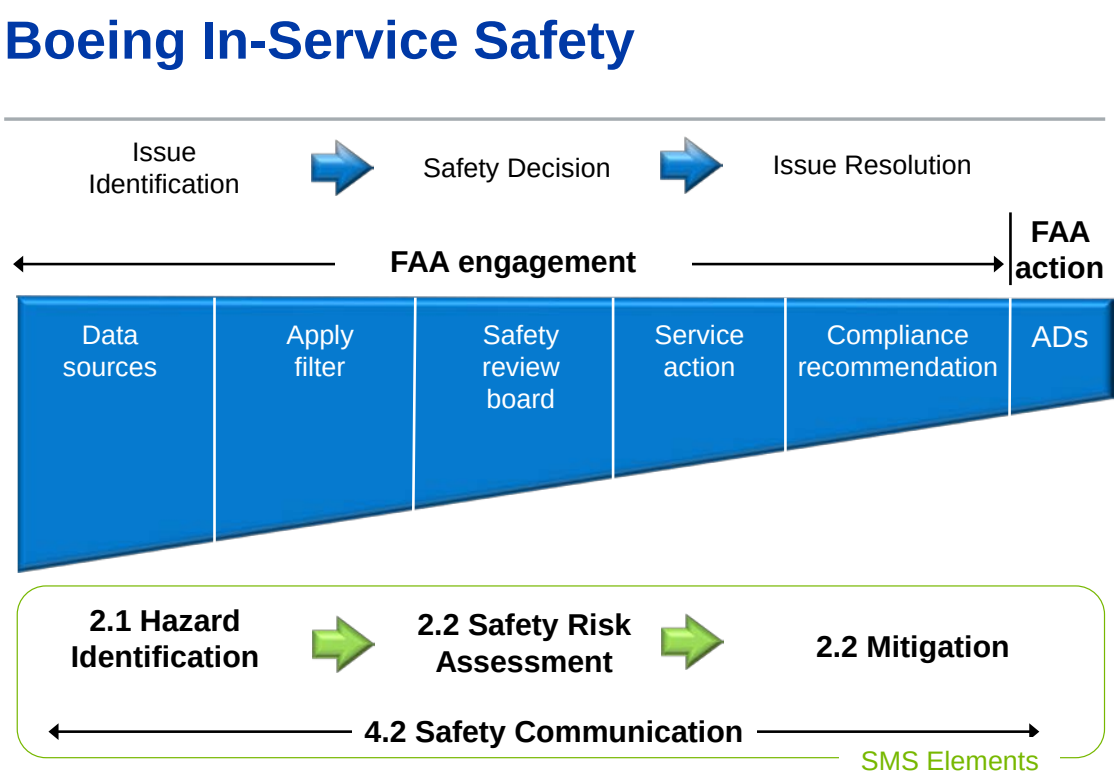

Figure 1 – The Boeing In-Service Safety Process. From left to right, the diagram depicts Issue Identification, Safety Decision, Issue Resolution as well as the associated ICAO Annex 19 Safety Elements.

Issue Identification

While some of the information needed to identify hazards is available within Boeing, much of the data needed comes from either airline operators or safety organizations. Because operators generate the vast majority of flight hours and flight cycles experienced by the fleet, it should come as no surprise that operators are the richest source of data that we have for unexpected events which might indicate or presage a hazard.

Boeing relies on operators to report incidents and other in-service events so they can be evaluated for safety implications. The safety process begins with the daily filtering of the hundreds of reports sent in by operators.

FAR 21.3 requires that manufacturers notify the FAA when certain events occur in the fleet[9]. To meet these requirements, Boeing has implemented a Continued Operational Safety Program (COSP) which includes all of the FAR 21.3 criteria as well as others.

[9] Examples include "Fires caused by a system or equipment failure, malfunction, or defect", "any engine failure", and "a brake system failure caused by structural or material failure during operation" and numerous other conditions.

These reporting criteria also serve as the first filter to determine which events may require further review for safety implications. A second filter is then applied to determine which events constitute potential safety issues that will be formally reviewed by Boeing's Safety Review Board.

It is important to point out that although much of the input to the safety process is in the form of *events*, the safety process itself is *issue* based. Often there is a one-to-one correspondence between event and issue, but that is not always the case. For example, a particular event may not constitute unacceptable risk, but several similar events might indicate there's an issue which requires formal evaluation.

On the other hand, one event can lead to the identification of multiple issues. This is a natural consequence of the fact that undesirable outcomes usually occur because multiple layers of safety barriers were breached.

In addition to operator-reported events, the safety process also receives input from a number of other sources -- including findings and safety recommendations from accident and incident investigations and internal Boeing organizations. Lastly, any Boeing employee can submit a potential airplane safety concern for evaluation. Together these sources of data and filtering criteria accomplish the intent of SMS Element 2.1, Hazard Identification.

The Safety Decision

Once a potential safety issue has been identified, the next decision is a simple one – is it a safety issue? In other words, does it create unacceptable risk? The process of finding an answer to that question is at the heart of the Boeing In-Service Safety Process.

The safety decision itself is made by a safety review board (SRB) using consistent processes and procedures. One of the key features of the decision-making process is that the board is responsible for deciding only if an issue is or is not a safety issue. Specifically excluded from the board's responsibilities are mitigating actions or decisions about whether an issue does or does not raise questions regarding airworthiness[10]. This allows the board to focus exclusively on the question of risk. Safety decisions are made at regularly scheduled board meetings. In exceptional cases, an "out-of-sequence" meeting will be held if an issue arises which warrants an immediate decision.

Each issue is presented to the board in a standard format that includes details of the issue, a risk assessment (severity and probability), and a recommendation to the board for "safety" or "not safety". For those issues that carry a safety recommendation, the presentation also includes a recommended corrective action compliance period to ensure the risk remains acceptable until the hazard is mitigated.

Within the presentation is contained the Safety Risk Assessment portion of SMS element 2.2, including both severity and probability aspects. The SRB consider two levels of risk: Airplane Safety and Personal Safety. An airplane safety risk is one for which the top level event is a catastrophic accident. As in the design phase, the acceptable level of probability for a catastrophic accident resulting from a specific safety issue is extremely improbable (typically 10^{-9} per flight or flight hour). Personal safety risks are those which could result in injury to a limited number of people (passengers, crew, maintenance personnel or members of the public), but do not create risk at the airplane level. An example of a

[10] Here as earlier, the term airworthiness is used to mean compliance with the regulations and conformance with type design data, as distinct from safe or unsafe.

personal safety issue might be sharp edges or jam points on a seat mechanism which could result in passenger injury. The probability level used to evaluate personal safety issues is extremely remote (typically 10^{-7} per flight or flight hour).

The presentation for the board is prepared by the subject matter experts (SMEs) most knowledgeable about the issue with assistance and guidance from the Aviation Safety organization, which is the custodian of the overall safety process. At the meeting, a SME presents the issue to the board, answers questions and participates in discussion. In addition to the presenting SME, experts from other disciplines will be available to answer questions that arise and participate in the discussion.

The board's raison d'être is the safety decision itself, which is taken as a vote. Voting members come from various engineering, flight operations, fleet support and safety departments within the company. One noteworthy feature of the voting process is that any single vote for "safety" results in a board decision of "safety". In other words, a vote of "not safety" must be unanimous, or else the result is "safety".

It should be noted there that a decision of "not safety" does not mean the matter will be dropped with no further action taken. A "not safety" issue may be causing delays or other disruptions at operators and therefor are taken to resolve the issue. All of this portion of normal fleet-support activities takes place separately from the Safety Process.

During our safety process, we remain engaged with the FAA from hazard identification all the way through to mitigation, including invitations for the FAA to attend every SRB meeting. Although the FAA has its own safety-decision making process, it is our joint goal to achieve consistency in safety decisions between the two organizations as well as consistency in the required mitigating action[11]. The open nature of the safety process and FAA engagement is one example of SMS element 4.2, Safety Communication.

In summary, the safety decision itself is made by a safety review boards representing various viewpoints through a voting process in which a single vote for safety can prevail. As a participant in SRB meetings, I have found that presentations by highly skilled subject matter experts on technical issues along with the singular focus on safety by all present representing varied viewpoints are some of the most interesting meetings I attend and demonstrate that Boeing's commitment to safety is the top priority.

Issue Resolution

As described above, the safety decision is intentionally separated from issue resolution. Once a safety decision is made, then the risk mitigation process begins. Issue resolution in managed by our Service Related Problem (SRP) process. The SRP process is a rigorous process that tracks issues from initial identification through to resolution.

The SRP process is also used to resolve non-safety problems which have an economic effect on the fleet. However, safety SRPs have first priority and will be described here. An SRP manager is appointed who leads a team to first define the scope of the problem and then determine root cause and most appropriate solution taking into account effectiveness, timeliness, complexity and other factors. The

[11] As a manufacturer, Boeing can recommend that operators implement actions to address safety issues, while the FAA as regulator can mandate such action. There have been cases where Boeing recommends one course of action and the FAA later mandates a slightly different action. It is our desire such situations be avoided.

timing of the mitigating action is determined by the risk assessment conducted in preparation for the SRB presentation. The severity and probability calculations determine an acceptable time to implement mitigating actions in the fleet before the risk rises to an unacceptable level. In some cases, interim actions such as inspections or temporary operating procedures are necessary to mitigate the risk before the final action is released. If the mitigating action involves a change to the airplane or special inspection requirements, Boeing will typically issue an Alert Service Bulletin to the affected fleet. This is one of three levels of service bulletins issued by Boeing. The others are Special Attention and Standard. Special Attention bulletins are often used for personal safety issues and may also be used for airplane safety issues for which the time to accumulate undue risk is lengthy. Each service bulletin contains a background section which describes the reason for the bulletin and the consequence that could occur if the bulletin is not implemented. This is another of the ways in which we accomplish SMS Element 4.2 Safety Communication -- we are conveying safety-critical information, explaining why particular safety actions are taken and explaining why safety procedures are introduced or changed.

Summary

While the application of SMS to airframe manufacturers is relatively new, the underlying safety principles and methodologies contained within SMS are equivalent to the safety processes that have been developed over the past several decades and are currently in place at Boeing. In particular, the In-Service Safety process used at Boeing maps directly to three elements of the ICAO Annex 19 safety framework: 2.1 Hazard Identification, 2.2 Risk Assessment and Mitigation, and 4.2 Safety Communication. As can be seen from the above description of the process, In-Service Safety, also called Continued Airworthiness, relies on the cooperative efforts of manufacturers, operators and regulators to ensure the continued future safety of the global air transportation system.

