A Systems-Based Model and Processes for Integrated Safety Management Systems (I-SMS)

Diogo Silva Castillo

A SYSTEMS-BASED MODEL AND PROCESSES FOR INTEGRATED SAFETY MANAGEMENT SYSTEMS (I-SMS)

Diogo Silva Castilho

Massachusetts Institute of Technology

Boston - MA

The study of the vulnerabilities of a system is often organized in a hazard analysis. Methods based on systems thinking are relevant tools to analyze the operation of modern products. The purpose of this research is to develop, implement, and validate a systems-based model for aviation Safety Management Systems (SMS) incorporating the treatment of collected data to foster the effectiveness of mitigating measures over time. The model uses data monitoring systems, management of change reports, flight inspections, voluntary reports, and other sources as input messages to an Active Hazard Analysis. The new requirements, constraints, and the preventing and mitigating measures are organized and delivered timely to the operators. The analysis on unstable approaches found contributions to documentation and procedures in practice. In accordance with SMS standards, the new framework provides organized safety information for management, fostering better planning on the use of workforce and resources.

Complex operations defy cognitive limitations. Safety-critical systems face accidents when these limits are unknown or ignored. A careful hazard analysis provides the knowledge that is necessary to reduce the risks. However, in dynamic systems, experience could generate negative learning, and even a thorough knowledge of the initial condition in which the system is delivered is not enough to guarantee safe operations.

The lifetime of an aircraft is expected to be long. A new airliner might endure more than four decades of operation. Throughout its lifetime, different generations of pilots, flight attendants, and mechanics will operate all the equipment developed for the system. This system comprised of hardware, software, and operators with different cultures will change over time because the environment and the mindset of operators will change. Technology will impact operations as upgrades of components, new functionalities, and different levels of automation are implemented. The challenge becomes to assure safety for operations when assumptions made at the beginning of the project are no longer valid.

The first efforts for hazard analysis should start during ConOps (Concept of Operations). In this phase, engineers need to make assumptions about how operators will interact with the product, and some of these assumptions will become obsolete. For example, the Boeing 777 entered into service in 1995. Back then, it would be impossible to imagine that airlines would be using electronic flight bags (EFB) or tablets[1]. It is easy to believe that this is a natural evolution

[1] EFBs and off-the-shelf tablets are accepted to be integrated to the dashboard to substitute all paper charts and manuals (FAA InFO, 2011)

in hindsight, but there was no smartphone when the aircraft was certified. The operational lifetime needs to be used to update the assumptions previously made, and consequently, the hazard analysis.

Safety Management Systems

The concept of an SMS (Safety Management System) was introduced in commercial aviation as a formal, top-down, organization-wide approach to manage safety risk and assure the effectiveness of safety risk controls. This perspective aims to make aviation even safer, but the processes within SMS leave room for improvement. It does consider software controlled systems and higher levels of automation, but it fails to proactively monitor the impacts of human factors and changes in the environment. It focuses on risk assessment (accident prediction) (FAA, 2016) rather than using a hazard analysis for accident prevention.

SMS is a new requirement for air operations, maintenance, and air traffic services. Annex 19, the document that formalized this initiative, is the first new ICAO (International Civil Aviation Organization) Annex to come out in over thirty years. All aviation organizations must show compliance with Annex 19 before November 2019, but there are a variety of ways to do it. The ICAO and the FAA offer manuals to guide Safety Risk Management (SRM) and Safety Assurance (SA), but there is no orientation on the use of hazard analysis at the organizational level.

There are tools based on Systems Theory that could be added to SMS. These techniques consider the operator's behavior to be the result of social, psychological and even environmental conditions. The mapping of actions applied to a controlled process and the analysis of the feedback that the operator is receiving provide a qualitative understanding of the real issues behind the unsafe behavior.

This research links systems engineering and management actions that are necessary to comply with SMS. In this context, we answered the following research question: How to apply systems-based concepts to collect aviation operational data and update a hazard analysis? The solution was the introduction of the Integrated Safety Management System (I-SMS) as a model to guide safety managers using concepts from Systems Engineering.

The purpose of this research was to develop and implement a systems-based model of safety management incorporating the treatment of collected data to foster the effectiveness of mitigating measures over time. This model has a general framework that the safety manager can adjust to each specific system.

This model work as a method to monitor safety in operations to maintain a higher level of safety by using an active hazard analysis. The foundation for the I-SMS is STAMP (Systems-Theoretic Accident Model and Processes), which is based on Systems Theory. STAMP is a modern model of causation that has proven to be successful in aviation. I–SMS is the model that improves the completeness on the application of STAMP techniques.

Systems-Theoretic Process Analysis (STPA) is the hazard analysis technique based on STAMP (Leveson, 2011). STPA covers not only the accidents caused by component failures but also the ones caused by a faulty interaction between components of a system that are each functioning properly, as a consequence of system design flaws. It recognizes safety and security

as emergent properties of a complex system caused by the interaction of its components. The main characteristic of security is the malicious intentions behind control actions. However, safety is a more general term, and it is affected by both well-intended operators and the ones attacking the system. The STPA is complemented by organizing assumption-based leading indicators (Leveson, 2015) to register the reasoning behind performance indicators.

Integration of Hazard Analysis and SMS

Proactive management requires effective communication and monitoring activities. The proposed solution is the use of a structure that puts the hazard analysis at its core to feed the decision making of higher hierarchical levels with new indicators and their trends.

The hazard analysis performed during system development becomes the structure that will be in constant evolution as it is revisited during the whole lifetime of a system. The output of this active hazard analysis adapts the organization to a dynamic reality. The general framework of the I-SMS is presented in figure 1.

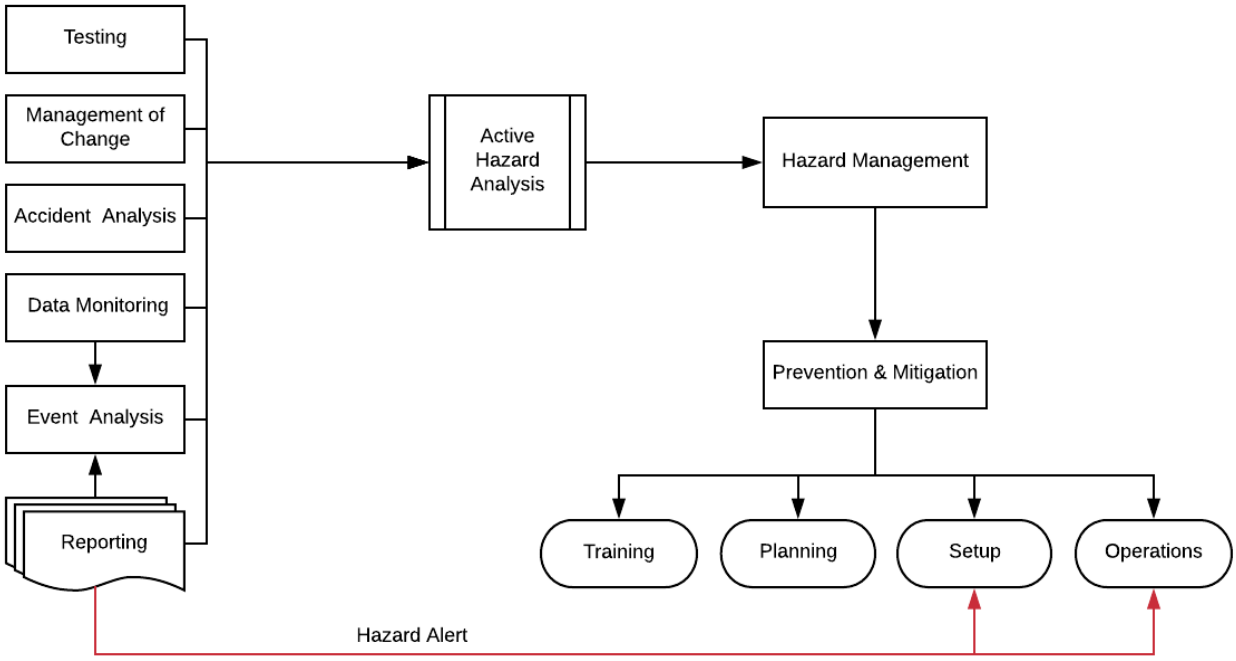

***Figure 1*. I-SMS general framework.**

On the left side, there are many different sources of input to the Active Hazard Analysis. The verification and validation tests become opportunities to add to the hazard analysis the details that developers did not consider when the product was just an abstract idea. When the system is already delivered and operating, changes initiate a process that requires revisiting the hazard analysis to avoid surprises. Incidents and accidents are seen as potential learning events. Also, the system must be open to voluntary contributions. The stakeholders' participation regarding hazardous conditions works both to enhance the system and to foster a safe attitude, keeping the organization awareness aligned with its culture.

On the right side, the output of the active hazard analysis feeds the hazard management and its preventive and mitigating actions that update the system's information flow, bringing it to a safer state. However, changing the documentation without understanding the operator's needs and difficulties is not effective management. It is essential to apply the mitigating measures considering how and when critical information is delivered to operators because it will be better assimilated if presented at a proper time.

A manager must guarantee that the information generated by the active hazard analysis will arrive at the desired destination, communicated to and understood by everyone who should have it, and applied to the system. Those tasks demand an observant manager to assure that all previous work is effective. Without monitoring the information flow, an accident could occur due to a causal factor that was identified and treated, but the measures to prevent it were not correctly followed over time.

The proper implementation of the model to a specific system requires tailoring the general framework. That means that each box of the general framework will need another particular label. Once this structure is drawn, the tasks are divided into the application of four processes. The following processes guide the organization of effective actions on management activities.

Process 1 - Communication Protocol for Sensitive Data

Proactive measures to prevent accidents require effective channels to communicate safety information. This goal is obtained only if all stakeholders use the same language. The format of the input message for the Active Hazard Analysis has a complete description of an event that starts with the context, lists all actions of each controller chronologically, and explain the reasoning for the decisions taken as reported by each controller.

Process 2 - Active Hazard Analysis Update

The input message from any source is treated to verify if the hazard analysis is incomplete or if it was not respected. In the first case, the safety manager conducts a systematic procedure to update the hazard analysis. In the second case, the analyst investigates why the rules were not followed to adapt the prevention or mitigating measures or to enforce them. In both cases, management acts preventively to avoid future losses. The list of actions and controllers from the previous process become a reference to relate the event with the correct part of the hazard analysis. The identified mental models are discussed to reason on assumptions previously made. The assumptions are updated, followed by the scenarios and measures derived from it.

Process 3 - Hazard Management

Currently, most aeronautical product development organizations use risk assessments to decide how to prioritize mitigating measures and to judge if it is worth taking action. This risk management is the evaluation of both on-going and new initiatives in a systematic attempt to address areas with the potential to pose a risk to safety during operations.

The concept of an "acceptable level of safety" is expressed by two measures required by ICAO: Safety Performance Indicators (SPI) and Safety Performance Targets (SPT). These

solutions are in place because the company top management requires measurable safety targets that are acceptable to regulators and other stakeholders, and consistent with the SMS.

The problem is that, without a structured hazard analysis, the selection of SPIs and SPTs is subjective and relies only on the experience of a few managers. Systems Engineering provides qualitative ways to manage hazards and the analysis result on the elaboration of SPIs that will explain if the system is drifting to a more hazardous status. In other words, the new set of SPIs diagnose the safety culture of the organization and verify if communication channels are effective.

Process 4 - Prevention & Mitigation

The strategy for mitigation involves a range of possible actions including:

- Revision of the system design with changes to the functional control structure.
- Modification of operational procedures.
- Re-arrangements of staffing.
- Training of personnel to specific scenarios.
- Development of emergency and contingency plans.
- Ceasing operation.

All updates of the hazard analysis will result in changes in the company's documentation. Most safety critical organizations have standard procedures that are taught during training and enforced throughout the operation. They culturally become rules to avoid blame.

The desired safe behavior requires building mental models to facilitate proper actions when specific conditions are detected and recognized. It also requires responding signs of those conditions that alert about the proximity to hazard. That becomes necessary as humans are affected both by an excess of information, that causes high workload and stress, or lack of information, which leads to low situation awareness and distractions. Most systems have hazards related to both extremes, but prevention is possible if human factors are properly considered.

The solution is to organize the required safety knowledge into communication events that occur at different moments. Each communication opportunity has specific characteristics. The four categories and their vehicles presented in the general framework are a proposed reference that should be adjusted to the desired system:

- **Training:** The first opportunity to teach and to present limitations and rules has the benefit of a mind clearer of biases and preconceptions. The study of manuals must have a set of information regarding safety reasonably complete. That will be used to form the mental models and to serve as a consultation source during operation.
- **Planning:** The time dedicated to plan a set of actions (e.g., a mission in military activities) is opportune to communicate safety concerns to operators. The addition of safety information during the planning activity reduces surprises and the variability of improvisations.
- **Setup:** When the task is complex and requires a fast and accurate response, the operator prepares himself or herself recalling the mental models and remembering the responses for off-nominal situations. In many systems, checklists are tools that deal

with memory limitations. New technology solutions provide multiple ways to feed up-to-date information in dynamic systems.

- **Operation:** In dynamic phases of operations, there is no time to search for the manual or to read an order. The solution for the communication of safety information is the use of cues that can be aural or visual. They must be simple, recognizable and unequivocal.

Alerting System

In the I-SMS framework, the voluntary reports are classified into two different types: Hazard Analysis update and Condition Alert. In the hazard analysis update, the safety officer receives the description of the situation observed by the operator to perform the reasoning described in Process 2. In the second case, time-critical observations, such as a drone crossing the runway final approach, potentially dangerous environmental phenomena, or even criminal actions, require extra instant communication. Instant messages called Condition Alerts are transmitted using software solutions and connectivity to alert other operators.

Case Study and Conclusion

A complete STPA on unstable approaches was used as basis for the I-SMS. This project had the participation of major airlines in the USA, Brazil, Europe, and Asia. To avoid the correlation of companies with unsafe events, all data was condensed in one single database and analyzed altogether. The airlines provided flight monitoring data, pilot reports, observation flights, and investigation reports on unstable approaches for landing.

The outcomes of the project included more robust documentation for training, a better understanding of the vulnerabilities of airline operations, a more complete hazard analysis, a more explicit allocation of responsibilities, optimized enforcement mechanisms, and the observation of new trends that gives the feedback that is required for proper management.

References

FAA, FAA InFO, 2011. The Apple iPad and Other Suitable Tablet Computing Devices as Electronic Flight Bags (EFB).

FAA, 2015. Advisory Circular 120-92B (Safety management systems for aviation service providers) 1–4.

ICAO, 2013. Annex 19 to the Convention on International Civil Aviation, Annex.

Leveson, N., 2015. A systems approach to risk management through leading safety indicators. Reliab. Eng. Syst. Saf. 136, 17–34. doi:10.1016/j.ress.2014.10.008.

Leveson, N., 2011. Engineering a Safer World: Systems Thinking Applied to Safety, Vasa. doi:10.7551/mitpress/8179.001.0001.

Acknowledgments

This research was possible due to the scholarship provided by CNPq/Brazil.