SUMMARY OF SAFETY RISK MANAGEMENT METHODOLOGIES AND TOOLS

INTRODUCTION

This document includes further reference material and hyperlinks to support the SRM Fundamentals course. It contains alternative approaches to hazard analysis and safety risk management. Some are already used in aviation, whereas some are still new to aviation and being implemented.

It is important for organisations to choose a methodology that is suitable to the organisation and the environment. This suitability needs to consider:

- the complexity of the methodology
- the resources needed to apply the methodology
- the costs of the software
- the quality of the output and the ease to understand the outputs
- the training of the system users
- the availability and quality of the data to be used
- the integration with other enterprise risk management solutions

The ICAO Safety Management Panel Safety and its Risk Management Working Group continue to assess different risk management methodologies and tools to be uploaded to the SMI Website: www.icao.int/SMI

ICAO HAZARD TAXONOMY

The Hazards Common taxonomy is a high-level categorization of hazards types. Each type contains a main category definition to identify the family of hazards and sub-categories to further define the hazard type to aid in identification, analysis, and coding of hazards.

Hazards are classified in families of hazard types—logical groupings—to determine their potential consequences. These types of hazards were identified as Environmental, Technical, Organizational, and Human. Hazards are further classified below a certain family of hazard types as they relate to the hazard types.

Each of the environmental, technical, or organizational types of hazards may exist in a particular operational context. The operational contexts were identified as aerodrome services, air navigation service providers, flight operations, maintenance operations, and design and manufacturing. The human family of hazards includes conditions of humans that have the potential to cause injury to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function, according to the hazard definition. Examples of hazard subcategories relating to the human hazard category are an unknown medical condition, physical limitation, or psychological condition. These do not relate to the behavior of the human being.

More information can be accessed through the ICAO Website: https://www.icao.int/safety/airnavigation/aig/pages/taxonomy.aspx.

ISO31000:2018 – RISK MANAGEMENT - GUIDELINES

The long-term success of an organization relies on many things, from continually assessing and updating their offering to optimizing their processes. As if this weren't enough of a challenge, they also need to account for the unexpected in managing risk. That's why we've developed ISO 31000 for risk management.

In addition to addressing operational continuity, ISO 31000 provides a level of reassurance in terms of economic resilience, professional reputation and environmental and safety outcomes. In a world of uncertainty, ISO 31000 is tailor-made for any organization seeking clear guidance on risk management.

Further information can be accessed through: https://www.iso.org/iso-31000-risk-management.html. The document is freely available in read-only format to support global efforts in dealing with the COVID-19 crisis: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

IEC 31010:2019 - Risk management — Risk assessment techniques

IEC 31010:2019 is published as a double logo standard with ISO and provides guidance on the selection and application of techniques for assessing risk in a wide range of situations. The techniques are used to assist in making decisions where there is uncertainty, to provide information about particular risks and as part of a process for managing risk. The document provides summaries of a range of techniques, with references to other documents where the techniques are described in more detail. This second edition cancels and replaces the first edition published in 2009. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: • more detail is given on the process of planning, implementing, verifying and validating the use of the techniques; • the number and range of application of the techniques has been increased; • the concepts covered in ISO 31000 are no longer repeated in this standard.

BOWTIE

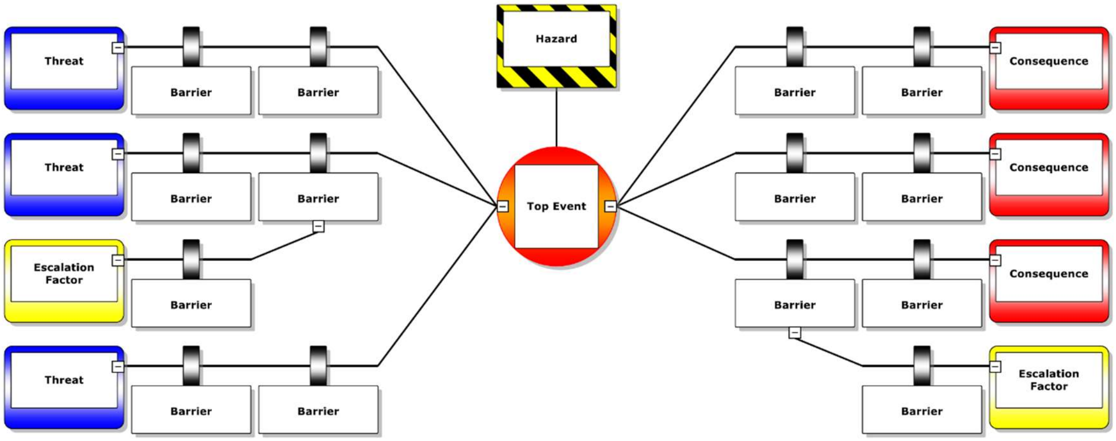
The bowtie methodology is used for risk assessment, risk management and (very important) risk communication. The method is designed to give a better overview of the situation in which certain risks are present; to help people understand the relationship between the risks and organizational events. The strength of the methodology lies in its simplicity; the phrase "less is more" is certainly applicable.

Risk management is all about risk-perception management, since most accidents happen because of actions or inactions of people. People working in hazardous environments should be aware of the present organizational risks and should have an accurate understanding of their role in it. This can only be accomplished by sufficient risk communication adjusted to the abilities of that part of the workforce you want to address, leading to the establishment of operational ownership.

Many risk assessments are done using quantitative instruments. These may be sufficient for certain types of equipment but are less valuable for organizational risk assessment. Human beings are less easy to predict than machinery and the operational combination of all factors present (think of people, equipment, time, weather, organizational factors, etc.) leads to even more difficulties. Making accurate predictions of the future in an environment that is as complex as the world itself, is simply impossible. In many organizations, the stakes of certain consequences (resulting from an accident) are too high to leave unmanaged. Therefore, it is wise to be prepared for 'everything'; think of all possible scenarios and assess how your organization is prepared to deal with them. This is exactly what the bowtie method will help you accomplish. This can be achieved either with software or a flip chart and some 'sticky notes'.

Risk in bowtie methodology is elaborated by the relationship between hazards, top events, threats and consequences. Barriers are used to display what measures an organization has in place to control the risk.

This model is valuable for simple explanation and organization of risk factors. Useful from very basic through intermediately complex applications. Further information can be accessed through: https://www.bowtiexp.com/ and https://www.caa.co.uk/safety-initiatives-and-resources/working-with-industry/bowtie/



ARMS METHODOLOGY FOR OPERATIONAL RISK ASSESSMENT

Operational Risk Management consists of three elements: Hazard Identification, Risk Assessment and Risk Reduction (mitigation, in ICAO terminology). The main objective of Risk Management is to make sure that all risks remain at an acceptable level.

Contributing to Safety Performance Monitoring through the establishment of risk-based Safety Performance Indicators can be considered a secondary objective. Risk information can also be used by the national authorities in their safety oversight.

Hazard identification is about collecting and analysing operational safety data, thereby identifying Safety Issues (see the Glossary for a definition of a Safety Issue). Such safety data typically includes safety reports, Mandatory Occurrence Reports (MOR), flight data events, and the results of safety surveys and audits. Hazard Identification provides the input for Risk Assessment.

The objective for Operational Risk Assessment (ORA) is the Assessment of operational risks in a systematic, robust and intellectually cohesive manner. Operational Risk Assessment is needed in three different contexts:

1. Individual safety Events may reflect a high level of risk and consequently require urgent action. Therefore, all incoming events need to be risk assessed. This step is called Event Risk Classification (ERC).

2. The Hazard Identification process may lead to the identification of Safety Issues, which need to be risk assessed to determine what actions, if any are needed. This step is called Safety Issue Risk Assessment (SIRA).

3. From time to time there will be a need to carry out Safety Assessments, typically related to a new or revised operational activity (e.g. new destination). The activity needs to be risk assessed at the planning stage, according to the “Management of Change” process of the company.

This methodology is useful for event analysis and issue identification, further information can be accessed through: https://www.skybrary.aero/bookshelf/books/1141.pdf.

Event Risk Classification (ERC)

In the Event Risk Classification (ERC), all the circumstances that conspired to produce the event are known and are considered as they were, so the subjectivity associated with determining the likelihood of the event occurring has been greatly reduced. • The ERC attempts to identify the likelihood of this event having resulted in an accident outcome by assessing the barriers that avoided this event being that outcome. The consideration of these barriers is still subjective but that subjectivity can be reduced by a good understanding of the barriers available in typical scenarios.

Safety Issue Risk Assessment (SIRA)

In carrying out a Safety Issue Risk Assessment (SIRA), the analyst him/herself should first define and scope the Safety Issue before risk assessing it. A precisely defined Safety Issue is much easier to assess quantitatively. For example a windshear Safety Issue that concerns only one aircraft type and one airport is easier to examine than one that covers the whole airline fleet and route network. Careful definition will ensure that the risk assessment is more likely to be based on facts rather than imagination and guessing.

SYSTEM-THEORETIC ACCIDENT MODEL AND PROCESSES – STAMP

STAMP focuses particular attention on the role of constraints in safety management. Instead of defining safety in terms of preventing component failure events, it is defined as a continuous control task to impose the constraints necessary to limit system behavior to safe changes and adaptations. Accidents are seen as resulting from inadequate control or enforcement of constraints on safety-related behavior at each level of the system development and system operations control structures. Accidents can be understood, therefore, in terms of why the controls that were in place did not prevent or detect maladaptive changes, that is, by identifying the safety constraints that were violated at each level of the control structure as well as why the constraints were inadequate or, if they were potentially adequate, why the system was unable to exert appropriate control over their enforcement. The process leading to an accident (loss event) can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values. The adaptive feedback mechanism allows the model to incorporate adaptation as a fundamental property.

STAMP also overcomes the other limitations of event chain models. System accidents arising from the interaction among components and not just component failure accidents are easily handled. While events reflect the effects of dysfunctional interactions and inadequate enforcement of safety constraints, the inadequate control itself is only indirectly reflected by the events—the events are the result of the inadequate control. STAMP considers the safety control structure itself to determine why it was inadequate to maintain the constraints on safe behavior and why the events occurred.

While STAMP will probably not be useful in law suits as it does not assign blame for the accident to a specific person or group, it does provide more help in understanding accidents by forcing examination of each part of the socio-technical system to see how it contributed to the loss (and there will usually be contributions at each level). Such understanding should help in learning how to engineer safer systems, including the technical, managerial, organizational, and regulatory aspects. To accomplish this goal, a framework for classifying the factors that lead to accidents was derived from the basic underlying conceptual accident model. This classification can be used in identifying the factors involved in a particular accident and in understanding their role in the process leading to the loss. The accident investigation after the Black Hawk shootdown identified 130 different factors involved in the accident. In the end, only an air traffic control operator was court martialed, and he was acquitted. The more one knows about an accident process, the more difficult it is to find one person or part of the system responsible.

STAMP provides a direction to take in creating new hazard analysis and prevention techniques that go beyond component failure and are more effective against system accidents, accidents related to the use of software, accidents involving cognitively complex human activities, and accidents related to societal and organizational factors. Because in a system accident model everything starts from constraints, the new hazard analysis approaches would focus on identifying the constraints required to maintain safety and then designing the system and operating conditions to ensure that the constraints are enforced. These constraints would include identifying what operators need to build accurate mental models and maintain safe operations. Such hazard analysis techniques would augment the failure-based methods and encourage a wider variety of risk reduction measures than simply adding redundancy to deal with component failures.

STAMP could also be used to improve performance analysis. Performance monitoring of complex systems has created some dilemmas. Computers allow the collection of massive amounts of data but analyzing that data to determine whether the system is moving toward the boundaries of safe behavior is difficult. The use of a system accident model and the basic concept of safety constraints may provide directions for identifying appropriate safety metrics; determining whether control over those constraints is adequate; evaluating the assumptions about the technical failures and potential design errors, organizational structure, and human behavior underlying the hazard analysis; detecting errors in the operational and environmental assumptions underlying the design, and identifying any maladaptive changes over time that could increase risk of accidents to unacceptable levels.

Further information can be accessed through: http://sunnyday.mit.edu/STAMP-publications-sorted-new.pdf and http://sunnyday.mit.edu/accidents/safetyscience-single.pdf .

System-Theoretic Process Analysis – STPA

STPA (System-Theoretic Process Analysis) is a relatively new hazard analysis technique based on an extended model of accident causation. In addition to component failures, STPA assumes that accidents can also be caused by unsafe interactions of system components, none of which may have failed. Some of the advantages of STPA over traditional hazard/risk analysis techniques are that:

- Very complex systems can be analyzed. “Unknown unknowns” that were previously only found in operations can be identified early in the development process and either eliminated or mitigated. Both intended and unintended functionality are handled.

- Unlike the traditional hazard analysis methods, STPA can be started in early concept analysis to assist in identifying safety requirements and constraints. These can then be used to design safety (and security) into the system architecture and design, eliminating the costly rework involved when design flaws are identified late in development or during operations. As the design is refined and more detailed design decisions are made, the STPA analysis is also refined to help make more and more detailed design decisions. Complete traceability from requirements to all system artifacts can be easily maintained, enhancing system maintainability and evolution.

- STPA includes software and human operators in the analysis, ensuring that the hazard analysis includes all potential causal factors in losses.

- STPA provides documentation of system functionality that is often missing or difficult to find in large, complex systems.

- STPA can be easily integrated into your system engineering process and into model-based system engineering. Many evaluations and comparisons of STPA to more traditional hazard analysis methods, such as fault tree analysis (FTA), failure modes and effects criticality analysis (FMECA), event tree analysis (ETA), and hazard and operability analysis (HAZOP) have been done.

In all of these evaluations, STPA found all the causal scenarios found by the more traditional analyses but it also identified many more, often software-related and non-failure, scenarios that the traditional methods did not find. In some cases, where there had been an accident that the analysts had not been told about, only STPA found the cause of the accident. In addition, STPA turned out to be much less costly in terms of time and resources than the traditional methods.

Further information: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Causal Analysis based on System Theory – CAST

The causal analysis approach taught in this handbook is called CAST (Causal Analysis based on System Theory). Like STPA [Leveson 2012, Leveson and Thomas 2018], the loss involved need not be loss of life or a typical safety or security incident. In fact, it can (and has been) used to understand the cause of any adverse or undesired event that leads to a loss that stakeholders wish to avoid in the future. Examples are financial loss, environmental pollution, mission loss, damage to company reputation, and basically any consequence that can justify the investment of resources to avoid. The lessons learned can be used to make changes that can prevent future losses from the same or similar causes.

Because the ultimate goal is to learn how to avoid losses in the future, the causes identified should not be reduced to an arbitrary "root cause." Instead, the goal is to learn as much from every accident as possible. This goal is what CAST is designed to achieve. Some accident investigators have actually complained that CAST creates too much information about the causes of a loss. But, is a simple explanation your ultimate goal? Or should we instead be attempting to learn as much as possible from 8 every causal analysis? Learning one lesson at a time and continuing to suffer losses each time is not a reasonable course of action. Systemic factors are often omitted from accident reports, with the result that some of the most important and far reaching causes are ignored and never fixed. Saving time and money in investigating accidents by limiting or oversimplifying the causes identified is false economy. The concept of "root cause" and "probable cause" are common ways to find someone or something to blame and then get on with life and business—until the next accident. The overriding question is whether to pay now or pay later.

Further information: http://psas.scripts.mit.edu/home/get_file4.php?name=CAST_handbook.pdf

SORA – SPECIFIC OPERATIONS RISK ASSESSMENT

The Specific Operations Risk Assessment (SORA) provides guidance to both the competent authority and the applicant as to what is required for an NAA authorization required to fly an Unmanned Aircraft System (UAS) in a given operational environment. The SORA is primarily aimed at the "Specific" category of UAS (as defined by EASA Technical Opinion 01/2018).

Risk in this context is understood to be the combination of the frequency (probability) of an occurrence and its associated level of severity. Safety means a state in which the risk is considered as acceptable. The way to reach an acceptable risk may differ for the "Open", "Specific" and "Certified" categories, considering both Unmanned Aircraft Systems (UAS) design integrity and the kind of intended operations. However, the safety level (i.e. probability of potential fatalities on the ground or in the air) shall remain the same for the three categories.

The operational volume is defined as including both the "Flight geography" (i.e. the UA flight path under normal operations) and the "contingency volume" (i.e. the projected UA flight path under abnormal conditions handled through contingency procedures). An out of control operation means that the UA is flying out of this operational volume (not including risk buffer), potentially leading to harm to third parties in the air or on the ground.

In order to show that the operator can keep control of the Unmanned Aircraft (UA) within the intended "operational volume" and that the operations have reached an acceptable level of risk, the SORA provides an adequate combination of design and operational mitigation mechanisms for known areas of harm to either people on the ground or in the air.

These mitigations have to be met with a Level of Robustness (Low, Medium, High) that is commensurate with the determined Ground and Air Risks classes. The level of robustness corresponds to an appropriate combination of the levels of integrity and the levels of assurance. The level of integrity is the safety gain achieved by the mitigation and the level of assurance is the method of showing that the level of integrity has been met.

Further information can be accessed through: http://jarus-rpas.org/content/jar-doc-06-sora-package.

FRAM – FUNCTIONAL RESONANCE ANALYSIS METHOD

THE FRAM is a method to analyse how work activities take place either retrospectively or prospectively. This is done by analysing work activities in order to produce a model or representation of how work is done. This model can then be used for specific types of analysis, whether to determine how something went wrong, to look for possible bottlenecks or hazards, to check the feasibility of proposed solutions or interventions, or simply to understand how an activity (or a service) takes place. The FRAM is a method for modelling non-trivial socio-technical systems. It is NOT a risk assessment method and it is not an accident analysis method. Neither is a FRAM model a flow model, a network model, or a graph. But the model produced by a FRAM analysis can serve as the basis for a risk analysis, an event investigation, or for something entirely different.

THE FRAM is based on four principles: the equivalence of failures and successes, the central role of approximate adjustments, the reality of emergence, and functional resonance as a complement to causality. The FRAM does not imply that events happen in a specific way, or that any predefined components, entities, or relations must be part of the description. Instead it focuses on describing what happens in terms of the functions involved. These are derived from what is necessary to achieve an aim or perform an activity, hence from a description of work-as-done rather than work-as-imagined. But functions are not defined a priori nor necessarily ordered in a predefined way such as hierarchy. Instead they are described individually, and the relations between them are defined by empirically established functional dependencies.

To get more information about FRAM, access: https://www.functionalresonance.com/.