

Integrated Safety Management System

Michael Kavoliunas and Zdzislaw H. Klim
Bombardier Aerospace

Dragan Komljenovic
Hydro-Quebec

Copyright © 2009 SAE International

ABSTRACT

The Safety Management System requires a structured Risk Management Process to be effective. In the technical fields where numerous potentially catastrophic risks exist, processes and procedures need to account not only for the hardware random failures but also of human errors. The technology has progressed to the point where the predominant safety risks are not so much the machine failures but that of the human interaction. Accidents are rarely the result of a single cause but of a number of latent contributing factors that when combined result in the accident.

In the Aerospace industry, the operational risk to the fleet is assessed by the manufacturer and the operator independently and is used in safety and/or regulatory decision-making. For the manufacturer, the risk assessment is a philosophy whereby risk of a potential or actual occurrence is evaluated in comparison to the event analyzed in the system safety assessment or structural analysis performed for certification of the product. The resulting safety decision-making process involves integration of the probabilistic risk assessment, deterministic and severity perception elements such that the decisions made leads to corrective or preventative actions. The evaluations of the human factors elements are subjectively assessed based on individual experience based criteria and are difficult to integrate into the safety decision. The risk assessment is viewed as the process that records all these factors as the basis for the safety decision and prioritization of the corrective actions.

In the Nuclear industry a risk-informed approach to safety and/or regulatory decision-making represents a philosophy whereby risk insights are considered together with other factors, including good engineering practice and experience, to establish the design requirements and operational issues commensurate with their importance to public health and safety. A standard risk-based approach to safety and/or regulatory decision-making is one in which a decision is based solely on the numerical results of a risk assessment. Quantitative risk analyses are important inputs to decision making, but they do not constitute an adequate or sufficient base of information for addressing the complex issues that face the nuclear power industry. For that reason such analyses are only one of the many contributing inputs to a comprehensive risk-informed decision making process. Risk-informed decision making involves integration of probabilistic, deterministic and non-quantifiable elements such that, overall, the decisions made lead to a resolution of the issue being considered that is commensurate with its risk-significance and is better to that likely to be reached if any approach is used in isolation.

This paper intends to compare the Risk Management methodologies and procedures used in the Aerospace and Nuclear industries to highlight similarities and differences. The learning from these differences may then identify potential improvements to either methodology.

INTRODUCTION

A Safety Management System (SMS) is a systematic approach to managing safety, including the necessary

organizational structures, accountabilities, policies and procedures in the Aerospace industry [1]. An SMS relies on developing an understanding of the safety risks involved in the way the operator operates the machinery and not just considering the safety risks of the machine failing to perform its intended function. The understanding of the risks and the acceptable level of risk each operator is willing to take then forms the baseline for which decisions are made. The decision may be to accept the current risk level or make further risk reductions to achieve a risk As Low As Reasonable Practical (ALARP). Risk Management is a significant part of a Safety Management System (SMS) and the difficulty is how to assess the risks in a meaningful way that represents all the aspects that is perceived by the public as a safe operation.

In the Aerospace Industry the Manufacturer evaluates the safety risks of the product failures to the operation considering that the personnel (flight crew, maintenance, ground handling) perform their duties as specified in the operating and maintenance manuals. The operator evaluates the safety risks of human errors or specific operation risks for their operation, which may differ from operator to operator. The manufacturer must consider not only the logically evaluated risk based on the probability of occurrence but also the perceived risks by the public and regulators as to the safety of the product. In order to come to a decision regarding accepting or reducing the risk, all the factors must be considered in this decision.

A fundamental rule of nuclear safety is that the licensee has the responsibility for safely operating a Nuclear Power Plant (NPP), and that “those who create risks from work activity are responsible for protecting workers, the public and the environment from the consequences” [2]. Thus, the primary responsibility for managing the risks associated with NPP operation rests with the licensee. However, it is also recognized that regulatory requirements, and the regulator’s *modus operandi*, constitute significant “shaping factors” for licensees’ operations in general.

International Atomic Energy Agency (IAEA) has issued a safety guide on periodic safety review for the nuclear industry [3]. The purpose of this document is to provide recommendations and guidance on the conduct of a Periodic Safety Review (PSR) for an existing nuclear power plant. A PSR is a comprehensive safety review of all-important aspects of safety, carried out at regular intervals, typically of ten years. PSRs are considered an effective way to obtain an overall view of actual plant safety, to determine reasonable and practical modifications that should be made in order to maintain a high level of safety and to improve the safety of older nuclear power plants to a level approaching that of modern plants. In this connection, it is useful to identify any lifetime limiting features of the plant in order to help evaluate whether a proposed modification is worthwhile.

The objective of a PSR is to determine by means of a comprehensive assessment of an existing nuclear power plant: the extent to which the plant conforms to current international safety standards and practices; the extent to which the licensing basis remains valid; the adequacy of the arrangements that are in place to maintain plant safety until the next PSR or the end of plant lifetime; and the safety improvements to be implemented to resolve the safety issues that have been identified. Several national regulatory bodies consider PSR as one of basic elements of a new licensing basis.

BASELINE SAFETY OF THE PRODUCT DESIGN

Both industries are strongly regulated by the international and national organizations. In the civil aerospace industry, the national regulations define basic requirements of the aircraft design to ensure manufactures produce the safe aircraft designs. Regulations such as the Federal Aviation Administration (FAA) Part 25 Airworthiness Standards: Transport Category Airplanes and specifically Subpart F, FAR 25.1309 Equipment, systems and installations [4] address the safety of the design of the systems on board an aircraft. The European Aviation Safety Agency (EASA) provides the similar regulations, Certification Specification for Large Aeroplanes CS-25 for all members of the European Union [5].

The regulatory framework in the nuclear power industry is stretching out from the international organizations up to the national government offices. The IAEA provides the series of regulations of nuclear facilities related to the licensing basis for safety of the nuclear power reactors operation [6]. It should be stressed however, that there are not uniform development at the national level. Each national regulatory body is in charge to develop a national specific regulatory framework. The pace and stage of implementation regarding new orientations varies significantly from one country to another. In addition, several activities and initiatives in the field of the operational safety are developed by industry. In Canada, the CANDU Owner Group (COG) is providing the principles and processes for the risk assessment of the nuclear power installations specific design and operation [7].

SAFETY OF THE AIRCRAFT IN-SERVICE

If “to err is human” then that is primarily why an SMS is required. The design may have errors, the analysis may have errors, the maintenance instruction, the maintenance actions and so on. There was never any intent by any of the involved people who designed, analyzed or wrote procedure to create errors but they still happen. The System Safety Analysis for the Aircraft systems is unique as its premise is “everything fails.” Applying this premise to evaluating processes within an organization, it identifies that hazards that can be introduced by any activity within an organization. With regards to the product, or failures induced by the use of

the product in a way that was not intended, then the following methodology is used.

IN-SERVICE SAFETY – RISK MANAGEMENT-

The Society of Automotive Engineers SAE ARP 5150 [8] describes a number of tools that can be used to collect data and evaluate the safety risks as a result of the aircraft failing to perform its intended function. It provides some tools to address the human factors and potential for human failures introducing hazards to the operation of the product either through maintenance errors or operational errors. These tools are more to identify the risks as opposed to considering these factors in evaluation of a Hazard from an in-service event.

As a result of an in-service event (or identified hazard), an evaluation of the risk to the aircraft fleet safety is started. First the event must be identified as having a potential impact to the product safety. Then a preliminary risk assessment is conducted to categorize the risk and define the exposure of the risk (portion or all of the aircraft fleet). A tool such as a risk matrix can help identify if the risk is “unacceptable” (too high for organization / authorities) and rank the risk level [9]. The ranking of risks is useful in order to manage the risk reduction activities, as there are often a number of safety issues in need of risk mitigation at any one time.

Once the initial risk level is determined, a maximum reaction time for organization is established for the risk decision in a corrective action process. As shown in Figure 1 Decision Process for Corrective Action, if the risk is not very high (immediate mitigation not required), then a more detailed (formal) risk assessment is conducted.

This risk assessment is a process that not only details what happened in the event but also what could potentially happen that may be of a greater severity or higher risk. In addition, an examination of the contributing factors is evaluated as to the behavior of the flight crew or the interpretations of the maintenance personnel as to how human factors contributed to the event or increased the severity or probability of the event. The risk assessment has to make a determination of the probabilities of the events for each of the identified hazards to assess the risk level. Another element in the risk management process is to establish a reasonably acceptable time for which an unacceptable risk can be tolerated. The reaction time determination can be addressed using a tool provided in guidance material from the European Aviation Safety Agency (EASA) in AMC and GM Part 21 Guidance Material (GM) 21A.3B (d) (4) Defect Correction – Sufficiency of proposed corrective action [10].

The EASA guidance material defines average rectification times for potentially Catastrophic or Hazardous cases based on the probability of occurrence. This assumes that the risk assessment estimated the probability of the event with some

justification (data). This reaction time provides a basis for the Corrective Action Review Board (CARB) to decide the maximum time it should take to rectify the affected fleet of the safety issue.

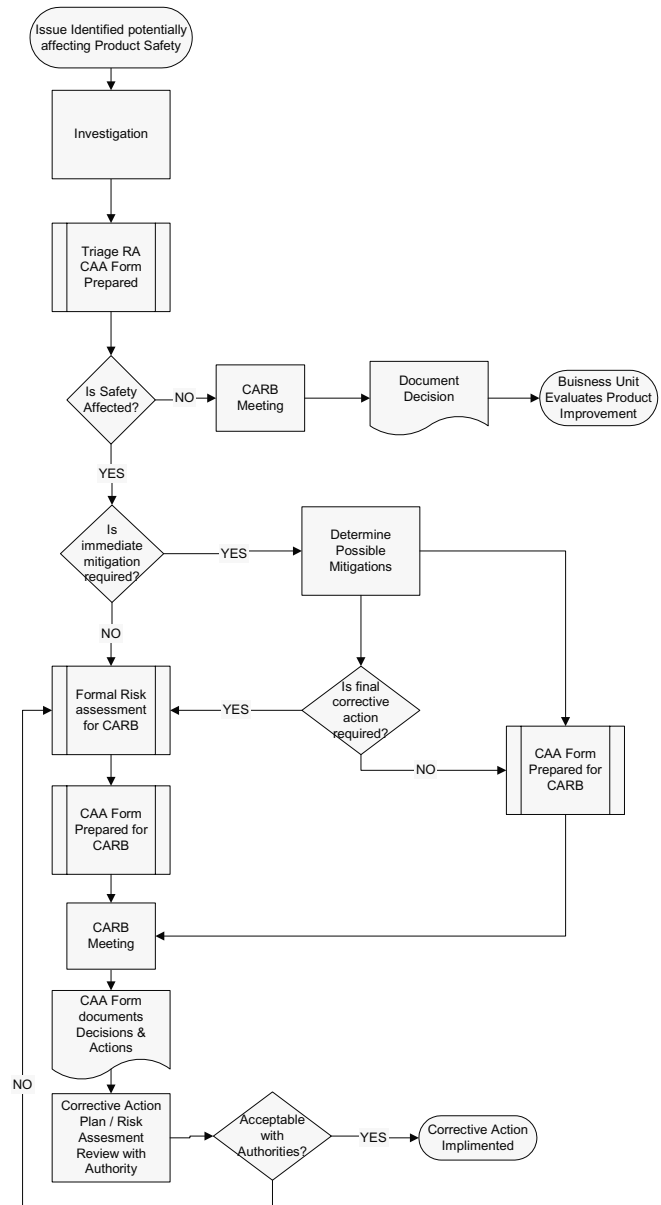


Figure 1 Decision Process for Corrective Action

It may be established that other contributing factors can influence the probability of occurrence or the severity. Therefore corrective action should be completed in a shorter period of time than computed using the EASA guidance. It is the CARB that determines if these contributing factors are relevant and how that affects the appropriate actions. Additionally, the severity of an event under normal operating conditions may have a lower severity than when the weather is adverse, for example. The severity of an event that was established for certification purposes may be now considered higher due to operational issues combined with human error. In this case the organization may deem the safety risk