INSTITUTIONAL FAILURE: ARE SAFETY MANAGEMENT SYSTEMS THE ANSWER?

J. G. Waddington[1], J.F. Lafortune[1], Romney Duffey[2]
[1] International Safety Research, Ottawa, Ontario, Canada
[2] Atomic Energy of Canada Limited, Mississauga, Ontario, Canada

Abstract

In spite of an overwhelming number of safety management programs, incidents and accidents that could seemingly, in hindsight, have been prevented, still occur. Institutional failure is seen as a major contributor in almost all cases. With the anticipated significant increase in the number of nuclear plants around the world, a drastic step in the way we manage safety is deemed essential to further reduce the currently already very low rate of accidents to levels that will not cause undue public concern and threaten the success of the nuclear "renaissance". To achieve this, many industries have already started implementing a Safety Management System (SMS) approach, aimed at harmonizing, rationalizing and integrating management processes, safety culture and operational risk assessment. This paper discusses the origins and the nature of SMS based in part on the experience of the aviation industry, and shows how SMS is poised to be the next generation in the way the nuclear industry manages safety. It also discusses the need for better direct measures of risk to demonstrate the success of SMS implementation.

1 Introduction

The analysis of accidents involving "high-risk" industries consistently shows that a significant number of concurrent factors have to occur to cause an accident; in most cases, the absence of any one of those contributing factors could have prevented the accident. Many studies indicate that human failures are dominant factors in 70% to 90% of cases [1]. These human failures may arise from the traditional "operator error", but much more common are failures of organizational and management systems. Indeed, many "operator errors", when examined more closely, can be attributed to organizational failures. We refer to such failures as "institutional failures". Institutional failures are associated with the collapse or ineffectiveness of the collective management, governance, corporate, regulatory, operational, design, licensing, and societal fabric. An institutional failure is a failure of the "system".

It appears, then, that institutional failures are the greatest single contributor to the likelihood of a major accident, and a much greater contributor than weaknesses in design or, for example, errors in the validation of a safety analysis code.

The aim of this paper is to examine typical sources of institutional failures and to discuss how the introduction of safety management systems (SMS) can help reduce them. The paper also discusses the need to obtain meaningful measures of risk that would provide feedback to management on the performance of SMS.

2 Real Cases: Anatomy of a Major Industrial Accident

2.1 Piper Alpha

The Piper Alpha accident took place on 6 July, 1988 in the North Sea, west of Scotland. It was caused by a series of failures that started with what was meant to be a routine maintenance procedure on a gas compressor. The work could not be completed in a day and was stopped until the following day. When restarting the procedure, a primary condensate pump failed and, not knowing that a vital part of the machine had been removed, the crew decided to start the backup pump. Gas leaked out and exploded, damaging critical equipment and safety systems. Key safety systems, such as the deluge system, were not activated; they had been turned off for the procedure. The fire spread, damaging more high-pressure flammable gas pipes. Personnel were not able to escape due to the escape routes being blocked by smoke. The accident lasted 22 minutes. Of the 229 people on board, 167 died.

Stated causes are numerous and include the following: the permit-to-work system in place had become too relaxed; the design of the safety systems was insufficient for this type of event; there was a lack of training in safety procedures; audits had become routine and superficial, and failed to uncover the latent weaknesses within the organization (a regulatory audit performed seven days earlier had passed); isolation procedures were not properly followed; and emergency facilities did not recognize this possible event and the complications that would arise. One major shortcoming was identified that links all these contributing factors: the safety systems in place were not properly "managed". The Cullen report [2] was highly critical of the management in general and of the management systems in place. Approximately one year before the explosion, company management had been warned that a large fire could pose serious concerns with respect to the safe evacuation of the platform. But this concern was not properly assessed and was discarded following a cursory examination. Cullen also found that the regulatory structure was partly to blame for establishing regulations that were unduly restrictive, and which focused on the solutions rather than on the objectives. Overall, the entire industry contributed to the disaster, not just the operators.

2.2 The Texas City BP Refinery Accident

Previously owned by Amoco, the Texas City BP Refinery was turned over to BP following a merger in 1999, but it was still managed largely according to pre-merger Amoco safety systems. At the time of the accident, on 23 March, 2005, about 800 additional contract personnel were present at the site. Temporary trailers had been installed 150 feet from a blowdown drum and stack. Placement of a trailer within 350 feet of a process unit called for a facility siting analysis as part of a Management of Change process; as a result of this process, occupancy of that trailer had not been authorized prior to the accident. However, the trailer was indeed occupied as early as November, 2004 and additional trailers had been placed in close proximity.

The accident occurred following a planned maintenance outage on the Isomerization Unit (ISOM). A Raffinate Splitter unit, shut down and cleared of hydrocarbons for the duration of the outage, needed to be restarted during a procedure that started on the evening of 22 March and was due to be completed on 23 March. Following a series of procedural deviations and miscommunications, including shift changes without turnovers and clear derogation of the procedures for pre-job briefings, flow control and firing unit control, the temperature and pressure in the splitter and the overhead condensers began to rise, and a relief valve opened to relieve directly into the Boiler Drum and Stack. Although fueling of the unit burners was stopped, gas and liquid started emerging from the stack like a geyser and ran down to form a pool of flammable mixture at the base of the stack. An operating vehicle present nearby may have provided the ignition, which caused a series of violent explosions killing 15 and injuring 170 personnel who were near the trailers.

The accident report [3] found several immediate causes to this accident, including violation of procedures by personnel and supervisors; improper decision-making; defective safety devices, inadequate equipment, lack of knowledge of hazards, distractions (human factors), complacency, and inadequate layout. More importantly, it pointed to serious management and cultural root causes: poor judgment, inadequate training, inadequate leadership, inadequate maintenance, inadequate enforcement of policies and standards, confusing business context, lack of safety as a priority, inability to recognize the risks, lack of proactive warning, organization complexity (conflicting roles and responsibilities), lack of safety meetings, and inadequate vertical and lateral communication. Although the report makes many recommendations regarding equipment, procedures and work management, most of the recommendations focus on two themes: the need for a better and more integrated management of safety, human and organizational factors, and the achievement of an enhanced safety culture through the clear definition of expected behaviours at all organizational levels. The independent “Baker Report” [4] criticized the company-wide lack of “safety culture” and the lack of appropriate safety processes.

2.3 Dryden

On 10 March, 1989, Air Ontario Flight 1363, a Fokker F28-1000 en route from Thunder Bay to Winnipeg, took on too many passengers on its way to a stopover in Dryden, which led to the need to refuel for the ongoing flight. There was light snow that afternoon. A layer of 0.6 to 1.3 centimetres of snow had accumulated on the wings and deicing was considered. However, the Fokker F-28 aircraft is not supposed to be de-iced while the engines are running, and the auxiliary power unit (APU) was unserviceable. In addition, there was no available external power unit at Dryden Municipal Airport. The choice was to shut down and terminate the flight or forego the deicing and proceed with the scheduled flight. Off-loading and reloading passengers would have taken considerable time and the longer the aircraft stayed on the ground the greater was the need for the wings to be sprayed with de-icing fluid. Although several passengers and cabin crew members had noticed the accumulation of snow on the wings, no one informed the captain, who did not request de-icing, which would have required the engines to be shut down. The engines were left running and de-icing was not done. Immediately after take-off, the aircraft crashed

because it was not able to achieve enough altitude to clear the trees beyond the end of the runway, causing the death of 21 of 65 passengers and 3 of 4 crew members.

The Dryden inquiry into this crash [5] revealed a number of contributing factors, including equipment deficiencies, management and commercial pressures, the absence of a safety officer, post-merger cultural differences (the airline had recently been acquired by Air Ontario), poor air crew communications, inadequate procedures for refueling and misguided regulatory oversight. But more importantly, the Honourable Virgil Moshansky, author of the inquiry report, stated that the accident had been the result of a number of underlying, latent failures in the organization, or widespread systems failures. Moshansky refers to "*a plethora of negligence, miscues, omissions, commissions, deficiencies, bad management and regulatory policies, human factors… in every aspect of the aviation system, which came together at Dryden*". Cost cutting measures, inadequate pilot training, lack of spare parts, useless policies, lack of risk management in all aspects of the operation, including in dispatch, and the complexity of the technology, all contributed significantly to making this accident possible, if not likely.

Once again, the inquiry into a serious technological accident points to the lack of a properly managed system to deal with safety.

2.4 Davis Besse

On 2 March, 2002, during a refueling outage, David Besse engineers inspected the nozzles that penetrate the Reactor Pressure Vessel (RPV) head and provide the path for the control rods to enter the core. The inspections had been ordered by the US Nuclear Regulatory Commission (NRC) to look for stress corrosion cracking triggered by boric acid that is dissolved in the primary coolant to control reactivity. The engineers found cracks in a number of nozzles. To repair them, the weld between the nozzle and the RPV head that provides the pressure boundary on the inner face of the head had to be machined out. When the head is manufactured, the nozzles are shrunk fit into the 6.63 inch thick head and then welded on the inside to the RPV head base material. When the machining head was withdrawn from nozzle no 3, it fell over, to the surprise of the engineers.

On inspection, it was found that the material of the reactor vessel head had disappeared over a 20-30 sq inch surface area, leaving a cavity that went through the full thickness of the PRV head. Only the 3/8-inch thick stainless steel cladding on the inside surface remained to provide the pressure boundary - a very thin membrane indeed that was preventing a major, unanalyzed, loss of coolant accident, and possibly a rod ejection accident. The cavity was caused by leakage from a through-wall axial crack in the nozzle leading to boric acid corrosion of the head enhanced by flow assisted corrosion, this last feature being very familiar to the Canadian nuclear business.

The NRC set up a Task Force to identify the lessons learned from this incident [6]. Most of its focus was on what the NRC could have done to prevent the incident, but it has also examined the activities of the plant operator. Stress corrosion cracking was first observed in Inconel 600, the material of the nozzles, in the late 1980's. Nozzle cracking was first observed in the Unit 3

reactor at Bugey, France, in 1991. This was not known to many NRC or Davis Besse staff. Nozzle cracking was also found in the Oconee station in the spring of 2001. Babcox and Wilcox reactors such as Oconee and Davis Besse were considered to be highly susceptible to circumferential cracking in the nozzles, and by November 2001, axial cracking had been found in all B&W plants, and circumferential cracking of at least one nozzle in 86% of them. The NRC bulletin recommended inspections be completed by Dec 2001; Davis Besse management felt it would be safe to operate until the next refueling outage in the spring of 2002.

The Task Force report [6] also provides a timeline leading to this event, which illustrates that the NRC, the industry and David Besse were all aware of stress corrosion cracking as an issue, with some parts of their organisation aware of previous incidents, indicating the presence of significant latent organizational and engineering issues. Leakage, for example, had existed for many years, to the extent that boric acid deposits were fouling some key components in containment, and cleaning the deposits off those components had become a routine event. However, these indicators were not integrally assessed, improperly evaluated or simply ignored.

The Task force concluded that Davis Besse was suffering from: (1) strained engineering resources; (2) an approach of addressing the symptoms of problems as a means of minimizing production impacts; (3) a long-standing acceptance of degraded equipment; (4) a lack of management involvement in important safety significant work activities and decisions, including a lack of a questioning attitude by managers; (5) a lack of engineering rigor in the approach to problem resolution; (6) a lack of awareness of internal and external operating experience, including the inability to implement effective actions to address the lessons-learned from past events; (7) ineffective and untimely corrective actions, including the inability to recognize or address repetitive or recurring problems; (8) ineffective self-assessments of safety performance; (9) weaknesses in the implementation of the employee concerns program; and (10) a lack of compliance with procedures.

2.5 What do these events have in common?

Many more famous and infamous events and major outcomes that constitute *institutional* as well as system failures could have been added to this list (e.g. the Toulouse fertilizer plant explosion, Columbia and Challenger space shuttle losses, Buncefield oil refinery fire, Quebec overpass collapse, Concorde aircraft crash, and train derailments in the UK). Many of these facilities and technologies had multiple safety programs, quality assurance, regulations, inspections, risk reviews, safety analyses and event reporting systems already in place, which were deemed effective. However, in spite of these programs and safety initiatives, these incidents or accidents happened.

Accidents generally exhibit the same four stages:

- The early unfolding of precursors;
- A confluence of a number of other events which made the whole vital and irreparable;
- An escalation arising from a continuous emphasis to keep on with the task at hand; and

- An initial (and sometimes lengthy) denial of the institutional sources of many of the contributing factors.

It is often easy to conclude that human error was the major contributor, but this is an oversimplification; other factors played a major role. In fact, in all cases, it is not possible to point to a single root cause. Each accident is a so-called complex accident, being the result of a combination of many failures - the absence of any of which could have prevented the chain of events that led to the accident - combined with deficient management oversight, and "loss of control" of the technological system [7]. The direct cause often appears to be an error, or series of errors, committed by an operator. However, the fact that these errors were possible and even, in many cases, accepted or encouraged, points to factors that are related to the culture, the "business environment" or the management regime in place. In most cases, well-defined safety envelopes are in effect, but this is not sufficient to prevent the accident. Three main reasons for this are:

- The safety envelope may not take into account all the known risks, which points to an organizational lack of risk awareness;
- The safety envelope does not take into account the actual operating environment in which it is supposed to be applied, which point to a lack of operational feedback into the very definition of the safety envelope; or
- The safety envelope is not systematically respected, which points to cultural and leadership weaknesses, or to a lack of operational feedback into the risk mitigation process.

In today's highly regulated environment, it is rather rare to see a blatant disrespect of safety standards. Most organizations in complex technological industries have established, and continuously demonstrate adherence to, stringent regimes of procedures and safety programs. Yet accidents that could have been prevented, with hindsight, still happen. And every time they happen, we learn one more lesson on what could have been done to prevent it. But we often lack the foresight to properly understand and forecast what should be done to prevent other, different and potentially more serious accidents. We must be able to predict events, and establish a learning environment that recognizes both precursors and events.

Another frequent reason for the failure of safety programs is their lack of integration, by which we mean that there are internal barriers to communication that result in "functional silos" within departments of an organisation, between departments, and within an industry. Most organizations have highly competent men and women running them who are committed to achieving safe operation. But the silos exist, and managers are often unaware of their existence or their effectiveness as barriers to communication.

3 The Management of Errors

3.1 Human Error: From the Individual to the Organization

The science of "human factors" was born out of a need to deal with the increasingly complex nature of the technologies with which we interact. Initially, this field focused on ways to improve individual performance to prevent errors. Most of the efforts focused on the man-machine interface and saw the worker as an integral part of the man-machine system. This cognitive engineering perspective of human factors led to the classification of errors in terms of external factors related to the level of activity performed: skill-based, rule-based or knowledge-based.

This further evolved to take into account the fact that organizational policies, management practices and organizational factors play a major role in determining individual behavior. The socio-technical perspective of human factors led to the development of performance influencing factors (PIF) and the Human Factor Analysis Methodology (HFAM), which focus on changing environmental and organizational factors rather than strictly on individual behaviour.

Modern error management theories adopt a holistic view that takes both the individual and the organization into account in error prediction and prevention. To understand conditions that lead to accidents, one must therefore consider the management structure, the policies, the procedures, the training, the communication and the prevalent culture, which encourages (or discourages) workers from following established procedures and practices. These factors form an integrated system of actions and interactions that determine the overall behaviour of the organization and of the individuals. Individual programs that target each of these individual factors are an essential element of the overall system behaviour but, without a proper integration into everyday operations, they will not adequately address all aspects of error and accident prevention.

3.2 The Aviation Industry

The commercial aviation industry has attained a very low accident rate of about 6 accidents per million aircraft departures [8]. The industry has gone to great lengths to train, manage, develop procedures, design safety systems and conduct flight operations to achieve this. But there is an inherent risk in flying, and there is a strong influence of human factors in the work of pilots, mechanics and ground controllers. Basic mistakes still occur, such as the jet aircraft running out of fuel over the Azores due to a human - caused leak, finally gliding to an emergency landing without any engine power, or the midair collision of two modern jets over European airspace, again due to human actions, in full view of a distracted ground control and with collision warnings sounding in *both* aircraft. These two very recent examples and the continued incidences of near misses demonstrate how already-known hazards are effectively ignored as we continue to try to continue to operate our technological systems.

The industry's failure rate has reached a plateau. Unless this rate is reduced, given the anticipated increase in traffic volume, there could be one major accident per week within 10 years (see

Figure 1). Detailed comparison with other data from many other high reliability industries around the world [9] suggests that the aircraft industry has reached a minimum failure rate, which cannot be lowered further without a significant change in technology. In 2001, Transport Canada introduced the concept of Safety Management Systems [10] with the aim of breaking through that minimum by focusing on the contribution from institutional failures.

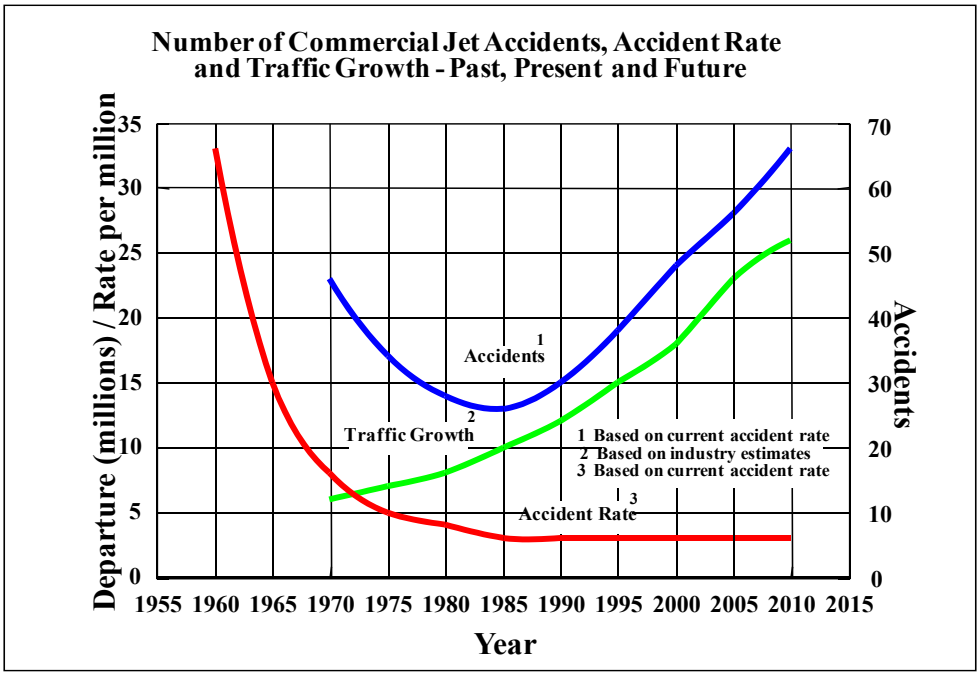

Figure 1: Accidents and accident rate in the aviation industry

3.3 The Nuclear Industry

The nuclear and aviation industries share many of the same challenges. There is the same very high level of attention to safety management, a similar low rate of events, and the attainment of a similar plateau in event rate. Despite this success, the Davis Besse incident, mistakes like leaving foreign material in the primary circuit, and other preventable events, continue to occur. As in the case of the anticipated increase in commercial aviation traffic volume, the number of nuclear plants can be expected to double over the next 20 years, and the rate of events is unlikely to decrease without a step change in the way business is conducted. Hence, the number of real events could also double. In the case of the nuclear industry, one really serious event, anywhere in the world, is likely to have a serious impact on the entire industry and could potentially halt the so-called nuclear "Renaissance".

What is the overall risk is? Probabilistic Safety Assessments (PSA) tell us that the risk of a severe accident in existing plants is likely less that 10^{-5} year^{-1}, and less than 10^{-7} year^{-1} in new plants. Allowances for human errors - in terms of individual errors - are incorporated in many of these analyses. What PSA does not currently model, however, is the influence of institutional failures; and institutional failures constitute over 70% of the contributing factors to real accidents.

As previously discussed, institutional failures can lead to a number of otherwise independent events, so they could be seen as a type of "common cause" failure mode. Therefore, one can safely assume that the likelihood of a serious accident, whilst still very low, will be higher than that suggested by PSA.

Achieving a significant reduction in the rate of serious accidents requires a renewed and concerted approach on the part of the entire industry. New designs with increased inherent safety are part of this effort. But, as for the aviation industry, the nuclear industry has also recognized the importance of human, organizational and cultural factors and is introducing Safety Management Systems (SMS) as a means of specifically reducing risks associated with institutional failures.

Furthermore, industry experience, as confirmed through the analysis of a very large amount of real data [9], shows that we will not be able to reduce the institutional failure rate unless two things occur:

- Safety Management Systems are put in place that really do what they are intended to do, so that learning from experience is a continuous, unrelenting process, thereby achieving a high level of safety culture; and
- A successful monitoring system is implemented to continuously monitor real operational risks and the performance of the Safety Management Systems established to manage those risks

4 Safety Management Systems

4.1 From Prescriptive Safety Management to Safety Management Systems

One can broadly identify two broad phases through which organizations have evolved in their quest for a high level of safety:

- Prescriptive safety management, also known as the command and control safety management phase. Under this regime, personnel do as they are told, and faith is placed in the ability of the organization to properly define the safe operating parameters and train its personnel. Questioning of the rules is not an option.
- The safety programs phase. In safety programs, error prevention is primarily team-driven within the framework of single-focused programs, each targeting one or a set of error-producing factors. Examples include Total Quality Management (TQM) programs, risk management programs, early human factors programs, etc. This approach greatly improved safety performance, but still failed to prevent some serious accidents that seemed to defy the basis for the implementation of such programs (programs appeared effective when considered individually but accidents still happened, revealing "holes" in the accident prevention - the "Swiss cheese" effect). This is roughly where we now stand.

It is generally accepted that the next step change in the management of safety is the introduction of a systemic (as opposed to just systematic), process-based approach to managing safety. This is what is now referred to as a Safety Management System (SMS). The core philosophy of SMS is that safety needs to be looked at as an integrated core business process.

In practice, SMS is an integrated process-based management system. SMS is designed to integrate all other types of safety programs, human factors tools and safety culture initiatives into a consolidated and harmonized system of processes. SMS processes are focused on operational risk management and rely heavily on the expertise of all levels of employees, from front-line workers to managers, from administrative to field staff, to identify and manage risks. It is aimed at enhancing communication of safety issues across all organizational and functional entities, promoting a good understanding of the operational risks at all levels, fostering a learning culture based on behavioural adherence to safe practices, and providing the systems and tools to allow an effective integration of risk-based information and decisions.

At its core, SMS is based on a standard business management cycle: the Deming PLAN-DO-CHECK-ACT (PDCA) cycle. The essence of SMS is based on *understanding the risks* and *promoting a learning organization*. Risk is understood through a systematic design and operational hazard identification and risk assessment, it is communicated to all levels and all areas of the organization, and it is managed in an intelligent, risk-informed framework, where people understand the "why's" and the goals of what they are doing, not just the "what". Hence SMS is a process- and performance-based way of managing safety.

SMS does not replace existing processes and programs; it integrates them. The importance of SMS has been recognized by the chemical industry, by the aviation sector (through, for example, the introduction of SMS regulations in Canada and internationally starting in 2002), and by the nuclear sector (through the publication of SMS standards by the IAEA in 2006). It is argued that only through the introduction of a system's approach to safety management, in concert with safety culture enhancement programs, can accident rates in high-reliability industries be further reduced.

4.2 What Does SMS Look Like in Practice?

In practice, SMS presents itself as a system of performance-based processes with well-defined expected outcomes. Together, these processes should cover the entire spectrum of activities that can affect risk. As can be expected, there are several ways to group and present those processes. Table 1 shows example of SMS structures. Most of these focus specifically on safety processes that are intended to be integrated into the existing business and operational processes. IAEA guidance on this subject, report GS-R-3 [11], is more comprehensive and calls for the integration of all business and operational processes, with safety, (amongst other considerations), representing one of the elements to consider in the integration. For this reason, the IAEA "SMS" model is more a standard for the overall management system than for just the management of safety.

Table 1: Different faces of the SMS structure

OHSAS 18001	**Transport Canada**
▪ Policy ▪ Planning o Hazards analysis and control o Identification of requirements o Safety objectives ▪ Implementation o Responsibilities and accountabilities o Competence and training o Communication and participation o Documented processes o Documentation control o Operational control o Emergency management ▪ Checking o Monitoring and performance measurement o Evaluation o Investigation o Records management o Internal audits ▪ Review o Review of inputs o Assessment of the management review o Management strategy o Communication of management review output	▪ Safety management plan o Safety policy o Non-punitive reporting policy o Roles, responsibilities and employee involvement o Communication o Safety objectives and goals o Performance measurement o Management review ▪ Document management o Identification and maintenance of applicable regulations o SMS documentation o Records management ▪ Safety oversight o Reactive processes o Proactive processes o Investigation and analysis o Risk management ▪ Training ▪ Quality assurance ▪ Emergency preparedness
IAEA GS-R-3	**International Civil Aviation Organization**
▪ Management system: general ▪ Management system: documentation ▪ Management commitment ▪ Satisfaction of interested party ▪ Organizational policies ▪ Planning ▪ Responsibility and authority for the management system ▪ Monitoring and measurement ▪ Self assessment ▪ Independent assessment ▪ Management system review ▪ Non conformances and corrective and preventive actions ▪ Improvement	▪ Safety policy and objectives o Management commitment and responsibilities o Safety accountabilities o Appointment of key personnel o Implementation and management o Documentation ▪ Safety risk management o Hazard identification o Risk assessment and mitigation o Internal safety investigations ▪ Safety assurance o Safety performance monitoring o Management of change o Continuous improvement ▪ Safety promotion o Training and education ▪ Safety communication

4.3 What Is Different?

As discussed above, in spite of the adoption of a large panoply of safety programs, many organizations still function in silos, and lateral communication between the silos, as well as

vertical, two-way communication within the silos, are often inexistent or inefficient. The aim of SMS is to break down these silos by providing mechanisms and processes that specifically address the need to integrate the "silo-ed" programs. Therefore, one of the main differences with previous approaches is the emphasis of SMS on integration and harmonization.

SMS is not a new program; it is intended as an integrator of existing programs. Hence, one of the aims of SMS is to simplify, consolidate and rationalize existing safety processes based on a common understanding of all risks associated with design, operations and maintenance. Under SMS, management processes are defined in terms of outcomes, and their interfaces are well defined and understood by all personnel. Traditional programs such as Operational Experience (OE or OPEX), human factors and human performance, risk assessment, quality management, safety communications, awareness program, awareness campaigns, etc. remain needed and are specifically addressed by the SMS requirement, but with an additional emphasis on the need for their full integration.

SMS also promotes a slightly different ownership of safety issues by focusing on the integration into line management of many of the risk management aspects traditionally reserved for specialists. Merlin Preuss, Director General of the Canadian Civil Aviation, was the first in Canada to implement SMS as a regulatory requirement. In one of the first national conferences on SMS, held in Calgary in 2006, he made the bold statement that one of the clues that SMS is alive and well in an organization is when the organizational chart no longer shows a "safety manager" or safety division in charge of all that is "safety". In other words, SMS recognizes that the responsibility for managing safety lies squarely in the hands of the operational line managers, and that the role of the "safety office" is to support, and not to manage safety.

Under SMS, hazard identification, risk assessment and risk control are disciplines that focus very much on operational risk and explicitly involve personnel at all levels within the organization and across all functional areas. Risk assessment, traditionally performed by "experts", is seen as a core activity involving all levels of personnel.

In more traditional safety programs, the emphasis is placed on the effectiveness of each program, the success of each being measured in quasi-isolation. In SMS, not only is the effectiveness of each process important, but the interaction between all processes and the overall performance of all processes in combination is explicitly considered in the overall evaluation of the system performance.

The safety management system frameworks discussed above are just that: frameworks. More important than the processes are the results achieved. SMS guidance and regulation generally recognize that there is an inherent risk in the fact that SMS may be perceived as a collection of processes that have to be implemented to meet regulatory obligations. To avoid this, most SMS-based requirements and standards are performance-based and require that the desired outcome of the system and its processes be *measured*, and that performance indicators be a true (as much as possible) reflection of the real operational risks. Defining what needs to be measured is thus a major challenge in the implementation of SMS.

5 Predicting Errors: the Measurement of an Organization's Safety Performance

As we have seen, all major events typically go through similar phases [9], and all involve the inextricably interwoven and inseparable contribution of humans with the technological system in which they operate and gain experience. Regardless of the system being examined, there are precursors, or prior events, which occur before a major event occurs. This data, as well as observations of major events themselves, if properly analyzed, can yield information on the likely risk of future events.

Predicting outcomes and the probability of success, failure or risk of a system or industry can have very real consequences for those who manage such systems. In today's legalistic and litigious world, learning from previous errors is the only sure way for corporations, managers and organizational governance to demonstrate that they are undertaking responsible actions, using due care and pursuing the relentless intention to improve.

As illustrated in the case of the BP refinery accident, in practice, organizations often have no means of properly assessing what their ***operational*** risk level is, or how well (or poorly) their safety management system is working. The focus is often on indicators such as lost-time accidents and this, the Baker Panel found, is wholly inadequate. In a complex homo-technological system, it appears essential to have reliable methods of how well an organization's safety intentions are actually being achieved. Without such a measurement, managers have little reliable feedback to assist them in understanding how well their safety management is working, i.e. whether or not the processes, procedures, training and attitudes that are being promoted have taken root. Duffey and Saull [9] have developed methods of analysis of outcomes data that would predict the probability of future incidents based on past history, and whether or not the institution is still learning. The data show very clearly that the probability of an accident steadily decreases ***if*** an organization learns from its own and others' experience. It eventually reaches a minimum value, consistent with a high level of safety culture. These data can also be used to infer when learning is not occurring; if the error rate is not declining with experience, the organization is not learning from experience, and the Safety Management Systems are not functioning as they should.

A significant challenge in the measurement of safety is choosing the right events or outcomes to be measured. In this respect, the nuclear industry can learn from the progress achieved in other industries, notably the Norwegian oil and gas industry [12]. It is outside the scope of this paper to present a detailed treatment of these techniques; suffice it to say that it appears there are ways to obtain a continuing measure of the success of an organization's safety management that builds on, and improves current performance measurement strategies.

6 Main Challenges in SMS Implementation

SMS implementation has proceeded in the commercial aviation for the past seven years. Our experience in this program indicates that the transition from a traditional, compliance-based safety program to a performance-based SMS is not an easy one. The following are ten of the top challenges that have been encountered in our work on SMS implementation.

1) SMS is a system of systems. To know if it works, we need to assess the system as a whole. This calls from a shift from program audits to integrated, systemic assessments of the entire suite of management processes. This requires a change in the industry and regulatory culture of program evaluation.
2) Many organizations feel that they are already doing it. This is especially prevalent in heavily regulated industries, where there are a large number of (often mandatory) safety programs, seemingly covering all aspects of safety management, and sometimes with a significant degree of overlap. SMS is thus perceived as an unnecessary burden. However, our experience indicates that the degree of integration between these various programs is often weak and that SMS can help reduce the program overhead and improve their effectiveness.
3) "If it ain't broke, don't fix it". Many organizations feel that past safety records are clear indications that existing programs work, and that the introduction of SMS could actually increase the risks. However, many organizations lack the instruments and the systems to detect the presence of latent organizational weaknesses that often act as precursors to serious accidents, and, as the Baker report noted, the safety indicators used may not actually measure what managers think they measure.
4) The "silo" effect. In many organizations, the degree of organizational integration between functional entities is lacking, with a resulting lack in the integration of management processes, in particular safety management, and deficiencies in the identification of systemic hazards and risks. For these organizations, SMS has to correct a well-entrenched culture.
5) Risk assessment is often considered a specialized discipline (e.g. PSA) carried out by experts and used to define an operating envelope that can provide a somewhat false sense of security for the operational staff. This approach may not take into account the operational knowledge of front-line personnel, the operating environment and the actual processes and practices. SMS attempts to broaden risk assessment activities to include the input of a wider cross section of employees.
6) Lack of buy-in. This is a cultural issue. In many cases, personnel follow procedures because they have to, not because they want to, and not because they understand the rationale. SMS aims at involving staff at all levels in the development of procedures and processes, as well as in the assessment of the risks.
7) Organizations often put an undue emphasis on the processes, sometimes to the detriment of the expected results. In such cases, SMS can become a collection of processes, or simply just another process that adds to the already cumbersome family of procedures that have to be followed.
8) Putting the cart before the horse. SMS introduction campaigns sometimes promote the concepts well before the organization is ready to proceed with the full integration of the SMS

tools. This often gives rise to the perception that SMS is just another "management flavour of the month".

9) Management does not always get the full picture. In an effort to "manage" safety-related information, there is often a tendency to under-filter it, thereby diluting important safety and regulatory issues, or over-filter it, with a resulting masking of important safety issues. Prioritization and the identification of key and meaningful safety performance indicators is a crucial element of a successful SMS.
10) The regulator is part of "the system" and must adapt its own regulatory style to the SMS philosophy of continuous improvement, learning from experience and integrated assessment. Therefore, it is always important to address the regulatory culture and processes concurrently with the introduction of SMS in the industry.

7 Conclusions

Institutional failures represent by far the greatest single contributing factor to major accidents and incidents in high reliability industries. If the probability of a serious accident in a nuclear reactor is to be reduced, the rate of institutional failures must be reduced. Achieving a safe design and meeting all the regulatory requirements will NOT, on their own, achieve this result. The expected doubling of the nuclear fleet worldwide over the next 20 to 30 years puts the nuclear industry in the same position as the airline business was a few years ago. For the nuclear industry to achieve a rate of serious accidents that is so low that the risk no longer imperils the future of the entire nuclear industry, and to maintain that low rate for the entire life of a plant, require a concerted effort, industry-wide, to make the risk of institutional failures very small. The data shows that the only way this can be achieved is by continuously learning from experience and by adopting a system's approach to the management of safety.

We believe that the likelihood of a serious event is higher than is commonly believed and that new techniques are needed to both bring existing rates down and to deal with the expectations of the future. The Safety Management System approach is presented as a way to achieve this accident rate reduction. This approach, supported by the development and analysis of real performance data, represents the best option we have today.

8 References

[1] Reason, James, *Human Factors: A Personal Perspective*, Presentation to the Human Factors Seminar, Helsinki, 13 Feb 2006.

[2] Lord Cullen, *The public inquiry in the Piper Alpha Disaster*, Department of Energy, UK, 1991.

[3] J. Mogford, *Fatal Accident Investigation Report, Isomerization Unit Explosion, Final Report*, Texas City, Texas, USA, 9 December 2005.

[4] James A Baker et al, *The Report of the U.S. Refineries Independent Safety Review Panel*, Jan 2007.

[5] Moshansky, V.P., *Commission of Inquiry into the Air Ontario crash at Dryden, Ontario*, Ministry of Supply and Services, Ottawa, Canada, 1992.

[6] USNRC, *Davis Besse Reactor Vessel Head Degradation Lessons Learned Task Force*, September 2002.

[7] Howlett II, H.C., *The Industrial Operator's Handbook*, Techstar/Gary Jensen, Pocatello, Idaho, USA, 1995.

[8] NSTB press release, SB-09-13, 2 April, 2009.

[9] Duffey, Romney B, Saull, John W., *Managing Risks- The Human Element*, Wiley, 2008.

[10] Transport Canada, *Introduction to Safety Management Systems*, TP13739, Minister of Public Works and Government Services, Ottawa, April 2001.

[11] IAEA, *The Management System for Facilities and Activities*, Safety Requirements No. GS-R-3, Vienna, 2006.

[12] Petroleum Safety Authority, *Trends in Risk Levels, Summary Report, Norwegian Continental Shelf Phase 7*, Norway, 2006.