PARALLEL SESSIONS ON

A SYSTEMIC APPROACH TO SAFETY

Papers submitted

PAPERS SUBMITTED FOR PARALLEL SESSIONS ON A SYSTEMIC APPROACH TO SAFETY

N. MESHKATI − Operators’ Improvization in Complex Technological Systems: The Last Resort to Averting an Assured Disaster

F. L. DE LEMOS − Evaluating Safety Culture Under the Socio-technical Complex Systems Perspective

N. GOTCHEVA − Enhancing Safety Culture in Complex Nuclear Industry Projects

J. SVENNINGSSON − Making Safety Culture a Corporate Culture: Modern Safety Thinking

F. MEYNEN − Perspective on Human and Organizational Factors (HOF): Attempt of a Systemic Approach

G. WATTS − Reinforcing Defence in Depth: A Practical Systemic Approach

T. COYE DE BRUNÉLIS − Operational Human and Organizational Factors Practices in the AREVA Group to Face New Challenges

J. WARD − The Application of Systemic Safety for Smaller Nuclear Installations

OPERATORS' IMPROVISATION IN COMPLEX TECHNOLOGICAL SYSTEMS: THE LAST RESORT TO AVERTING AN ASSURED DISASTER

N. MESHKATI
University of Southern California
Los Angeles, United States
Email: meshkati@usc.edu

Y. KHASHE
University of Southern California
Los Angeles, United States

Abstract

Complex safety-critical technological systems breakdowns, which are often characterized as 'low probability, high consequence', could pose serious threats for workers, the local public, and possibly neighboring regions and the whole country. System designers can neither anticipate all possible scenarios nor foresee all aspects of unfolding emergency. Front-line operators' improvisation via dynamic problem solving and reconfiguration of available recourses provide the last resort for preventing a total system failure. Despite advances in automation, operators should remain in charge of controlling and monitoring of safety-critical systems. It is concluded that human factors and safety culture can make or break nuclear power plants or other safety-critical systems. Operators' individual mindfulness and improvisation potential need to be nurtured and cultivated by the organizations that operate such systems; and regulatory regimes should envision, encourage, and enforce them. Furthermore, at the time of a major emergency, operators will always constitute the society's both the first and last layer of defense; and it is eventually their improvisation and ingenuity that could save the day and avert a disaster.

> *"One thing comes through very clearly from this attempt to identify the main ingredients of heroic recovery: if there is one single most important contributing factor it is having the right people in the right place at the right time… But these individual ingredients did not appear altogether out of blue. They had to be selected for and then trained, nurtured and supported by the organizations that the heroic recoverers served."*
>
> *Professor James Reason [1, p.236]*

Prologue

The above epigraph succinctly captures the essence of our contention and analysis in this paper. It is an excerpt from a conclusion of Professor James Reason's seminal book, *The Human Contribution: Unsafe Acts, Accidents and Heroic Recoveries* [1]. It also sets the stage for our *further* discussion; as he has extensively analyzed major ingredients of 11 "heroic recoveries" from assured major failures or disasters. And concluded that a heroic recovery is made of amalgamation of "training"; "discipline and leadership"; "sheer unadulterated professionalism"; "luck and skill"; and "inspired improvisation" (p, 221).

[Professor Reason, who is considered a foremost authority in human error and organizational systems' failure analyses, is the author of numerous scholarly articles and several other renowned books including *Human Error* [2]*, Managing the Risks of Organizational Accidents* [3], and *A Life in Error* [4]. His "Swiss Cheese Model" (SCM) of accidents, which was formally introduced and elaborated in late 1980's [2] was/is nothing less than a total "paradigm shift" [5] in study of complex human-organization-technology systems failures. The SCM and Professor Reason's other pioneering concepts on safety culture, system resiliency, etc. have become the foundation for other models which followed suit that can be considered as masterful renditions of his many original creative compositions. "For example, in 2000 Shappell and Wiegmaan adapted the Reason model to develop the Human Factors Analysis & Classification System (HFACS), and incident/accident analysis methodology sponsored by the Office Aviation Medicine of the US Federal Aviation Administration" [6, p. 2]. The European Organization for the Safety and of Air Navigation (EUROCONTROL Agency), after the tragic midair collision of two large aircrafts over the sky of the city of Überlingen, Germany, which resulted in 71 fatalities, organized a two-day workshop in September 2004 and published a report entitled "Revisiting the "Swiss Cheese" Model of Accident [6] which extensively discussed the evolutionary process, applications and outreach of the SCM. Professor Reason's SCM and other concepts are presently utilized by nuclear power, aviation, railroad, maritime, petrochemical and refinery, offshore drilling, healthcare, and many other industries throughout the world.]

Moreover, we are extremely pleased and proud to come across the following related gracious "End Piece" in Professor Reason's upcoming book, *Organizational Accidents Revisited* [7, p. 135]:

> *"I cannot end without once more expressing my enormous indebtedness to Professor Najmedin Meshkati and his coauthor, Yalda Khashe. Their paper, 'Operators' Improvisation in Complex Technological Systems: Successfully Tackling Ambiguity, Enhancing Resiliency and the Last Resort to Averting Disasters', was published in the Journal of Contingencies and Crisis Management [8]. In 2008, I wrote a book entitled The Human*

> *Contributions: Unsafe Acts, Accidents and Heroic Recoveries. Their paper goes well beyond what I wrote there or had thought about."*

The following is a revised version of our above-mentioned paper, which was originally published in the Journal of Contingencies and Crisis Management (JCCM).[1] It includes a new section entitled "Other Lesser-Known and Unsung Heroes of Improvisation", a modified Conclusion, and an additional new Epilogue on the vital role of human factors and safety culture in nuclear safety, entitled: "From SL1 to Onagawa and Beyond".

> *"Operators are maintained in [complex technological] systems because they are flexible, can learn and do adapt to the peculiarities of the system, and thus they are expected to plug the holes in the designer's imagination." -Professor Jens Rasmussen [9, p. 97].*

1. INTRODUCTION

The 2009 astonishing emergency water "landing" and safe evacuation of US Airways Flight 1549 has been called the "Miracle on the Hudson." Notable American philosopher and psychologist William James (1842-1910) stated with prescience that "great emergencies and crises show us how much greater our vital resources are than we had supposed" (emphasis added). This moment of celebrity and celebration is a focused moment to consider the greater factors (and actors) that converged and created this and other un-choreographed but beautiful ballet of rescue and survival.

The Presidential Policy Directive (PPD) 21 [10], defines resilience as the ability to "prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions." This is similar to the generic definition of resiliency, as "the power or ability to return to the original form, position, etc., after being bent, compressed, or stretched; elasticity." Without understanding the vital role of human and organizational factors in technological systems and proactively addressing/facilitating their interactions during unexpected ("beyond design basis") events, recovery will be a sweet dream and resiliency will only be an unattainable mirage.

Moreover, improvisation is considered as an "engine" of resiliency [11]. Improvisation in safety critical situation, which inhabits ambiguous information, could result in either mitigation or prevention of catastrophic system failures or a

[1] [The original JCCM article is reproduced with a written license (number 3778870650952, December 30, 2015) from the JCCM's publisher, John Wiley and Sons.]:

less favorable outcome [12]. In order to create an environment that fosters successful improvisation, numbers of factors such as expertise, teamwork quality, training and information flow and feedback have to be in place [13]. Two examples of successful improvisation, which averted assured disasters, were the landing of flight 1549 and restoration of Fukushima Daini nuclear power station after the 2011 Tōhoku earthquake and tsunami, which are the main focus of this paper.

2. US AIRWAYS FLIGHT 1549 AND FUKUSHIMA DAINI NUCLEAR POWER STATION

The cast of heroes did a fantastic job on that fateful day. Capt. Chesley B. 'Sully' Sullenberger III, and his first officer, Jeffrey Skiles have been appropriately saluted for one of the greatest feats of skillful airmanship ever seen. The many years of regular and simulation-based crew training and assessment that these crews had received prepared them to respond professionally to the rapid sequence of unexpected adverse events. According to Ms. Kathryn O. Higgins, the assigned National Transportation Safety Board (NTSB) member, the "very senior flight attendants" was one of the main reasons everyone survived after "landing" (or ditching) on the Hudson. She observed that "This is a testament to experienced women doing their jobs, because they were, and it worked."

The landing of flight 1549 was a great example of a successful improvisation in the face of ambiguous information portraying an 'amazingly good' crew co-ordination on the flight deck "considering how suddenly the event occurred, how severe it was, and the little time they had to prepare." This shows particularly on the non-verbal communication between Captain Sullenberger and first officer Jeff Skiles, although they "did not have time to exchange words" through "observation" and "hearing", they knew that they were on the same page. At the NTSB hearings Captain Sullenberger mentioned the critical role of "a dedicated, well-experienced, highly trained crew that can overcome substantial odds, work together as a team" [14].

Other heroes include air traffic controllers at New York Terminal Radar Approach Control (TRACON), who so calmly and professionally communicated with and helped the crew of the Airbus in their critical decision-making during the emergency.

The New York rescuers that included ferries, tugboats, Coast Guard and others who, prompt in their arrival and bravely facing the deadly cold, picked up the passengers and crew from the floating airplane, performed the final act.

However, what else made this "miracle" possible? The invisible "glue" that made these different, independent operational entities rapidly assembles and coordinate together in a seamless fashion revolves around the concept of the High Reliability Organization (HRO). For twenty years, we have been conducting research to understand these organizations, which operate relatively error free, over long periods of time, and make consistently good decisions that result in high quality and reliable operations.

Another incident that was nothing short of a miracle was the restoration of four nuclear reactors at the Fukushima Daini plant. After the 2011 Tōhoku earthquake and tsunami, the four reactors at the Fukushima Daini Nuclear Power Plant automatically shut down. The heroic act of a dedicated group of human operators, who went out of their way and by encountering multiple sources of hazards and harms, taking personal risk, and by relaying on their ingenuity, teamwork, sensemaking, and dedication despite all odds, brought all four reactors to cold shutdown and consequently averted the second assured nuclear disaster in Fukushima prefecture with serious implications for travelling fallouts to Tokyo and need for its evacuation [15].

The Superintendent of the Fukushima Daini Nuclear Power Station, Mr. Naohiro Masuda, and his operators resorted to improvisation to save the day after experiencing station black out; and their improvised acts are too numerous to mention. Nevertheless, the most memorable noteworthy ones include, “flexibly applying EOPs” [16], and “temporary cable of 9 km length was laid by about 200 personnel within a day. Usually this size of cable laying requires 20 personnel and more than 1 month period.” [17] Their personal sacrifices and dedication of staying in the plant and continuing working in dire conditions, while not knowing whether their families survived the earthquake and tsunami, and working relentlessly to bring the four reactors to the cold shutdown state, is of epic proportion. These operators, who certainly are *unsung heroes*, deserve to also be considered as national heroes of Japan [18]. Their problem solving behaviour was the perfect examples for a successful knowledge-based level of cognitive control (for further information, pleases see the following SRK-Framework).

Fukushima Daini operators once more verified and exemplified the notion that at the time of a major accident at a complex, large scale technological systems, such as a nuclear power plant, human operators always constitute the society’s both the first and last layer of defence. The recently released seminal report of the U.S. National Academy of Sciences (NAS*), Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants* [19], which of course for obvious reasons has focused more on Daiichi, affirmed this important fact:

> *"The Fukushima Daiichi accident reaffirms the important role that people play in responding to severe nuclear accidents and beyond-design-basis accidents more generally... Recovery ultimately depended on the ingenuity of the people on the scene to develop and implement alternative mitigation plans in real time...There is a growing evidence that people are a source of system resilience because of their ability to adapt creatively in response to unforeseen circumstances...The Fukushima Daiichi accident*

> *reaffirmed that people [human operators] are the last line of defense in a sever accident."* (Emphasis added, p. 1& 3)

3. OTHER LESSER-KNOWN AND UNSUNG HEROES OF IMPROVISATION

Professor James Reason in one of his aforementioned seminal books [1], provided an excellent analysis of 11 heroic recoveries by "people" - human operators - in different domains and systems. The number of reported heroic recoveries, thanks to skillful improvisations of many deft pilots such as Captain Sullenberger as described before, in the civil aviation is much more than other industries. A major reason, of course, could deal with the nature of this international industry, its openness and exposure to public and media scrutiny.

Reason has extensively discussed 11 heroic recoveries, which included the most renowned aviation recovery before Captain Sullenberger's recovery [1]. It was solely because of the masterful improvisation of Captain Al Haynes on July 19, 1989, who recovered his crippled flight and averted an assured total disaster. While flying at cursing altitude, his McDonnell Douglas DC-10 tail-mounted engine fan rotor disintegrated and cut through all three of the aircraft's hydraulic systems. "The probability of losing all three hydraulic systems was considerable by the designers to be less than one in a billion (10 to the power of -9) and no emergency procedures were able to cover this almost unthinkable possibility" [1, p. 200]. Captain Haynes instinctively and skillfully operated engine throttles to stabilize the aircraft attitude and used the differential thrusts of the two remain wind-mounted engines to navigate the almost disabled aircraft into Sioux City, Iowa airport. His actions saved lives of 184 (out of 296) people who were aboard.

There are two equally noteworthy, however lesser known cases of aviation recoveries owing entirely to pilots improvisations, from Iran and Australia, that fit our discussed pattern.

On November 20, 2002, Captain Alireza Kooshki was in command of a Saha Air (aged) Boeing 707 with 170 passengers and crew on a flight from Iran's capital city of Tehran to Asalouyeh, a small city on the Persian Gulf coast. While during the landing, at 700ft, he faced inflight structural breakup. The whole flap on the left wing was torn apart, became separated from the aircraft due to metal fatigue of the ageing aircraft (reportedly it had more than 70,000 hours of service), which also caused its hydraulic control systems to fail. It was only due to Captain Kooshki and his two cockpit crew member's remarkable flying skills, performance, and improvisation that after 30 minutes of daring manoeuvres, he was able to land the crippled aircraft safely on the ground with no injuries [20].

On November 4, 2010, Captain Richard Champion de Crespigny was the Pilot in Command of Qantas Airbus A380 flight with 440 passengers and 29 crew from Singapore to Sydney, Australia when he faced uncontained engine failure [21]. The aircraft had also suffered damages to the nacelle, wing, fuel system, landing gear, flight controls, the controls for engine No. 1 and an undetected fire in the left inner wing fuel tank that eventually self-extinguished[2]. Despite the severe damage to multiple subsystems, Captain de Crespigny was able to bring the aircraft to an emergency landing at Singapore Changi Airport; all 469 people survived with no injury. A major lesson that Captain de Crespigny has learned and also detailed in his book about this accident can be summarized in his words, as: "Technology cannot replace pilots yet. Pilots must expect the unexpected, anticipate failures and have the confidence and courage to recover their aircraft when the unthinkable happens" [20, p. 3].

Another case of life-saving improvisation which saved 211 workers and asset is about a Central Azari offshore platform (operated by the BP) in the Caspian Sea, which experience a major gas leak on September 17, 2008. According to Palast [22, p. 81], the platform was "engulfed in methane, exactly the same as the [BP] Deepwater Horizon. A quick-thinking captain on Central Azari ordered the platform to "go dark." So no lights, no sources of flame, not even a light switch flicked." It has been contended that had the BP Deepwater Horizon did the same thing on April 20, 2010, when they "smelled gas", as the Central Azari platform did, before the runaway flammable gas reached the platform, the disaster that killed 11, injured 16, and spilled nearly 5 million barrels of oil into the Gulf of Mexico, could have been prevented.

There are certainly many more noteworthy cases of front-line operators' improvisations and recoveries from system failures which are unfortunately either not documented or reported to public from many safety-sensitive industries throughout the world. Nevertheless, a common observed pattern among most aforementioned cases studies were all revolved around successful actions taken by the front-line people. (As Gladwell [23, p. 115] suggested, "Bad improvisers block actions, often with a high degree of skill. Good improvisers develop action.") Other common issues among all case studies deal with perceiving the critical elements in the current situation; understanding the significance of these elements; and making projections as to their future status. "All three of these factors are essential for successful recovery; but, of these, situational awareness is the most important…good situational awareness is a prerequisite for survival in all potentially hazardous domain" [1, p. 223].

4. COMPLEX TECHNOLOGICAL SYSTEMS' FAILURES, AMBIGUITY, AND HIGH RELIABILITY ORGANIZATION

When complex technological systems, such as aircrafts and nuclear power plants, move from routine to non-routine (normal to emergency) operation, the

[2] Aviation Safety Investigation Report 089 - In-flight uncontained engine failure Airbus A380-842, VH-OQA. Australian Transport Safety Bureau, Department of Transport and Regional Services, Government of Australia.

control operators need to dynamically match the system's new requirements. This mandates integrated and harmonious changes in information presentation, changes in performance requirements in part because of operators' inevitable involuntary transition to different levels of cognitive control, and reconfigurations of the operators' team (organizational) structure and communication.

In order to survive, a technological system must have the ability to respond to operational anomalies before any undesirable consequences, which the system seeks to avoid, can occur. That is, the control structure must run at a faster rate than the environment it seeks to control; or else, the system will lose control. However, a hierarchically structured team has only a limited control model of the system, which oversees. For instance, in the case of a power plant particularly during an emergency, the operators not only comply with (EOPs), they must also respond to the changing system's environment. To the extent that for every possible deviation in this environment that has not been foreseen by the 'hierarchy,' control is transferred to the work domain level -- to operators -- and due to (their) survival needs and instincts the system's control team inevitably embraces structural forms that fit the situational demands, often the more naturalistic form such as 'self-organizing.' Moreover, the hierarchical (team) structure becomes even more counter-productive when decisions need to be made by the whole team using the 'team mind'.

As task uncertainty increases in complex systems, (typical in "non-normal" or emergency situations), the number of exceptions to routine operations increases, overloading organizational hierarchy. In order to meet the new challenges, the organization must use another mechanism to sustain itself. Furthermore, the "normal function" of tightly coupled technological systems is to operate on the boundary to loss of control. That is, people are involved in a dynamic and continuous interaction with the failure and hazard [24]. Thus, "touching the boundary to loss of control is necessary (e.g., for dynamic "speed-accuracy" trade-offs) [25]. This is a rapidly changing environment, and in order to survive it, the system should be able to respond in a safe and effective manner. Occasionally, it may require an improvised response from the operator(s), but it should certainly be coordinated and in concert with others' activities and stay within the boundaries or "space" of acceptable work performance [24]. Otherwise, it would be just *noise* in the control of the system and could lead to errors. It must also be able to flexibly reconfigure and synchronize all of its system elements to address the threatening issues. The HRO approach enables independent systems to become interdependent in a manner that any organization can accomplish. The fundamental characteristics of an HRO foster a culture of trust, shared values, unfettered communication, and process improvement. It nurtures, promotes, and takes advantage of distributed decision-making, "where the buck stops everywhere."

According to Weick and Sutcliffe [26], "hallmarks of high reliability" or major characteristics of HROs include preoccupation with failure, reluctance to simplify interpretation, and sensitivity to operations, when they are "anticipating and becoming aware of the unexpected.” In addition, when the “unexpected occurs”, HROs attempt to contain it by committing to resilience, and deferring to expertise.

Fukushima Daini and US Airways Flight 1549 are two great examples showing that HROs can detect, contain, and rebound from unexpected events. An HRO is not necessarily error free, but errors do not disable it; the system absorbs or adapts to disruptions without fundamental breakdowns. Through fast, real time communication, feedback, and improvisation, the system can restructure or reconfigure in response to external (or internal) changes or pressures. In these organizations worst-case scenarios are always imagined, modelled, and rehearsed.

In HROs, expertise is distributed and the system controller typically defers to the person with the expertise relevant to the issue they are confronting. An expert is not necessarily the most experienced or the highest ranked person; it is usually someone at the “sharp end” -- where the real work is done. In other terms, HROs aim to empowering expert people closest to a problem and shifting leadership to people who have the answer to the problem at hand.

It is the nature of complex, tightly coupled and complexly interactive systems, according to Reason [27], to spring “nasty surprises.” As case studies repeatedly show, accidents may begin in a conventional way, but they rarely proceed along predictable lines. Each accident is a truly novel event in which past experience counts for little, and where the plant is returned to a safe state by a mixture of good luck and hard, knowledge-based effort. Accident initiation and its propagation through possible pathways and branches within the system is a highly complex and hard to foresee event. It is analogous to the progression of a crack in an icy surface, which can move in several directions, hit different levels of thickness, and if not stopped, can cause the surface to break up and open (“uncover the core” and break the system).

The safe, efficient operation and resiliency of infrastructural technological systems is a function of the interactions among their three major Human, Organizational, and Technological (i.e., engineered) (HOT) subsystems. The role of each individual subsystem, which is alike a link in a chain, can determine and affect the integrity of the whole system; obviously, the chain (i.e., system) could break down if any link breaks down. Most failures of technological systems have been caused by breakdowns of the weakest links in this chain, which are most often the human or organizational subsystems. Through fast, real time communication, feedback, and improvisation, the system can restructure or reconfigure in response to external (or internal) changes or pressures. Worst-case scenarios should always be imagined, modeled, and rehearsed.

Operators’ control of complex, large-scale technological systems can be termed *coordination by pre-planned routines* [28]. However, coordination by pre-planned routines is inherently “brittle.” Because of both pragmatic and theoretical constraints, it is difficult to build mechanisms into pre-planned routines that cope with novel situations, adapt to special conditions, or recover from human errors in following the plan. When pre-planned routines are rotely invoked and followed, performance breaks down in the light of under-specified instructions, special conditions or contexts, violations of boundary conditions, human execution errors, bugs in the plan, multiple failures, and novel situations (incidents not planned for) [28]. This is the problem of *unanticipated variability,* which happens frequently during emergencies at complex technological systems. Moreover, in virtually every significant disaster, or near disaster, in complex systems, there have been some points where expertise beyond the pre-planned routines was needed. This point involves multiple people and a dynamic, flexible, and problem solving organization. Handling unfamiliar events (e.g. emergencies) also requires constant modification of the design of the organization, coordination, and redeployment of resources [29]. However, as it has been observed and reported many times, usually the pre-programmed routines of decision support in expert computing systems sets the organization in a static design [30].

Ambiguity can interfere with the coordination of pre-planned routine as people might interpret ambiguous information differently. Resilient organizations are ready to respond to unforeseen events by fostering characteristics like flexibility, creativity, and spontaneity, which are filtered through individuals' capacity to perceive, understand, and make sense of events [11]. Sense making is one the main characteristics of HROs. Studies show that HROs strive to develop the ability to identify situations that had the potential to evolve into safety critical situations by learning from previous events [31]. Experience provides individuals with a valuable pool of information and knowledge to draw on when engaging in pattern recognition, which could consequently enable them to identify leverage points to create a successful improvised solution [32].

Complex and safety-critical organizations' emphasize on order and control and reliance on routine to reduce the probability of error could suppress creativity and innovation when faced with an unexpected situation. Improvisation in such organizations could be affected by the "chronic temptation to fall back on well-rehearsed fragments to cope with current problems even though these problems don't exactly match those present at the time of the earlier rehearsal." [33 p. 551]

Ambiguity triggers innovation. If individuals and organizations shy away from ambiguity in the workplace and relationships, they would only be able to reproduce routine actions. [34] "Requisite imagination" is a required principle for a resilient organization [11].

Furthermore, it has been empirically validated that experts in high stress demanding situations do not usually operate using a process of analysis. Even their rules of thumb are not readily subjected to it; whereas most of the existing artificial intelligence-based automated systems always rely on analytical decision process. If operators of complex systems rely solely on computer's analytic advice, they would never rise above the level of mere competence -- the level of analytical capacity -- and their effectiveness would be limited by the inability of the computer systems to make the transition from analysis to pattern recognition and other more intuitive efforts [35].

5. A FEW WORDS ABOUT THE ROLE OF SKILL, RULE, AND KNOWLEDGE-BASED (SRK) FRAMEWORK IN ADDRESSING AMBIGUITY

The Skill, Rule, and Knowledge-based (SRK) model is a powerful framework for holistic analyses of different aspects of complex human-machine systems. In Moray's [36] judgment, the SRK model is "nothing less than a paradigm shift in the study of complex human-machine interactions" (p. 12). Also, according to Reason [2] "the SRK framework is a market standard for the human reliability community the world over" (p. xiii). The SRK taxonomy of cognitive processing developed by Rasmussen is a useful model for representing operator information processing [37,38]. Within this model, cognitive performance is divided into three, qualitatively different levels of processing, skill-based, rule-based, and knowledge-based behaviour, which utilize three different types of information, referred to as signals, signs, and symbols, respectively.

According to Rasmussen [38], skill-based behaviour "represents sensorimotor performance during acts or activities that, after a statement of an intention, take place without conscious control as smooth, automated, and highly integrated patterns of behaviour." The information that guides this type of behaviour is in the form of signals, which "have no 'meaning' or significance except as direct physical time-space data."

Rule-based behaviour is defined as the composition of a sequence of skill-based subroutines that are "typically consciously controlled by a stored rule or procedure that may have been derived empirically during previous occasions, communicated from other persons' know-how as an instruction or cookbook recipe, or it may be prepared on occasion by conscious problem solving and planning." Rule-based behaviour is goal directed, but "very often, the goal is not even explicitly formulated, but is found implicitly in the situation releasing the stored rules." The information that is utilized during this type of behaviour is in the form of signs which "refer to situations or proper behaviour by convention or prior experience; they do not refer to concepts or represent functional properties of the environment." "Signs can only be used to select or modify the rules controlling the sequencing of skilled subroutines; they cannot be used for functional reasoning, to generate new rules, or to predict the response of an environment to unfamiliar disturbances."

Knowledge-based behaviour occurs in situations in which a goal is "explicitly formulated, based on an analysis of the environment and the overall aims of the person. Then, a useful plan is developed - by selection, such that different plans are considered and their effect tested against the goal; physically by trial and error; or conceptually by means of understanding of the functional properties of the environment and prediction of the effects of the plan considered." Because reasoning at this level is based upon the individual's mental model of the system, this type of processing can also be referred to as "model-based" reasoning. "To be useful for causal functional reasoning in order to predict or explain unfamiliar behaviour of the environment, information must be perceived as symbols. Whereas signs refer to percepts and rules for action, symbols refer to concepts tied to functional properties and can be used for reasoning and computation by means of a suitable representation of such properties.” Symbols “are defined by and refer to the internal, conceptual representation that is the basis for reasoning and planning.”

The determination of whether skill- or rule-based processing will occur is based primarily upon the level of experience of the individual. As one is learning a new process, performance is dominated by rule-based behaviour. As these rules become internalized, however, the sequence of actions required begin to be integrated into smooth patterns, which no longer need to be consciously attended to be performed correctly. The distinction between rule- and knowledge-based behaviours, on the other hand, is generally determined by the familiarity of the current situation. In unfamiliar situations, an appropriate set of rules for action may be either unavailable or not immediately obvious. In this situation, reasoning about the state of the system will be necessary in order to determine a course of action. Once this goal is selected, processing may shift back to rule-based or even skill-based reasoning as the required steps are performed.

Improvisation implies the presence of imagination and reluctance to simplify, the ability to interpret signals in different ways and be sensitive to different variety of inputs [11]. Research shows that experience and practice improves people’s intuition and patter recognition to be more skilled-based rather than based on “potentially faulty heuristic” [32].

Skill-based behaviour and rule-based behaviour are both considered to be primarily perceptual in nature while knowledge-based behaviour is considered to be analytical in nature. Vicente and Rasmussen [39] report that results from a variety of studies indicate that perceptual processing tends to be faster and, although not as exact in its result, can lead to performance, which has lower variability than does analytical processing, which can lead to more extreme errors. This type of processing is seen as more appropriate for the often time-critical type of performance that is required of the operators of complex processes. Further, the authors state that there is some evidence that individuals attempt to utilize simple perceptual strategies in favor of analytical processing even while performing complex tasks, and that this indicates that perceptual processing is preferred to analytical processing.

At the same time, the authors note, the control of complex processes will require analytical or knowledge-based reasoning, particularly when reacting to an unfamiliar fault condition. The overall goal of ecological interface design that flows from these findings is to allow the operator to perform control tasks at as low a level of processing as possible while providing appropriate support for all three processing levels. The following guidelines have also been generated, each corresponding to a specific level of cognitive control [39].

Nuclear reactor operators’ response to nuclear power plant disturbances is shown in Figure 1 [40]. The operators are constantly receiving data from the displays in the control room and looking for change or deviation from standards or routines in the plant. It is contended that their responses during transition from the Rule-based to the Knowledge-based level of cognitive control, especially in the Knowledge-based level, are affected by the safety culture of the plant and are also moderated or influenced by their cultural background. Their responses could start a vicious circle, which in turn could lead to inaction, which wastes valuable time and

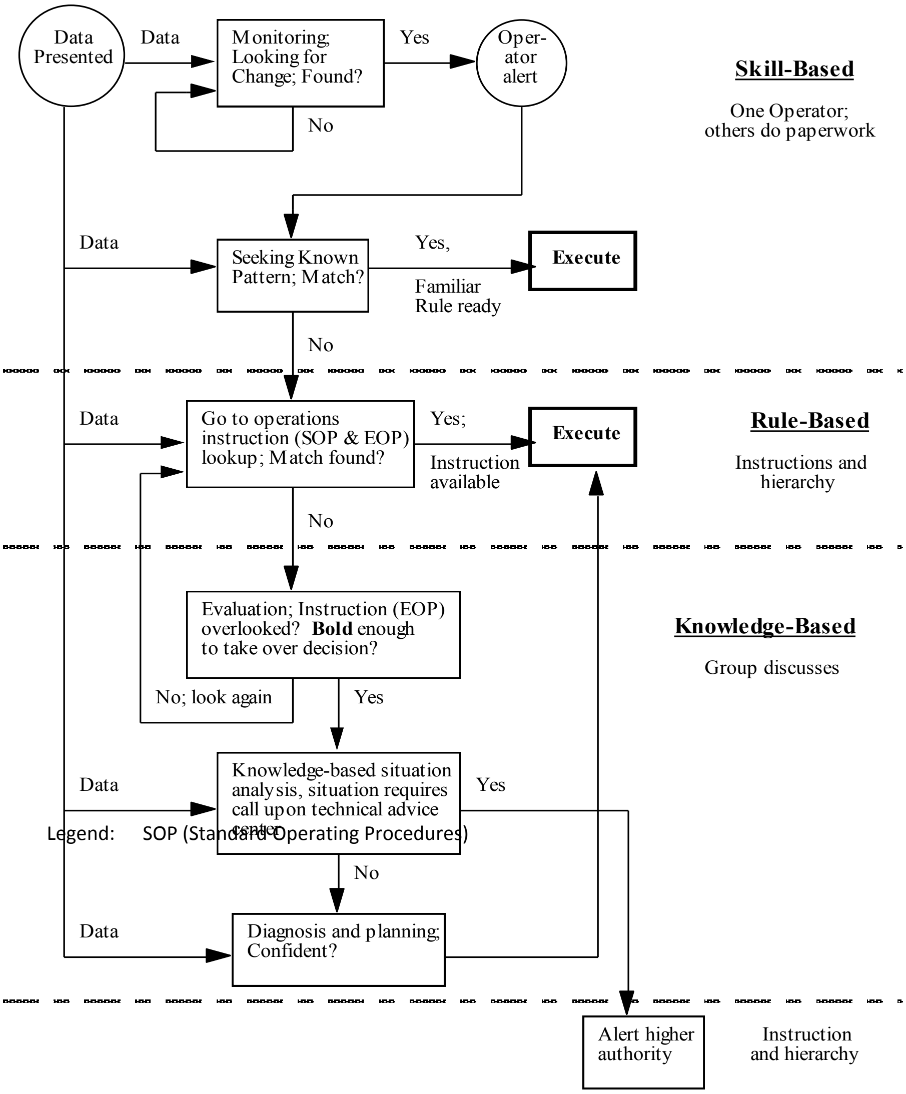

Data Presented
Data
Monitoring; Looking for Change; Found?
Yes
No
Oper-ator alert
Skill-Based
One Operator; others do paperwork
Data
Seeking Known Pattern; Match?
Yes,
Familiar Rule ready
Execute
No
Data
Go to operations instruction (SOP & EOP) lookup; Match found?
Yes;
Instruction available
Execute
Rule-Based
Instructions and hierarchy
No
Evaluation; Instruction (EOP) overlooked? Bold enough to take over decision?
Knowledge-Based
Group discusses
No; look again
Yes
Data
Knowledge-based situation analysis, situation requires call upon technical advice center
Yes
Legend: SOP (Standard Operating Procedures)
No
Data
Diagnosis and planning; Confident?
Alert higher authority
Instruction and hierarchy

FIG. 1. Model for nuclear power plant operators' responses to disturbances. (From: Rasmussen, personal communication 1992)

control room resources. Breaking this vicious circle requires 'boldness' to make or 'take over' decisions so that the search for possible answers to the unfamiliar situation does not continue unnecessarily and indefinitely. It is contended that this new situation when there is no Standard Operating Procedures (SOP) and Emergency Operating Procedures (EOP) that can be called up, requires 'boldness' to break out (from the aforementioned iterative vicious cycle) and to solve the system's problem requires improvisation. Operators need to continue to operate and control the system in a totally new and unprecedented environment and adverse conditions. They work as a team, conduct a real-time situational analysis, brainstorm, develop solutions, evaluate alternatives, and execute the most feasible and available ones immediately. Coming up with an unprecedented plan is strongly culturally driven, and is a function of the plant's organizational culture, reward system, and the regulatory environment. Boldness, of course, is also influenced by operators' personality traits, risk taking, and perception (as mentioned before) which are also strongly cultural. Improvisation requires mastery of the subject matter, a total system comprehensive (including knowledge of key components, subsystems and their potential interactions), and ability to extrapolate the behaviour of the newly "improvised" and patched up system, and to shepherd it to the safe state. Other important aspects of the national culture include "hierarchical power distance" and "rule orientation" [41], which govern the acceptable behaviour and could determine the upper bound of operators' boldness.

6. CONCLUSION

We have learned that unthinkable disasters can happen regularly; and we cannot be immune from the possibility of this fate. As such, we need to be chronically uneasy, and be constantly thinking about the unthinkable and plan for them.

As the experience of US Airways Flight 1549 and Fukushima Daini Nuclear Power Station, and other cases (e.g., Captain Al Haynes) demonstrated, operators' improvisation in the absence of computer-aided control or inapplicability of SOPs and EOPs is the last resort of averting an assured disaster and saving the day. Improvisation, in turn, is conducted at the Knowledge-based level of cognitive control and requires among others a deep, total system comprehension ("internalized knowledge") of the technological system and its interacting subsystems, along with supportive organizational framework and dedication, boldness and positive attitude of the operating personnel.

For the foreseeable future, despite increasing levels of computerization and automation, human operators will have to remain in charge of the day-to-day controlling and monitoring of complex technological systems, since system designers cannot anticipate all possible scenarios of failure, and hence are not able to provide pre-planned safety measures for every unexpected event and contingency. Professor Jens Rasmussen's earlier-mentioned epigraphic and climactic observation ("operators are maintained in [complex technological] systems because they are flexible, can learn and do adapt to the peculiarities of the system, and thus they are expected to plug the holes in the designer's imagination"), which can also be considered as the best finale for this article, has most succinctly articulated this conclusion.

7. EPILOGUE – FROM SL1 TO ONAGAWA AND BEYOND

Past events and history of sever accidents have demonstrated that human and organizational factors play a crucial/vial role in the safety of nuclear power plants around the world [29]. The accident on January 1961 at the SL1 (Stationary Low Power Reactor No. 1), located at the National Reactor Testing Station, Idaho Falls, Idaho, could be considered as one those early accidents which involved fatality. A quotation from the general conclusions as to the causes of this accident could, as well and almost exactly, be applied to the Three Mile Island and Chernobyl cases [As such, one may argue that should it be heeded, these accidents could have been prevented] [42, p. 681]:

> *"Most accidents involve design errors, instrumentation errors, and operator or supervisor errors... The SL1 accident is an object lesson on all of these... There has been much discussion of this accident, its causes, and its lessons, but little attention has been paid to the human aspects of its causes... There is a tendency to look only at what happened, at to point out deficiencies in the system without understanding why they happened; why certain decisions were made as they were... Post-accident reviews should consider the situation and the pressures on personnel which existed before the accident"*

The same theme has echoed in several reports concerning the root-causes of the Chernobyl accident. The following are a few representative samples and noteworthy snippets from credible, influential sources:

According to the International Atomic Energy Agency's (IAEA) Nuclear Safety Review for 1987 [43, p. 43]:

> *"The Chernobyl accident illustrated the critical contribution of the human factor in nuclear safety".*

According to the IAEA's Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident [44, p. 76]:

> *"The root cause of the Chernobyl accident, it is concluded, is to be found in the so-called human element.... The lessons drawn from the Chernobyl accident are valuable for all reactor types."*

It is noteworthy to revisit what Dr. Hans Blix, the legendary Director General of the IAEA said about the above-mentioned INSAG-1 stage-setting report concerning safety culture:

> *"The report is intended for use by governmental authorities and by the nuclear industry and its supporting organizations. Prepared by a highly authoritative body, it should help to promote Safety Culture. It is intended to stimulate discussion and to promote practical action at all levels to enhance safety."*

According to the IAEA's International Nuclear Safety Advisory Group (INSAG), The Chernobyl Accident Updating of INSAG-1 [44, p.24]:

> *"The (Chernobyl) accident can be said to have flowed from deficient safety culture, not only at the Chernobyl plant, but throughout the Soviet design, operating and regulatory organizations for nuclear power that existed at the time...Safety culture...requires total dedication, which at nuclear power plants is primarily generated by the attitudes of managers of organizations involved in their development and operation."*

And finally, according to the late Academician Dr. Valeri A. Legasov, the First Deputy Director of the Kurchatov Institute at the time of the Chernobyl accident, and the head of the former Soviet delegation to the Post-Accident Review Meeting of the IAEA in August, 1986, quoted in Monipov [45, p. 340]:

> *"I advocate the respect for human engineering and sound man-machine interaction. This is a lesson that Chernobyl taught us."*

It may come as a surprise to some people that the Fukushima Daiichi accident, which was caused by a natural disaster, the March 11, 2011 Tohoku earthquake and tsunami, was an anthropogenic accident. All investigations have concluded that Fukushima Daiichi was mostly preventable [46], and that the natural hazards acted only as a triggering mechanism for the ensuing disaster [47-48]. And, a recent study goes even further by asserting that "the Fukushima accident was preventable" [49]. In the words of Dr. Kiyoshi Kurokawa, chairman of the National Diet (Parliament) of Japan Fukushima Accident Independent Investigation Commission (NAIIC), Fukushima was "a man-made disaster" and "made in Japan". Because Japan's nuclear industry failed to absorb the lessons learned from Three

Mile Island and Chernobyl nuclear accidents, "it was this mindset that led to the Fukushima Daiichi disaster" [50]. Other official reports, such as the one by the US National Academy of Sciences [51], have also acknowledged and extensively discussed the instrumental role of safety culture in this accident.

Former US Nuclear Regulatory Commission (US NRC) Chairman, Dr. Allison M. Macfarlane at the International Nuclear Safety Group (INSAG) Forum (held at the IAEA, on Monday, September 17, 2012) stated:

> *"There are many lessons that we must all take away from the accident at Fukushima, but some of the most valuable extend beyond the technical aspects and are embedded in human and organizational behaviours. Among these is safety culture."*

Lars Högberg [52], who was Director General of the Swedish Nuclear Power Inspectorate (SKI) (1989–1999) and also has served as a Governor of the IAEA (and a member of the INSAG; contributed to INSAG-15, 2002) and as Chairman of the Steering Committee of the OECD Nuclear Energy Agency, has conducted an excellent thorough analysis of the root causes and impacts of three severe accidents at large civilian nuclear power plants (the Three Mile Island, Chernobyl, and the Fukushima Daiichi) has concluded:

> *"All three severe accidents discussed in this paper had their root causes in system deficiencies indicative of poor safety management and poor safety culture in both the nuclear industry and government authorities."*

However, it should be noted that Tohoku Earthquake and Tsunami on Tuesday March 11, 2011 had two drastically different impacts on TEPCO's Fukushima (Daiichi and Daini) nuclear power plants versus Tohoku Electric Power Company's Onagawa Nuclear Power Station. While the Fukushima and Onagawa power plants shared similar disaster conditions, nuclear reactor types (Boiling Water Reactor BWR, Mark I), dates of operation, and an identical regulatory regime, it was only Tohoku Electric's Onagawa power plant that went unscathed. Fukushima Daini was damaged by the earthquake and severely hit by the tsunami, but thanks to the heroic efforts of its operators and their epic improvisation managed the cold shutdown of all its four operating reactors. On the other hand, Fukushima Daiichi plant experienced a fatal meltdown and radiation release while Onagawa managed to remain generally intact, regardless of its proximity to the epicentre of the enormous earthquake.

Everyone knows the name Fukushima, but even in Japan few people are familiar with the Onagawa power station. Fewer still know how Onagawa managed to avoid a disaster. According to a report by the International Atomic Energy Agency mission that visited Onagawa and evaluated its performance, "the plant experienced very high levels of ground motion—the strongest shaking that any nuclear plant has ever experienced from an earthquake," but it "shut down safely" and was "remarkably undamaged."

Why is there such a stark contrast? How Oangawa weathered the tsunami relatively unscathed, while Daiichi didn't? Answers to these vexing questions and lessons learned are important for every operating and under-construction nuclear reactor in the world.

Most people believe that Fukushima Daiichi's meltdown was predominantly due to the earthquake and tsunami. The survival of Onagawa, however, suggests otherwise. Onagawa was only 123 kilometers away from the epicenter, 60 kilometers closer than Fukushima Daiichi, and the difference in seismic intensity at the two plants was negligible. Furthermore, the tsunami was bigger at Onagawa, reaching a height of 14.3 meters, compared to 13.1 meters at Fukushima Daiichi. The difference in outcomes at the two plants reveals the root cause of Fukushima Daiichi's failures a corporate "safety culture" [53-54].

Finally, according to a most recent voluminous report on the Fukushima accident by the International Atomic Energy Agency (IAEA) [55], the regulation guidelines and procedures were not adequate concerning safety culture, and it stated that "it is necessary to take an integrated approach that takes account for complex interactions between people, organizations and technology" [55, p.67]. And the IAEA Director General, Mr. Yukiya Amano, has asserted (p.7):

> *"There can be no grounds for complacency about nuclear safety in any country. Some of the factors that contributed to the Fukushima Daiichi accident were not unique to Japan. Continuous questioning and openness to learning from experience are key to safety culture and are essential for everyone involved in nuclear power. Safety must always come first."* (emphasis added)

It seems that human performance and organizational factors were "recurring" themes and constituting major root-causes of past sever nuclear accidents – starting from the SL1 in 1961 all the way to the Fukushima Daiichi in 2011. And Fukushima Daini was only saved because of the heroic efforts and skilful improvisation of its dedicated operators and Onagawa went unscathed because of the proactive organizational safety culture of its utility.

Thus, a most important and unequivocal lesson of the past tumultuous history of nuclear power in the world is: Human factors and safety culture can make or break nuclear power plants or any safety-critical system; and operators' individual mindfulness and improvisation potential need to be nurtured and cultivated by the organizations that operate such systems; and regulatory regimes should envision, encourage, and enforce them. Let's hope that under the IAEA's stewardship some 30 years after the Chernobyl accident, the global nuclear power industry, as a whole, has internalized the defining feature of high-reliability organizations (HRO) - “preoccupation with the possibility of failure” [56] - and has achieved the needed “collective mindfulness” [57], at both the plant and industry levels, to not only remember but also heed and operationalize the above vital lesson; otherwise, as renowned Spanish-American philosopher and essayist George Santayana [58, p. 284], pointed out:

“Those who cannot remember the past are condemned to repeat it.”

ACKNOWLEDGEMENTS

We would like to acknowledge the key role of the former Director General of the IAEA (1981-1997), Dr. Hans Blix, whose leadership and steadfast support of the safe and peaceful usage of nuclear technology in the world is legendary. We would also like to express our gratitude to distinguished Professor Jens Rasmussen and Professor James Reason, whose intellectual leadership, pioneering thoughts and innovative concepts as well as their invaluable inspiration, support and mentorship in the last 30+ years have been instrumental in our scholarly efforts. This work, which is a tribute and dedicated to these three remarkable gentlemen and their legacies; nevertheless, should not necessarily be construed as a representation of their position(s).

REFERENCES

[1] REASON, J. The Human Contribution: Unsafe Acts, Accidents and Heroic Recoveries. Ashgate Publication, Farnham, UK (2008)

[2] REASON, J. Human Error. Cambridge University Press. New York, NY (1990)

[3] REASON, J. Managing the Risks of Organizational Accidents. Ashgate Publication, Franham, UK (1997)

[4] REASON, J. Life in Error. Ashgate Publication, Franham, UK (2013)

[5] Kuhn, T. S. The Structure of Scientific Revolutions. Chicago University Press, Chicago (1970)

[6] EUROCONTROL EXPERIMENTAL CENTRE, revisiting the Swiss Cheese model of accidents, EEC Note No. 13/06, EUROCONTROL, France (2006).

[7] REASON, J. Organizational Accidents Revisited. Ashgate Publication, Franham, UK (2016)

[8] MESHKATI, N., KHASHE, Y. Operators' Improvisation in Complex Technological Systems: Successfully Tackling Ambiguity, Enhancing Resiliency and the Last Resort to Averting Disaster. Journal of Contingencies and Crisis Management, **23** 2 (2015), 90-96.

[9] RASMUSSEN, J. "What can be learned from Human Error Reports?" Duncan, K. D. Gruneberg, M. M. Wallis, D. (ed.). Proceedings of an International Conference on Changes in the Nature and Quality of Working Life. Chichester: John Wiley and Sons. (1980) 97-113.

[10] OFFICE OF THE PRESS SECRETARY, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience." The White House. February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed Octoer 2014).

[11] GRØTAN, T.O., STØRSETH F., RØ M.H., and SKJERVE, A.B. "Resilience, Adaptation and Improvisation - increasing resilience by organising for successful improvisation." the 3rd Symposium on Resilience Engineering. Antibes, Juan-Les-Pins, France (2008)

[12] TROTTER, M. J., Salmon, P. M. and LENNE, M. G. "Impromaps: Applying Rasmussen's Risk Management Framework to improvisation incidents." Safety Science, **14** 5 (2014) 60-70.

[13] TROTTER, M. J., Salmon, P. M. and LENNE, M. G. "Improvisation:theory, measures and known influencing factors." Theoretical Issues in Ergonomics Science, **64** 5 (2013) 475-498.

[14] FRAHER, A. L. "Hero-making as a Defence against the Anxiety of Responsibility and Risk: A Case Study of US Airways Flight 1549." Organisational & Social Dynamics, **11** 1 (2011) 58-78.

[15] GULATI, R., CASTO C., and KRONTIRIS C. "How the Other Fukushima Plant Survived." Harvard Business Revie, **23** 2 (2014) 111-115.

[16] KAWAMURA, S. "Lessons Learnt from Fukushima Daini NPP and Status of Fukushima Daiichi NPP." Atomexpo. June 4, 2012. http://2012.atomexpo.ru/mediafiles/u/files/Present2012/Kawamura.pdf (accessed March 4, 2015).

[17] MASUDA, N. "East Japan Earthquake on March 11, 2011 and Emergency Response at Fukushima Daini Nuclear Power Plant." IAEA. March, 2014. http://www-pub.iaea.org/iaeameetings/cn233p/OpeningSession/6Masuda.pdf (accessed March 9, 2015).

[18] MESHKATI, N. The Unsung Heroes of Fukushima. The Japan Times (2014, August 25).

[19] NATIONAL ACADEMY OF SCIENCES. Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants. NAS Committee on Lessons Learned from the Fukushima Nuclear Accident for Improving Safety and Security of U.S. Nuclear Plants, The National Academis Press, Washington D.C., 2014.

[20] THOMAS, G., On autopilot?, Austrian Aviation Journal, (2014) 2-5.

[21] De Crespigny, R., Resilience – recovering pilots' lost flying skills, Aerospace Magazine (2015) 32-37.

[22] PALAST, G., Vultures' picnic: in pursuit of petroleum pigs, power pirates, and high-finance carnivores, Dutton Adult, USA (2011).

[23] GLADWELL, M., Blink: The Power of Thinking Without Thinking, Back Bay Books, United States (2007).

[24] RASMUSSEN, J. Human error and the problem of causality in analysis of accidents. unpublished invited paper for Royal Society meeting on Human Factors in High Risk Situations (1989)

[25] RASMUSSEN, J., PEJTERSEN, A. M., and GOODSTEIN, L. P. Cognitive systems engineering, Wiley, New York, NY (1994).

[26] WEICK, K., SUTCLIFFE, K., Managing the Unexpected: Assuring High Performance in an Age of Complexity, Jossey-Bass, San Francisco, CA(2001).

[27] REASON, J. Cognitive aids in process environments: prostheses or tools? *International Journal of Man-Machine Studies , 27*, (1987) 463–70.

[28] WOODS, D. Commentary: cognitive engineering in complex and dynamic world. International Journal of Man-Machine Studies , 27 5-6 (1987) 571-585.

[29] MESHKATI, N. Integration of workstation, job, and team structure design in complex Human–machine systems: A framework. International Journal of Industrial Ergonomics , **7** 2 (1991). 111-122.

[30] SLOANE, S. B. The Use of Artificial Intelligence by the United States Navy: case study of a failure. *AI Magazine* ,**12** 1 (1991). 80-92.

[31] DEKKER, S., WOODS, D., "The High Reliability Organization Perspective", *Human Factors in Aviation*, Academic Press, Boca Rton, FL (2010).

[32] TROTTER, M., SALMON, M., LENNÉ, M., Improvisation:theory, measures and known influencing factors, Theoretical Issues in Ergonomics Science, **14** 5 (2013) 475-498.

[33] WEICK, K. Introductory Essay: Improvisation as a Mindset for Organizational Analysis. Organization Science , **9** 5 (1998) 543-555.

[34] AHMED, K.,Culture and climate for innovation, European Journal of Innovation Management, **1** 1 (1998) 30-43.

[35] DREYFUS, H., DREYFUS, S., Mind over machine.: The Free Press. New York, NY(1986).

[36] MORAY, N., JONES, B., RASMUSSEN, J., LEE, J., VICENTE, K., Performance Indicator of the Effectiveness of Human-Machine Interfaces for Nuclear Power Plants, Technical Report , University of Illinois at Urbana-Champaign, Deptartment of Mechanical and Industrial Engineering, Urbana, IL (1993).

[37] RASMUSSEN, J. Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. IEEE Transactions on Systems, Man, and Cybernetics , **13** 3 (1983) 257-266.

[38] RASMUSSEN, J., Information processing and human-machine interaction: An approach to cognitive engineering, North-Holland, New York, NY (1986).

[39] VICENTE, K. J., RASMUSSEN, J., "Ecological interface design: Theoretical foundations" IEEE Transactions on Systems, Man, and Cybernetics, SMC-22 (1992) 589–606.

[40] MESHKATI, N., BULLER, B., AZADEH, M., Integration of Workstation, Job, and Team Structure Design in the Control Rooms of Nuclear Power Plants: Experimental and Simulation Studies of Operators' Decision Styles and Crew Composition While Using Ecological and Traditional User Interfaces, Los Angeles, CA (1994).

[41] LAMMERS, C., Hickson, D., "A cross-national and corss-institutional typology of organizations", Organizations Alike and Unlike: International and Interinstitutional Studies in the Sociology of Organizations, Routledge & Kegan Paul, London , UK (1979).

[42] THOMPSON, T., "Accidents and destructive tests", The technology of nuclear reactor safety, MIT Press, Cambridge, MA (1964).

[43] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Safety Report for 1987, IAEA, Vienna (1987).

[44] INTERNATIONAL ATOMIC ENERGY AGENCY, The Chernobyl Accident: Updating of INSAG-1 (INSAG-7), IAEA, Vienna (1992).

[45] MONIPOV, V.M., Chernobyl operators: criminals or victims? Applied Ergonomics, **23** 5, (1992) 337-342.

[46] ACTON, J., HIBBS, M. Why Fukushima was preventable (2012), http://carnegieendowment.org/2012/03/06/why-fukushima-was-preventable, (Accessed June 23, 2015).

[47] MESHKATI, N., Fukushima's Unsung Heroes and Implications of the New Seminal Report by the U.S. National Academy of Sciences for the Future of (Japan's) Nuclear Power Industry., Huffington Post, (2014, September 12), http://www.huffingtonpost.com/najmedin-meshkati/fukushimas-unsung-heroes-_b_5801926.html?utm_hp_ref=tw

[48] MESHKATI, N., TABIBZADEH, M., FARSHID, A., RAHIMI, M., ALHANAEE, G., People-Technology-Ecosystem Integration: A Framework to Ensure Regional Interoperability for Safety, Sustainability and Resilience of Interdependent Energy, Water and Seafood Sources in the (Persian) Gulf, Human Factors, (2016) 44-57.

[49] SYNOLAKIS, C., KANOGLU U., The Fukushima Accident Was Preventable, Philosophical Transactions of the Royal Society A 373: 20140379 (2015), http://dx.doi.org/10.1098/rsta.2014.0379

[50] NUCLEAR ACCIDENT INDEPENDENT INVESTIGATION COMMISSION, The official report of Nuclear accident independent investigation commission, NAIIC, The National Diet of Japan (2012).

[51] NATIONAL ACADEMY OF SCIENCES, Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants, National Academies Press, Washington, DC (2014).

[52] HÖGBERG, L., Root causes and impacts of severe accidents at large nuclear power plants, AMBIO, **42** 3 (2013) 267–284.

[53] RYU, A., MESHKATI, N., Onagawa: The Japanese nuclear power plant that didn't meltdown on 3/11, Bulletin of the Atomic Scientists (March 10, 2014).

[54] RYU, A., MESHKATI, N., Culture of safety can make or break nuclear power plants, The Japan Times, (March 15, 2014).

[55] INTERNATIONAL ATOMIC ENERGY AGENCY, The Fukushima Daiichi Accident, Report by the Director General, IAEA, Vienna, Austria (September 2015)

[56] WEICK, K., Sensemaking in Organizations, Sage, Thousand Oaks, CA (1995).

[57] WEICK, K., SUTCLIFF, K., Managing the unexpected: resilient performance in an age of uncertainty, 2nd ed, Jossey-Bass, San Francisco, CA (2007).

[58] SANTAYANA, G., Reason in Common Sense, The Life of Reason, volume 1, Echo Library, Fairford, UK (1905).

EVALUATING SAFETY CULTURE UNDER THE SOCIO-TECHNICAL COMPLEX SYSTEMS PERSPECTIVE

F.L. LEMOS
IPEN – Nuclear and Energy Research Institute
CNEN – National Nuclear Energy Commission
Sao Paulo/SP, Brazil
Email: fllemos@ipen.br

Abstract

Since the term "safety culture" was coined, it has gained more and more attention as an effort to achieve higher levels of system safety. A good deal of effort has been done in order to better define, evaluate and implement safety culture programs in organizations throughout all industries, and especially in the Nuclear Industry. Unfortunately, despite all those efforts, we continue to witness accidents that are, in great part, attributed to flaws in the safety culture of the organization. By the way safety culture has been defined it is as if it is an identity on its own right, or even a component of the system. In this sense, blaming flaws in the safety culture for accidents, or incidents, would follow the same line of reasoning as blaming human errors, or an equipment failure, for an accident. Conversely, it would be expected that, if the safety culture is evaluated as positive, or strong, the system should be safer. The paper argues that, although all the components of a system may work the way they should, it does not guarantee that the system will be safe. Safety is a property of the system that emerges from the interactions between its components, and, therefore, safety will depend on the constraints imposed by the higher levels of the hierarchical structure of the system. A short practical example, based on the Davis-Besse Nuclear Power Plant head degradation event, is presented.

1. INTRODUCTION

Certain behaviours of people can easily be attributed to a weak safety culture, such as an employee not wearing his/her individual protection equipment, e.g. dosimeter, or when they ignore basic safety procedures for operating equipment. However, when it comes to more subtle interactions between components of the system, it becomes harder to detect potentially hazardous situations that are hidden, and can lead the system to hazardous states.

For example, leaders can take decisions that are potentially in conflict with decisions taken by other colleagues at a very different department, and without knowing, be contributing to future unintended consequences to the system. Such a situation may not be easily detected by direct observation.

These situations can occur in spite of the safety culture being regarded as positive.

Another point, that we discuss, is about considering the organization under a perspective of a broader system, from which it is a component. By considering the safety culture in an organization alone we fail to capture possible unintended consequences of the interactions between other components that will have impacts on the decision making process in the organization.

With the objective of having a deeper understanding of the relation between the safety culture and the safety of the system we propose a combination of the STPA, Systems Theoretic Process Analysis methodology [1], and the Three Lenses approach [2].

STPA is an extension of the STAMP, Systems Theoretic Accident Model [3]. Both methodologies are explained in some more detail later on in this paper.

In STPA it is assumed that accidents are the result of flaws in the control of the interactions between components and, therefore, even when all components of the system are working exactly the way they should, accidents can happen.

The Three Lenses is an approach for organizational analysis through three perspectives: strategic design, political, and cultural [2].

The three lenses perspectives can help on a better understanding of the mechanisms that could lead to the deterioration of the control structure of the system. More details are provided later on in this paper.

Some definitions important for a better understanding of this study are presented next.

2. STAMP – SYSTEMS THEORETIC ACCIDENT MODEL

STAMP, Systems Theoretic Accident Model and Processes is based on systems thinking and systems theory [1].

A system can be defined as a set of components and subsystems acting together towards a common goal or purpose. A system has boundaries, input and output. In STAMP a system is viewed as composed by hierarchical levels of control, where the upper levels have properties that emerge as a result of the interaction between components at the lower levels [4]. In this sense, the socio-technical system, as for example, a nuclear power plant, has a structure that is comprised of the following basic elements: human controllers, automated controllers and controlled process. The controlled process is the physical or sensed process that can potentially exhibit hazardous behaviour [1].

The operation of the system is modelled as a Safety Control Structure, which is a feedback control loop. The controllers update their process model (or mental model for humans) through feedback they receive from the controlled process, and input from other sources. With this updated knowledge, about the state of the system, the controllers issue the control actions to modify the controlled process according to its algorithm.

In STAMP, safety is considered an emergent property that arises from the interactions between the system components [1].

An Accident can be defined as an inadmissible loss; it can be loss of lives, equipment, but it can also be loss of credibility, money, and so on. An accident occurs when the system is in a hazardous state in combination with a worst environmental set of conditions [1].

The hazardous state occurs due to inadequate control of the safety constraints on the system behaviour.

STPA/ Systems Theoretic Process Analysis, is based on STAMP and is used for safety analysis, i.e. analysis of accidents before it happens [4].

To start the STPA analysis we need first to define the boundaries of the system, and then define the accidents. After defining the accidents, we can define what hazardous states of the system that together with worst environmental conditions, can lead to the accidents.

Note that the accidents are defined in accordance with the stakeholders' interests. Then, for example, for the US NRC, one accident could be defined as: "People and the Environment being harmed by radiation". For the Utility, and accident could be defined as: "Reputation loss".

For example, if the system is a Nuclear Power Plant, NPP, and its boundaries are defined as its physical limits, then an accident can be defined as: "Public exposed to a harmful level of radiation"

For this accident to happen two conditions are necessary:

(a) System hazardous condition: the release of radioactive material from the NPP

(b) Worst environmental condition: Public living close enough to be reached by the radioactive material.

Then we have:

Accident = Hazardous condition + Worst Environmental condition

It should be noticed that the term "environmental conditions" refer to conditions that are "external" to the system. These are conditions over which the designers of the NPP do not have control. In other words, the designers cannot make assumptions about the behaviour of the public outside of the physical limits of the Plant.

3. STPA – SYSTEMS THEORETIC PROCESS ANALYSIS

The STPA consists in identifying how the control actions, issued by the controllers, can lead to the hazardous states, and the causes for those potentially hazardous control actions to occur. In other words, it helps to identify what safety constraints can be violated for the system to get to a hazardous state [5].

3.1. The safety control structure

The safety control structure is a functional control model of how the system enforces the safety constraints. A safety control structure is organized hierarchically. The controllers at higher levels provide control actions that affect lower level controllers or processes. Feedback is provided by lower level components and is used by higher-level controllers to decide what control actions to provide next.

Figure 1 shows a generic control structure. Note that the controller can be a single component, e.g. an operator, or it can be a complex structure, e.g. a department or an institution, with an internal safety control structure [3].

Each controller—whether human or machine—contains a model of the process they are controlling, called process model. The process model represents the knowledge the controller has about the state of the system. This knowledge must in accordance with the system state in order for the controller to make safe decisions.

Inconsistencies between the real state of the system and the process model, or improperly imposed constraints, can lead the system to the hazardous states [3].

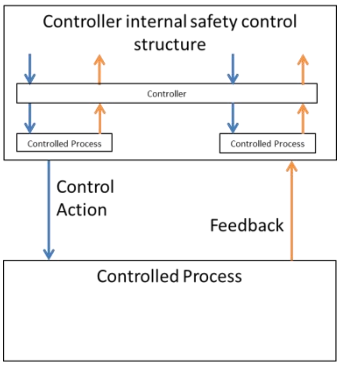


FIG. 1. A generic control structure, adapted from [3].

The process model variables capture the information needed by each controller to decide what control action to provide. Different process model variables may be associated with each control action.

The controlled process can be a physical process in an organization, for example, the safe operation of a NPP, or it can also be, for example, the safe generation of nuclear energy in the country.

After identifying the controllers and other components of the system we can identify their safety related responsibilities. For example, pilots may be responsible for properly executing all instructions from air traffic control, automated systems may be responsible for maintaining process parameters within certain limits, and plant operators may be responsible for monitoring automated systems and reporting any problems found [5].

STPA can be applied in two steps:

- Step 1: Identifying Potentially Hazardous Control Actions

The control action, CA, can be potentially hazardous if it is inconsistent with the state of the system. If the knowledge about the state of the system is not properly updated, then the CA may be potentially hazardous.

To know whether the CA is potentially hazardous, it is necessary to know the context at the time it was issued.

The potentially unsafe control actions can be classified into four categories according to the state of the system:

(1) A required action is not provided or is provided and not followed
(2) A required action is provided and leads to a hazard
(3) A required control action is provided too early or too late, or in the wrong order
(4) A required control action is stopped too soon or applied too long

A fifth scenario is identified, when the control action is issued but not followed [3, 5].

To assure that the control actions are in accordance with the state of the system, it is necessary to apply the safety constraints, i.e. certain behaviours are constrained in order to make sure the system is kept in a safe state.

- Step 2: Identifying causal factors

Once the safety constraints are defined, we can proceed to identifying the causal factors that can lead to violations of the constraints. Figure 2 shows the general control loop components. This representation helps to identify the causal factors for the control action to be potentially hazardous [5].

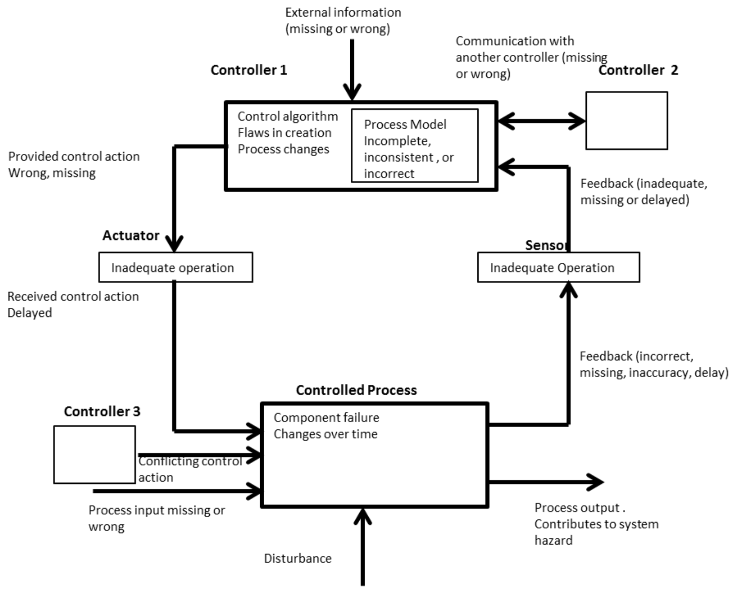


FIG. 2. A general control loop with causal factors, adapted from [5].

As can be seen from Figure 2 the decision making process to issue a control action can be a result of a very complex process. In a large and very complex socio-technical system all the flow of information, mental maps, algorithm, etc. are subject to constant influences from many components, such as multiple controllers and multiple stakeholders.

Models are abstractions of the actual system. Therefore, it is important to note that these elements are figurative and do not always represent physical equipment.

Also, it is important to note that a control action does not have to be a command by a superior. For example, a control action can be a direct action such as “open valve”, but it can also be in form of guides, laws, rules, etc.…

Feedback can be reports, surveys, or other means that provides information on the state of the system.

3.2. Safety

Safety has similar meanings for STPA and the IAEA. However, in STPA safety has a broader meaning. In STPA an accident is an unacceptable loss.

For the IAEA, [6], any harmful effects of ionizing radiation to people and the environment would be considered as an unacceptable loss, or an accident.

For the utility owner perspective, an economic loss can also be considered as an unacceptable loss, or an accident.

In STPA, both, “economical loss” and “harm to people and environment”, are considered within the same safety assessment, which makes it relatively easier to deal with conflicting goals in the same framework. It should be pointed out, however, that a company which has frequent problems out of safety concerns would almost certainly have problems with its productivity, and reputation, eventually leading to economical loss. All aspects of a system are indeed interconnected.

Safety Culture

The International Nuclear Safety Group (INSAG) defines safety culture as:

“The assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receives the attention warranted by their significance.”

One important observation about this definition of safety culture is: what do the expressions “emphasize safety over competing goals” or “make nuclear safety the overriding priority” mean?

The definition do not make it clear how to make it a priority, i.e. how to deal with different goals, during design and operations of the system. Safety and production do not necessary need to be competing goals as it will be seen later on.

In the example some of these issues can be observed in more details.

4. THE THREE LENSES

In the previous sections we saw that a system, an organization, can be modelled in terms of a control structure. The borders of the system can be extended in order to incorporate other components of a much broader system, of which the organization is one of the components.

We begin this section with an excerpt from the book Design for a Brain [7].

“The system state, at any point in time, is the set of relevant properties describing the system at that time. These properties are represented by state variables. As the system can have an infinite number of state variables that can describe its state, only a subset of those variables are chosen to describe the relevant behaviour of the system according to stakeholder and the purpose being analysed. In other words, the analyst chooses his system.”[7]

The “Three Lenses” is an approach for organizational analysis. It is about using different perspectives to view an organization. Depending on the perspective different variables and relationships in the system are considered [2].

The three lenses are: Strategic Design Lens, Political Lens and Cultural Lens. It is important to keep in mind that all the variables, and relationships, highlighted by each one of the lenses co-exist in the system, and that the lenses approach helps us to make sense of these variables and their relationships, which reveals a much more complex socio-technical system.

Following, a short description for each of the lenses is presented. The reader is encouraged to seek more information elsewhere [2].

The Strategic Design Lens: The model assumes that goals are achieved with plan and information flow. Management is based on logical principles of efficiency and effectiveness.

The basic idea of strategic design is "get people with the right knowledge and give them appropriate tasks to do and sufficient information to accomplish the organizational goals" [2].

Political Lens: The organization is viewed as a contest for power among stakeholders with different goals and underlying interests. Goals and strategy are either imposed by a ruling coalition or negotiated among interest groups. As circumstances change, power shifts and flows, coalitions evolve, and agreements are renegotiated [2].

Cultural Lens: The cultural perspective assumes that people take action as a function of the meanings they assign to situations. The cultural lens focuses on norms, meaning, artefacts, and values. Managers become the creators of meaning, using symbols and stories.

5. EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION

STPA is a safety analysis methodology, and not an accident analysis methodology. This example is meant to be an illustration of how STPA could be applied to the safety analysis of a system by using data from a real case. The Davis-Besse head degradation event was chosen, as a real case example, because there is relatively good information about it and because the Davis-Besse NPP had good performance indicators, from the NRC and the INPO, before the event [8].

Although data from the incident is used, it is not our intention to make an analysis of the event per se.

We built this example based on some limited data from literature; mainly a text by Dr. Corcoran [8], therefore, this should be considered only as a preliminary study to launch basic ideas for further research.

Simplifications were necessary in order to complete the study for this paper.

5.1. Identification of the system

The STPA analysis is a top-down approach. It starts from a higher level of the system to the lower levels. The controllers at a higher level issue the control actions to assure that the lower level components will interact accordingly for the desired behaviour to emerge at the higher levels.

As the analysis of the event involves a national interest (e.g. the whole nuclear industry), the USNRC and other institutions should be part of the system, then we defined the system at a higher level than the Devis-Besse Plant itself.

We can name this system as, for example, the National Nuclear Energy Generation System, from which the Davis-Besse is one of the components. As a regulator, the USNRC has a higher hierarchical position in relation to the nuclear industry, which has a higher position in relation to the Davis-Besse NPP.

The controlled process could be defined as: "The safe production of nuclear energy".

The safety control structure for this system is shown in Figure 3. Note that this is an incomplete representation of the system, as there are many more players to be considered. In a more detailed study the system would certainly be much more complex.

Also, we will limit our analysis to one control action only.

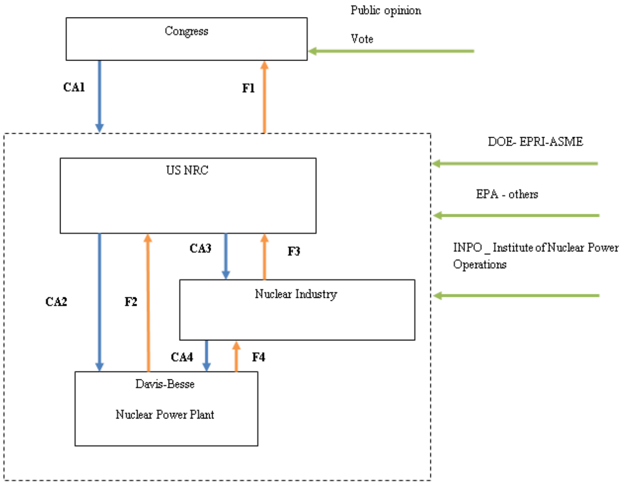


FIG.3. National nuclear energy generation partial safety control structure.

After defining the system, it is time to identify the accidents to be considered. This identification can be a result of an agreement between members of a team of experts. For this system we consider the following accidents:

A1: People or the environment are exposed to radiation
A2: Loss of reputation for the USNRC
A3: Loss of reputation for the Nuclear Industry

Next, we identify the hazardous states that could lead to the already identified accidents:

H1: Radioactive material released from a NPP: A1; A2; A3
H2: Generation of Electrical Power Stopped: A2; A3

H3: Serious Equipment Damage: A1; A2; A3

It is interesting to note that the hazardous states can lead to more than one accident. Also, one accident can be linked to others. For example, accident A1 can lead to A2 and A3, i.e. if the company is shut down because of an incident it will have economic loss and probably will have damage to its reputation as well.

From the above observation it can be inferred that the safety culture traits are indeed important to all aspects of the operation of the NPP and not only to the accident A1. In other words, a strong safety culture does not only help to assure the safety, i.e. prevention of accident A1, but it would also help on the prevention of the other accidents, A2 and A3.

As mentioned earlier, the control actions can have different forms according to the level and other characteristics of the controller. For example, the control action CA1 could be in the form of laws, while the feedback F1 could be in the form of reports. The highest the level of the controller the more general are the control actions and with longer time scales [9].

We start the exercise by defining the control action, CA3, issued by the US NRC, requiring the shutdown of reactors in 2001. This CA was issued after receiving a feedback from the industry, F3. This feedback was the result of inspections in similar plants as mentioned bellow:

F3: "*Inspection of Oconee Nuclear Station 1 (Nov. 2000), Arkansas Unit 1 (Feb. 2001), Oconee Unit 3 (Feb. 2001) and Oconee Unit 3 (April 2001) showed both axial and circumferential cracks in Control Rod Drive Mechanisms*" [10].

CA3: "*October 15, 2001: The NRC staff distributed a draft order requiring the shutdown of reactors by December 31, 2001, for CRDM nozzle inspections"* [10].

The next step is to identify how this control action can be hazardous. To this end it is necessary to analyse the context, and modes, in which the control action is issued.

When analysing the context of a control action we look for the worst set of environmental conditions. It is important, at this point, to let all possibilities of scenarios to be considered. The analyst could be helped by a team of experts involved in the operation and design of the system.

Also, during this analysis one should not be limited by possible barriers, or redundancies, to prevent any condition from happening. The barriers are part of the system, and as such, they should be included in the safety control structure.

Table 1 shows some of the possibilities for the control action to lead to hazardous states.

TABLE 1. CONTROL ACTION 3 – CA3: INSPECTION REQUIRED

Control Action	Potentially Hazardous				
	1- Not Providing causes hazard	2- Provided causes hazard	3- Provided Too early or too late causes hazard	4- Applied too long or stopped too soon long causes hazard	5- Provided but not followed
Inspection Required	- There is a corrosion process that continues until the vessel is perforated by corrosion - LOCA **H1-H2-H3**	- There was no need for the inspection **H2**	*1- Too early* - Provided when there is no corrosion visible. Makes the Plant to shut down unnecessarily. **H2** - Causes unnecessary delays in the generation of energy. **H2** *2- Too late* - Provided after the corrosion is in a very advanced stage or had already perforated the RV **H1-H2-H3**	*1- Stopped too soon* - Inspection initiated but stopped before any sign of corrosion is found **H1-H3** *2- Applied too long* - Inspection lasts for a long time causing unnecessary delays in the generation of energy. **H2**	- The corrosion continues until the vessel is perforated by corrosion **H1-H2-H3**

In the example, there are basically two contexts, or conditions, for the control action to be hazardous:

(a) The Plant is continuing operation when there is a corrosion process in the RPV, leading to damage to the equipment and consequent release of radioactive material.

(b) The Plant is unnecessarily shutdown when there is no corrosion at all.

After identifying the potentially unsafe control actions, we proceed to STPA step 2 for the analysis of what could have contributed for these control actions to be issued, or not, in those conditions.

There should be no limitations by judgements of whether the causes are highly improbable. As long as the cause is not impossible, it should be considered [1].

(a) Provided causes hazard:

The regulator decides for the inspection requirement in spite of the low probabilities of the occurrence of the process.

DB Plant decides to conduct the inspection without pursuing further information about the differences in the Plants.

(b) Not providing causes hazard:

Regulator thinks that there is no need for inspections; therefore, the regulator does not issue an inspection requirement. This could be a result of a flawed feedback from the industry, F3 and F2, which convinces the NRC that there is no safety concern and there is no need for inspections.

The Plant asks to cancel the inspection.

(c) Provided too early or provided too late causes hazard:

Provided too early:

Regulator decides for an early inspection for precaution.

Plant decides for an early inspection for precaution.

Provided too late:

Regulator takes a long time to identify indicators of the urgency of the problem.

The Plant asks for a delay in the inspection.

(d) Applied too long or stopped too soon causes hazard:

Applied too long:

The NPP workers unsecure whether they should stop or continue with inspection, carrying out extra tests to assure that there is no corrosion, causing unnecessary delays in energy generation.

Regulator asks for more explanations and requires extra inspections.

Stopped too soon:

The NPP think it is unnecessary to continue inspection as they feel pressed by the industry to be productive.

The NPP stop inspection because they would have to go through very difficult procedures to continue and they think it is not worth it.

(e) Provided but not followed

Industry receives requirement but does not follow it because they think it is not necessary or they do not want to stop generation of energy. Industry asks for a delay.

The DB does not understand the requirement and, therefore, does not follow it.

5.2. Causal analysis for the hazardous control actions

Some possible causes for the control actions to be potentially hazardous were presented. It is not an exhaustive list, but it is enough for our discussion. The objective of the causal analysis is to identify the constraints, or requirements, for the hazardous control actions not to happen, or if they happen, find ways to cope with the consequences.

Here is where the Three Lenses approach comes into play. The Three lenses approach helps us to understand the underlying processes for the causes to happen.

To facilitate the discussion, Table 2 presents the five potentially hazardous control actions and their respective causes approximately classified into the three categories according to the Three Lenses.

TABLE 2. APPROXIMATE CLASSIFICATION OF CAUSAL FACTORS ACCORDING TO THE THREE LENSES

Lens Control Action	Cultural	Strategic Design	Political
Provided		DB decides to proceed with inspection	Regulator takes isolated decision
Not provided	They thought the plant was safe – Leaks were not a safety concern	Technical Specifications were followed	DB prevailed over NRC arguments
Provided Too early		DB decides to proceed with inspection	
Too late	DB thought plant was safe – Leaks were not a safety concern The process was long and people got used to it making it difficult to notice changes	DB was well evaluated by NRC and INPO	
Provided For Too long			
Stop too soon	DB thinks it is not necessary further inspections	DB thinks inspections is waste of time	
Provided but not followed	DB was well evaluated They thought plant was safe – Leaks were not a safety concern		DB wants to obtain economic benefits and the industry prestige associated with very short maintenance outages.

5.2.1. Rationale for the classification

The classification of the causes was based on some information found in the literature [8, 1, 11, 12], and it would need further research in order to be improved. We looked for predominant characteristics in the decisions that would match them with the characteristics of each of the three lenses.

In the real world things are not neatly arranged and, therefore, we should not expect a right answer [2].

The decisions of issuing, or not, a control action, as well as the decision to follow, or not, the CA's, can be a result of complex interactions and relationships throughout the system. These relationships and interactions do not necessarily have to be related to culture. Following, some examples of rationale for the classification of the causal relationships into political, cultural, and strategic design are presented. We present them in form of excerpts from literature followed by the respective reference number.

The Cultural Lens

(1) Decisions based on perceptions and beliefs:

In all but a few cases, cracking in nozzle applications has been attributed to primary water stress corrosion cracking (PWSCC). The mechanism of PWSCC is not completely understood, and prediction of crack initiation time has proven to be difficult, if not impossible [11].

"This resulted in less vigorous inspections and dismissal of some indicators because they believed the plant was safe" [12].

This produced "a whole new phenomenon," says John Grobe, head of an NRC task force investigating the incident. "This kind of corrosion has never been seen before on a reactor pressure vessel head." [13].

(2) People became used to a situation. There was a disconnection from the situation of a safety concern*:*

Another confounding factor was pressurizer relief valve leakage that was bad enough to cause a rupture of a rupture disk (a mechanical "fuse", intentional protective weak link") in a drain tank. This was more leakage that distracted attention from the nozzle leakage. It apparently strengthened the plant staff penchant for living with reactor coolant system leakage and treating it as normal. [8].

(3) Same as item 2. People became so used to the situation that there was a disconnection with safety concerns*:*

Ironically, the plant's "Technical Specifications" (official rules of operation) were never violated by the leakage, per se. Before this event it was believed that adhering to the Technical Specifications guaranteed that the assumptions of the Safety Analysis were being met and that the plant was therefore safe. Eventually the symptoms of the nozzle leak that caused the reactor vessel head degradation were erroneously dismissed as symptoms of flange leaks, which were apparently acceptable. Once this was done the progress of the degradation was virtually assured [8].

Strategic Design

(1) This situation could be classified as a cultural as well. However, the access had not been fixed because they had plans for future modernization, for example, as part of a strategy to achieve more efficiency*:*

The inspections were made more difficult by the design of the reactor service structure, which provided only "mouse holes" for inspection [8].

(2) Decision can be part of a strategy to achieve goals:

Another factor that motivated against inspection was that the neighbourhood of the reactor vessel head is an intense radioactive field and hence radiation exposure of individual workers would be involved. Low radiation exposure is one of the measures of success among nuclear power plants [8].

(3) This situation could reinforce the strategies to seek a goal:

Davis-Besse had been rated 'INPO 1', which meant that an independent review process undertaken by industry peers had judged it to be a high-performing organisation [14].

It is apparently possible for the indicators to be misleading, as occurred in this case, since the NRC rated Davis-Besse as 'all green" and INPO found "no significant weaknesses" [8].

Political Lens

(1) The Plant can be considered as a stakeholder in a broader system. This situation could be associated with strategic Lens as well:

Notice that this whole scenario unfolded during the world-wide phenomenon of electric power industry restructuring. Did the competitive pressures of restructuring exacerbate conditions at Davis-Besse? Only by digging into the details of the behaviours and conditions will we ever find out [8].

(2) This situation was also cited as having strategic design characteristics. It is repeated here because this situation can also mean political power in the broader system where the Plant is one stakeholder:

Davis-Besse had been rated 'INPO 1', which meant that an independent review process undertaken by industry peers had judged it to be a high-performing organisation [14].

It is apparently possible for the indicators to be misleading, as occurred in this case, since the NRC rated Davis-Besse as 'all green" and INPO found "no significant weaknesses" [8].

(3) This situation could be classified as a strategic design as well. They could have plans for future modernization, for example, and a modification would be considered as unnecessary at that time:

In 1990 a modification to improve inspectability was proposed by station employees. It was deferred by management [8].

(4) This citation mentions strategic design and political power motivations:

The inspections were motivated against because they are expensive to conduct and because they could delay power production. Avoiding the comprehensive inspections gave economic benefits as well as the industry prestige associated with very short maintenance outages [8].

6. DISCUSSION AND CONCLUSIONS

The proposal of this paper was to analyse the role of the safety culture in the safety analysis of a complex socio-technical system. Most of the literature treats safety culture under the perspective of an organization alone, giving little consideration to the broader system in which this organization is inserted.

By blaming flaws in the safety culture for accidents, or incidents, we fail to grasp important underlying mechanisms that shape the decision making process throughout the system.

The systemic approach, STAMP/STPA, showed that the Nuclear Power Plants are part of a broader system and, therefore, they affect, and are affected by, other components of that system.

The Three Lenses approach offers yet an additional, or complementary, perspective, by introducing the cultural, political, and strategic design lenses, to interpret the mechanisms that underlie the decision making process throughout the system.

While we still need a strong safety culture, we need to shift the focus, from the safety culture itself, to a broader perspective.

For a short example on how the STPA and The Three Lenses could be applied, we chose an example of a real case incident in an organization that had previously been well evaluated by the US NRC and IMPO.

It is not the intention of this paper to claim that STPA would have done a better job at the time of the event. However, it would certainly have facilitated to put the problem into new perspectives and, hopefully, bringing new dimensions for the solutions. For example, it was shown that safety culture can be viewed as pertaining not only to an organization, but as a feature that permeates a broader system, from which the organization is one of the components.

We think that STPA and the Three Lenses approach could help answer, or at least help to answer, to the following questions:

(a) How strong should the safety culture have to be to prevent the incident from happening?
(b) If the degraded head had been discovered during earlier inspections, would it mean that Davis-Besse deserved a better safety culture classification?
(c) How would have the event unfolded in case the workers had a better access to that spot in the RPV? (The "muse hole" access [8])
(d) This is a good example of interactions between components of the system, i.e., the designers and the operation workers.
(e) How much more training, on safety culture, the workers would need to help avoid the next big accident?

We conclude that, while a strong safety culture is necessary to keep the systems safety, it is not enough. The combination of STPA and The Three Lenses approaches could help us to go deeper in the understanding of the system variables and components interactions. Hopefully, it could help find the gaps in the safety control structure for a lasting solution.

ACKNOWLEDGEMENTS

The author would like to thank to IAEA for the financial support that made possible our participation in this Conference.

Also, would like to thank Professor John S. Carroll, MIT Sloan School of Management, for his kindness in providing comments and suggestions for this research.

REFERENCES

[1] LEVESON, N., Engineering a safer world: Systems thinking applied to safety. MIT Press, 2011.

[2] CARROLL, J. S., "Introduction to organizational analysis: the three lenses", unpublished class paper, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA (2006).

[3] LEVESON, N., "An STPA Primer." Cambridge, MA (2013).

[4] LEVESON, N., The drawbacks in using the term ‘system of systems’, Biomedical Instrumentation and Technology, March/April (2013) 115-118.

[5] Thomas, John, F. Lemos, and Nancy Leveson. "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants." Research Report: NRC-HQ-11-6-04-0060 (2012).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[7] Ashby, W. R., An introduction to cybernetics, Chapman & Hall, London (1956)

[8] CORCORAN, W.R., The Near Miss at Davis-Besse, Part I (2002), http://www.rootcauselive.com/Files/Past%20Investigations/Davis-Besse/Davis-Besse%20Narrative%202002_06_30_0700.pdf.

[9] FLEMING C. H., “Safety-driven Early Concept Analysis”, PhD Thesis, Massachusetts Institute of Technology, Cambridge (2015).

[10] KADAK,A.C., Operational Reactor Safety (2008), http://ocw.mit.edu/courses/nuclear-engineering/22-091 -nuclear-reactor-safety-spring-2008/lecture-notes/MIT22_091S08_lec21.pdf

[11] LOEHLEIN, S.A., Root Cause Analysis Report, CR 2002-0891, FirstEnergy: Davis-Besse Nuclear Power Station, Oak Harbor, 2002.

[12] DANIEL SARGIS, PAUL ARNETT, RAYMOND SPORNHAUER, Davis-Besse Reactor Vessel Head Degradation (TESC NUC-495), (2014), https://www.youtube.com/watch?v=5JO1baLUnb0

[13] HEBERT, H. J., “Holes, Crack in Reactor Raise Big Nuclear Safety Questions”, The Brian Times (2002),

[14] https://news.google.com/newspapers?nid=799&dat=20020507&id=PtIJAAAAIBAJ&sjid=o0kDAAAAIBAJ&pg=4192,4421759&hl=en

[15] Berman P., Ackroyd P., “Organisational drift – A challenge for enduring safety performance”, IChemE Symposium Series No. 151, 2006, https://www.icheme.org/communities/subject_groups/safety%20and%20loss%20prevention/resources/hazards%20archive/~/media/Documents/Subject%20Groups/Safety_Loss_Prevention/Hazards%20Archive/XIX/XIX-Paper-07.pdf.

ENHANCING SAFETY CULTURE IN COMPLEX NUCLEAR INDUSTRY PROJECTS

N. GOTCHEVA
VTT Technical Research Centre of Finland Ltd.
Tampere, Finland
Email: nadezhda.gotcheva@vtt.fi

Abstract

The paper provides an integrative overview of an ongoing research project MAPS "Management principles and safety culture in complex projects". It aims at constructing a more comprehensive perspective on enhancing safety culture in complex projects in the Finnish nuclear industry context. Business-related challenges, such as delays and quality issues in projects have generally been perceived as economic problems. However, safety cannot be separated from other performance aspects when a systemic view is applied. Schedule and quality challenges may reflect deficiencies in coordination, knowledge and competence, distribution of roles and responsibilities, or attitudes issues of project participants. The four-year MAPS research project focuses on identifying the generic safety principles of managing complex projects, clarifying the cultural phenomena and how they affect safety, and facilitating management and safety culture development by providing new theoretical and practical knowledge. The paper highlights the importance of bridging interdisciplinary insights to advance theoretical and practical understanding on enhancing safety culture and nuclear safety in complex nuclear industry projects.

1. INTRODUCTION

Increased outsourcing and complexity in technology, work tasks and organizational structures bring new challenges for safety-critical industries [16]. During the past decade there has been significant increase in large projects globally, for instance energy, disaster clean-up, aerospace, transport infrastructure, sports and culture, cities and urban renewal. A *large project* is seen as "a dynamic network of organizations that combines the resources, capabilities and knowledge of the participating actors to fulfil the needs of the owner" [27]. These projects are huge financial undertakings, which have potentially substantial impacts on communities and environment. They bring together a number of stakeholders, such as investors, contractors, subcontractors, local interest groups, government organizations, communities, political decision-makers, and environmental bodies. These groups have differing values, knowledge, cultures, traditions or goals [7].

New build projects and modernization projects in the nuclear industry are often carried out by networks of companies as well. In the Finnish nuclear industry currently there are several complex projects that are taking place: two nuclear new builds - TVO's Olkiluoto 3 and Fennovoima's Hanhikivi 1 - as well as Posiva's final disposal facility for spent nuclear fuel in Olkiluoto. Moreover, modernization and modification projects are currently ongoing in the operational power plant units. In such a dynamic network of different organizations, some subcontractor companies may have little experience in the nuclear industry or insufficient consideration of specific regulatory requirements in the host country.

Prior evidence indicated that major projects have often experienced schedule, quality and financial challenges, both in the nuclear industry [32] and in the non-nuclear domain [1,3]. Suboptimal project management and an insufficient nuclear safety culture in the network have been recognized as challenges in this respect [13]. Still, project management issues remain understudied in safety research because business-related challenges, such as project delays and quality issues have been perceived mainly as economic problems. However, safety cannot be separated from other performance aspects when a systemic view is applied. Schedule and quality challenges may reflect various deficiencies, for example in coordination, knowledge and competence, distribution of roles and responsibilities or attitudes of the project participants.

The paper integrates the preliminary insights of an on-going interdisciplinary research project MAPS 'Management principles and safety culture in complex projects', which aims at bridging management principles and safety culture in complex nuclear industry projects. The assumption is that by synthesising different perspectives integration improves understanding and clarifies potential applicability of research knowledge. It is increasingly understood that the performance of the project network in all lifecycle phases contributes to the defence in depth. Recently, the Radiation and Nuclear Safety Authority in Finland (STUK) has issued new YVL guides, which specify requirements on project management and safety culture of suppliers and subcontractors [33]. International nuclear institutions have also paid attention to safety culture in networks of organizations [12,13,26]. In a recent study, Gotcheva and Oedewald [18] summarized safety culture challenges in different lifecycle phases of large nuclear industry projects, and many of them were found to be related to inter-organizational set-ups. *Project governance* deals with this inter-organizational space as it aims at aligning multiple diverse project stakeholders' interests to work together towards shared goals [34].

The remaining part of the paper presents the research project's objectives, summarizes its theoretical foundation, highlights the preliminary insights from the current research phase, and ends with discussion and conclusions.

2. MAPS PROJECT OBJECTIVES

The main research question of the MAPS project is: what are the safety management principles that should be applied in managing complex projects in the nuclear industry, and how these principles can be implemented in practice? The main objective of the MAPS project is to *enhance nuclear safety by supporting high* *quality execution of complex nuclear industry project*s, including modernisations and new builds. The four year project is aimed at the following three objectives:

(1) Identifying the generic safety principles of managing complex projects in the nuclear industry.
(2) Clarifying the cultural phenomena in major projects and the influence of time, scale, governance models, and the diversity of the involved actors on safety culture, and thus on safety.
(3) Facilitating management and safety culture of ongoing and planned major projects by providing practical tools and guidance on e.g. facilitating communication, organising decision making in unexpected situations, encouraging openness, and distributing knowledge and lessons learned.

MAPS is an interdisciplinary project, which brings together expertise in nuclear safety culture, governance of complex projects, construction industry network management, societal research on safety regimes and system dynamics modelling. The project is led by the VTT Technical Research Centre of Finland Ltd and project partners are University of Oulu and Aalto University in Finland. The expected results are a set of guidance and practical tools for defining and assessing project management practices and safety culture enhancement for nuclear industry projects.

3. THEORETICAL PERSPECTIVES

As the scale and diversity of activities in a project network increase, new phenomena emerge that require different logics of control than a traditional hierarchy. Project networks are seen as *complex adaptive systems*, which exhibit features such as self-organization, non-linear interactions and polycentric control [4,25]. Although such systems cannot be fully controlled or predicted, there is a practical need to manage these systems and to at least anticipate the system-wide patterns [25]. These features challenge some of the basic assumptions of traditional safety management approaches and project management models, such as expectations for following a pre-determined course of activities, clear communication and control structures.

Concepts and models for improving system safety are often based on the assumption that activities are carried out by an organization. For example, in safety management system literature, a management system is usually seen as a company specific system. Culture has also been predominantly studied in safety research as an intra-organizational phenomenon [29]. Therefore, when it comes to applying safety culture models across organizational boundaries, the task is challenging. One of the reasons is that project networks consist of multiple heterogeneous actors with somewhat conflicting objectives. Project partners bring own national and organizational cultural features and practices, which create a complex mix of influences on the overall project culture. Another challenge stems from the fact that traditionally, cultural approaches emphasize that creating a culture takes time and continuity, which does not reflect well the short time frames, high diversity and temporal dynamics typical for projects.

A systemic view on safety implies that human, technological, organizational and cultural factors are understood as mutually interacting elements [24], which produce system-wide emergent patterns. *Safety* is seen as an emerging property of the sociotechnical system, continuously created in daily activities [11,23]. The concept of *safety culture* has originated from the concept of organizational culture, which aimed at shedding light at success of organizations [19,29,30]. Overall, safety culture studies seem to propose a harmonious view of the organization [2]. However, it remains unclear what should safety management system or safety culture improvement program look like in an 'organization', which is actually a dynamic network of actors from different companies? This is a practical challenge in the nuclear new build and modernization projects, as well as a theoretical challenge for researchers.

During the past two decades safety science has increasingly utilized complex systems approaches to explain accidents. Activities in safety critical organizations have been characterized as involving uncertainties, multiple conflicting goals, non-linear action-outcome effects and dynamic self-adaptation, which makes them challenging to control [20,21,22,23,35]. *Complexity* approaches imply that safety cannot be created by decomposing the system into components, and improving them one by one. Instead, understanding the dynamics of the system behaviour and develop system capabilities for coping with varying conditions need to be in the spotlight [5,11,15,17]. Recent research on the governance of megaprojects has brought up conflicting results on the effects of different types of contractual arrangements on aligning interests of various stakeholders, manage uncertainty and ensure good performance [1]. Organizational arrangements that optimize complex project's capability to respond to unforeseen and unexpected events have been discussed [6]. An emerging research stream is also starting to address complex projects as hybrid meta-organizations consisting of multiple stakeholders and examine the implications of different types of organizational arrangements and their effects on performance [10].

System dynamics modelling is another discipline relevant for studying complex adaptive systems. It could be beneficial for understanding and supporting the overall performance of a complex project network. In the system dynamics methodology the focus is on uncovering the feedback mechanisms, time delays, and accumulations that cause certain dynamic behaviour over time in a system. The importance of simulation is emphasized in the system dynamics methodology as a way to gain a better insight of a system than by verbal reasoning alone [31]. Although many theoretical mechanisms related to project dynamics have been identified, various effects of managerial policies, system dynamics application to inform real life project management are still understudied. Also, while previous work in system dynamics has examined the interrelationships between work quality, project delays and cost overruns, the effects of these factors on safety have not yet been explored systematically.

4. INSIGHTS FROM THE CURRENT PHASE OF THE PROJECT

In this first stage of the MAPS project, the focus was on five main tasks:

- Understanding typical governance models and their effects on safety;
- Carrying out baseline interviews in the power companies to gain an insight on the main characteristics of complexity in nuclear industry projects in Finland and to highlight the features that are challenging from management of safety point of view
- Understanding nuclear specific regulatory requirements in complex projects
- Modelling the cultural dynamics and safety culture challenges in networks
- Reviewing the application of system dynamics modelling to complex safety critical projects

4.1 Understanding typical governance models and their effects on safety

The task focused on developing a framework of key governance dimensions and discussing their effects on safety. To this end, a systematic literature review of project governance in a network context was conducted. Two leading journals on project management were selected to capture and integrate research on project governance, International Journal of Project Management (IJPM) and Project Management Journal (PMJ) (IJMPiB). Altogether 16 papers were considered to be relevant for the analysis. Project governance in networks was categorized in a framework that consists of six key interdependent dimensions: goal setting, incentives, monitoring, coordination, roles and decision-making power, and capability building. The framework further links these dimensions to motivation and capability of project actors to work towards achieving shared safety objectives of the project [14].

4.2 Characteristics of complexity in nuclear industry projects

The task focused on carrying out literature summary on project complexity and nine baseline interviews at the Finnish power companies Fortum, TVO and Fennovoima on the characteristics of complexity in selected projects. The results highlighted the need to pay more attention to non-technical aspects of complexity, e.g. organizational, emergent or institutional, for example when considerations are made for resources allocation. Organizational complexity is more challenging from management of safety point of view than technical complexity. Dealing with technical complexity was seen as a part of professionalism in the nuclear industry. The results also indicated that different dimensions of complexity are closely interrelated in nuclear industry projects, and this should be taken into account [9].

4.3 Understanding nuclear specific regulatory requirements in complex projects

The task focuses on gaining understanding about the sources of complexity and the means to govern safety and complexity in projects with emphasis on the regulatory perspective. The results, based on empirical analysis of 12 interviews and documents analysis, indicated that there are several sources of complexity and various means to deal with it. The Finnish nuclear industry requirements were seen both as a source and solution to complexity. The scale of the project and long supply chains, cultural and organisational complexity, and inter-connectedness between different elements were considered as contributing to complexity. A second part of this task focused on comparing governance of safety at the Norwegian Petroleum Safety Authority (PSA) and STUK. The findings indicate that the concept of safety is broader in Norway compared to Finland as it includes also economic aspects. Also, the Norwegian regime is more focused on capacity building among stakeholders, and self-governance is supported by the regulator [36].

4.4 Modelling the cultural dynamics and safety culture challenges in networks

The task provided theoretical framing and description of the cultural complexity in terms of how the different cultures interact and to what extent it is possible to create a shared safety culture in such a context. The literature review discussed the concept of cultural complexity and existing frameworks. It also provided a summary of recent quality and safety-related challenges experienced in complex projects in the safety critical domain and other related industries. The results indicated that subcultural variety and dynamics require balancing between dealing with fragmentation and utilizing richness of perspectives, flexibility and identification of emergent risks as potential advantages for enhancing safety in multicultural projects [8].

4.5 Applying system dynamics modelling to complex safety critical projects

The task focused on conducting a literature review of the use of system dynamics modelling of complex safety critical projects. The aim was to gain insight on the existing uses of system dynamics to project management issues in general, and the applications of system dynamics for analysing and improving safety culture. The literature review indicated that key issues in the existing project management models, such as the number of undiscovered errors, have implications for safety, yet the current models are mainly discussed from financial perspective, focusing on cost overruns and schedule slippages [28].

5. DISCUSSION AND CONCLUSIONS

By bridging project governance and safety science research, the paper provides an initial attempt to understand the connections between the different elements of project governance and safety culture in complex nuclear industry projects. The presented preliminary insights from the first year of the MAPS projects are complementary. Shedding light on the main characteristics of complexity and highlighting features that are challenging from management of safety point of view set the wider context, in which the nuclear industry projects in Finland are planned and executed. The interrelation of technical, organizational, institutional/regulatory and emergent dimensions of complexity projects needs to be recognized and acted upon. Substantial part of the context is related to comprehension and interpretation of the nuclear specific regulatory requirements in complex projects. More specifically, grasping the sources of complexity and the means to govern safety and complexity in projects from a regulatory perspective contributes to the big picture.

Further, understanding typical network governance models and their effects on safety provides further insight on approaches for improving the coordination and building of a shared understanding between different stakeholders. Appreciating the cultural diversity and dynamics in project networks requires capabilities to balance between dealing with issues of fragmentation and utilizing the richness of available perspectives in the network for enhancing safety. In that sense, system dynamics modelling represents a practice-oriented integration approach, which could be relevant in at least two ways: co-development of shared understanding about safety by interactive workshops (models can be used as boundary objects) and theory building or generation of insights (models can be used to develop practical recommendations for companies to notice and take action on vicious cycles that could erode safety culture).

The study brings new insights about the links between complexity and safety culture in project networks. Further theoretical and empirical work is ahead to develop a more nuanced appreciation of these links by in-depth case studies, and to translate the findings into valuable practical tools for different stakeholders in the industry. Benchmarking between the oil & gas industry and the nuclear industry in terms of key challenges, practices and innovations in the governance of complex projects is also in the pipeline. Next steps in the MAPS project include coming up with a set of best practices for identifying and specifying methods to improve, facilitate and assure safety culture in complex project networks, as well as developing a system dynamics simulation model of governance and cultural phenomena interactions in complex nuclear industry projects.

ACKNOWLEDGEMENTS

The study received funding and support by SAFIR2018, the Finnish Research Programme on Nuclear Power Plant Safety 2015-2018. The author is grateful to the power companies in Finland, TVO, Fortum and Fennovoima, and the Radiation and Nuclear Safety Authority (STUK) for their cooperation. The author would like to thank the MAPS project team for excellent collaboration.

REFERENCES

[1] AHOLA, T., RUUSKA, I., ARTTO, K., KUJALA, J., What is project governance and what are its origins? International Journal of Project Management, **32** (2014) 1321-1332.

[2] ANTONSEN, S., Safety culture and the issue of power, Safety Sci, **47** (2009) 183–191.

[3] BRADY, T., DAVIES, A., Managing structural and dynamic complexity: A tale of two projects. Project Management Journal, **45** (2014) 21-38.

[4] CHOI, T. Y., DOOLEY, K. J., RUNGTUSANATHAM, M., Supply networks and complex adaptive systems: control versus emergence. Journal of Operations Management, **19** (2001) 351-366.

[5] DEKKER, S., The Field Guide to Understanding Human Error. Adelshot, UK: Ashgate (2006).

[6] FLORICEL, S., MILLER, R., Strategizing for anticipated risks and turbulence in large-scale engineering projects. International Journal of Project Management, **19** (2001) 445-455.

[7] FLYVBJERG, B., BRUZELIUS, N., ROTHENGATTER, W., Megaprojects and risk: An anatomy of ambition. Cambridge University Press (2003).

[8] GOTCHEVA, N. Modelling the cultural complexity and safety culture challenges in nuclear industry project networks, article manuscript, forthcoming.

[9] GOTCHEVA, N., YLÖNEN, M., KUJALA, J., AALTONEN, K., Characteristics of complex projects in the Finnish nuclear industry: Interview study of three cases. Internal working report (2016).

[10] GULATI, R., PURANAM, P., TUSHMAN, M., Meta-organization design: Rethinking design in interorganizational and community contexts. Strategic Management Journal, **33** (2012) 571-586.

[11] HOLLNAGEL, E., The four cornerstones of resilience engineering. In Nemeth, C., Hollnagel, E., Dekker, S. (Eds.) Resilience Engineering Perspectives, Volume 2. Preparation and Restoration. Ashgate Publishing Ltd (2009).

[12] IAEA, Safety Reports Series 74. Safety Culture in Pre-operational Phases of Nuclear Power Plant Projects. Vienna: International Atomic Energy Agency (2012).

[13] INPO, Principles for Excellence in Nuclear Project Construction, INPO 09-007 (2010).

[14] KUJALA, J., AALTONEN, K., GOTCHEVA, N., PEKURI, A., Key dimensions of project governance and implications for safety in nuclear industry projects, Paper presented at the Sixth International Project Business Workshop, 19-20 November, 2015, Trondheim, Norway (2015).

[15] LEVESON, N., DULAC, N., ZIPKIN, D., CUTCHER-GERSHENFELD, J., CARROLL, J., BARRETT, B., Engineering Resilience into Safety-Critical Systems. In E. Hollnagel, D. D. Woods and N. Leveson (Eds.), Resilience Engineering – Concepts and Precepts. Ashgate Aldershot (2006) 95-123.

[16] MILCH, V., LAUMANN, K. Interorganizational complexity and organizational accident risk: A literature review, Safety Sci. **82** (2016) 9-17.

[17] NEMETH, C., HOLLNAGEL, E., DEKKER, S. Resilience Engineering Perspectives: Preparation and Restoration. Ashgate, Burlington (2009).

[18] OEDEWALD, P., GOTCHEVA, N. Safety culture and subcontractor network governance in a complex safety critical project, Reliab Eng Syst Safe, Special Issue 'Resilience Engineering', **141**, September (2015) 106-114.

[19] PETERS, T., WATERMAN, R. H., In Search of Excellence. Harper and Row, New York (1982).

[20] RASMUSSEN, J., Risk Management in a Dynamic Society: A Modelling Problem. Safety Sci. **27** (1997) 183-213.

[21] REASON, J., Human Error. Cambridge: Cambridge University Press (1990).

[22] REASON, J., Managing the Risks of Organizational Accidents. Ashgate, Aldershot (1997).

[23] REIMAN, T., OEDEWALD, P., Assessment of complex sociotechnical systems - Theoretical issues concerning the use of organizational culture and organizational core task concepts. Safety Sci. **45** (2007) 745-768.

[24] REIMAN, T., ROLLENHAGEN, C., Does the concept of safety culture help or hinder systems thinking in safety? Accident Analysis and Prevention, **68** (2014) 5-15.

[25] REIMAN, T., ROLLENHAGEN, C., PIETIKÄINEN, E., HEIKKILÄ, J., Principles of adaptive management in complex safety critical organizations. Safety Sci, **71** Part B (2015) 80-92.

[26] ROYAL ACADEMY OF ENGINEERING, Nuclear constructions lessons learned. Guidance on best practice: nuclear safety culture. The Royal Academy of Engineering, London, UK (2011).

[27] RUUSKA, I., AHOLA, T., ARTTO, K., LOCATELLI, G., MANCINI, M., A new governance approach from multi-firm projects: lessons learned from Olkiluoto 3 and Flamanville 3 nuclear power plant projects. International Journal of Project Management, **29** (2011) 647-660.

[28] RUUTU, S., System dynamics modelling of complex safety critical projects, Research report, VTT-R-05827-15, VTT Technical Research Centre of Finland Ltd. 2015.

[29] SCHEIN, E. Organisational Culture and Leadership (2nd ed) Jossey-Bass (1992).

[30] SCHEIN, E., Coming to a new awareness of organizational culture. Sloan Management Review, 25 (1984) 3-16.

[31] STERMAN, J., Business Dynamics: Systems Thinking and Modeling for a Complex World. Boston: Irwin McGraw-Hill (2000).

[32] STUK, Investigation of the procurement and supply of the emergency diesel generators (EDG) and related auxiliary systems and equipment for the Olkiluoto 3 nuclear power plant unit. The Radiation and Nuclear Safety Authority (2011).

[33] STUK, Management System for a Nuclear Facility, Guide YVL A.3 / 2 June 2014. Radiation and Nuclear Safety Authority (2014).

[34] TURNER J.R., SIMISTER S., Project contract management and a theory of organization. International Journal of Project Management, 19 **8** (2001) 457-464.

[35] VICENTE, K. J., Cognitive Work Analysis: Towards Safe, Productive, and Healthy Computer-Based Work. Mahwah, NJ: Lawrence Erlbaum (1999).

[36] YLÖNEN, M. Characteristics of safety regulation – comparison between Finnish nuclear industry and Norwegian petroleum industry, article manuscript, forthcoming.

BIBLIOGRAPHY

GOTCHEVA, N. OEDEWALD, P., WAHLSRTÖM, M., MACCHI, L, OSVANDER, A.-L., ALM, H. Cultural features of design and shared learning for safety: A Nordic nuclear industry perspective, Special Issue 'Learn and Train in Safety and Health', Safety Sci, January, **81** (2016) 90-98.

GOTCHEVA, N., OEDEWALD, P. SafePhase: Safety culture challenges in design, construction, installation and commissioning phases of large nuclear power projects, February, 2015:10, ISSN 2000-0456, Swedish Radiation Safety Authority (SSM) (2015).

REIMAN, T., OEDEWALD, P., Evaluating safety critical organizations: focus on the nuclear industry. Swedish Radiation Safety Authority, research report **12** (2009).

GOTCHEVA, N., OEDEWALD, P. Supporting safe design in the nuclear industry by understanding cultural features of design organizations. In 'Managing safety culture throughout the lifecycle of nuclear plants' (MANSCU), 2011-2014, Final project report, VTT Technology (2015).

OEDEWALD, P., PIETIKÄINEN E., REIMAN, T., A guidebook for evaluating organizations in the nuclear industry – an example of safety culture evaluation. Swedish Radiation Safety Authority (2011).

GOTCHEVA, N., OEDEWALD, P., VIITANEN, K., WAHLSTRÖM, M. Managing resilience throughout the nuclear power plant lifecycle: The significance of pre-operational phases, the 6th Symposium on Resilience Engineering, June 22-25, Lisbon, Portugal (2015).

GOTCHEVA, N., WATTS, G., OEDEWALD, P. Developing smart and safe organizations: An evolutionary approach, IJOA, 21 **1** (2013) 83-97.

MACCHI, L., GOTCHEVA, N., ALM, H., OSVALDER, A.-L., PIETIKÄINEN, E., OEDEWALD, P., WAHLSTRÖM, M., LIINASUO, M., SAVIOJA, P. Improving design processes in the nuclear domain: Insights on organizational challenges from safety culture and resilience engineering perspectives, Final report, Nordic Nuclear Safety Research, NKS-30 (2014).

OEDEWALD, P., GOTCHEVA, N., VIITANEN, K., WAHLSTRÖM, M. Developing safety culture and organizational resilience in nuclear industry throughout the different lifecycle phases, 'Managing safety culture throughout the lifecycle of nuclear plants' (MANSCU), 2011-2014, Final project report, VTT Technology (2015).

REIMAN, T., PIETIKÄINEN, E., OEDEWALD, P., GOTCHEVA, N. System modeling with the DISC framework: Evidence from safety-critical domains, Work, **41** (2012) 3018-3025.

MAKING SAFETY CULTURE A CORPORATE CULTURE
Modern safety thinking

J. SVENNINGSSON
Uniper
Malmö, Sweden
Email: johan.svenningsson@uniper.energy

J. LUNDSTRÖM
OKG AB
Oskarshamn, Sweden
Email: johan.lundstrom@okg.uniper.energy

S. BERGLUND
OKG AB
Oskarshamn, Sweden
Email: sara.berglund@okg.uniper.energy

Abstract

Safety Culture is something that has actively been worked with in the nuclear industry for a long time. Formally it has been on the agenda since the Chernobyl accident. However, the work with creating a safe organizational culture can of course be traced back even further in time. Over the years a lot has happened in the approach to safety culture and especially the view of human being as a part of the system and how the humans interact with the organization and technology. The paper is a general overview and will look at the evolution of the work conducted in establishing safety culture in the nuclear industry. Further, the aspects of modern safety thinking will be discussed and how this will aid in the continuous progression of safety culture. It will also highlight some of the problems in the past and present approach towards safety culture and how this can hinder future development. Finally, the importance of how to make safety culture into a corporate culture will be explained.

1. INTRODUCTION

For an organization to have a culture that promotes safety it is essential to create an ownership of safety with all workers within the site. To create this ownership it is vital to have the undivided commitment of the management. It all starts with the fundamental values of the organization. These values must then be concluded in firm expectations of behaviours that apply to all workers and management. This could be referred to as Expectation of a Professional Behaviour that allows us to live up to the company values.

Naturally, there are many aspects that are important to help us create an organizational climate which will promote the safety culture efforts. It is not as easy as just stipulating a number of values and expectations of behaviour. This could only be considered the foundation of success. However, to get a positive effect it is very important to have a certain frame of mind when it comes to safety and the development of a safety conscious organization. First of all, safety is nothing that “we have”; safety is something that we continually “do”! Furthermore, safety is not about the absence of accidents and incidents; safety is to understand what normally makes us succeed with what we do every day! This culture is set by the corporate management through values and behavioural expectations. The ownership of this culture is however something that must be in every workers possession, managers included.

To help keep this frame of mind alive there are nine (9) attributes (or tools) for integrating state-of-the-art safety in the outline for the future work within the field of safety culture [1].

These nine (9) attributes (or tools) lay as a foundation in the view of how the organization will reach a higher and safer effect regarding the organizations safety culture efforts. Accidents, or “bad things”, in the organization are not created by a combination of latent and active failures; they are the result of humans and technologies operating in ways that seem rational at a local level but unknowingly create unsafe conditions within the system that remain uncorrected. From this perspective, simply removing a ‘root cause’ from a system will not prevent the accident from recurring. To further develop our safety culture efforts, a more holistic approach is required whereby safety deficiencies throughout the entire system must be identified and addressed. An understanding of this is significant for the future development of our safety culture.

We must also stop treating safety as something we have or not-have. Safety is something that we continually are doing!

2. EVOLUTION OF SAFETY CULTURE

Safety culture as a concept was born after the Chernobyl accident, but the path was formed much earlier. The technical view of safety, or “the age of technology” was introduced within the industrial revolution in the 1800th century [2]. The invention of new machines and new technology brought effectiveness to the industry – but also new kinds of risks. Faults were mainly focused on the technology and whether it was safe or not. Even though the risks were greater when the technology became more common, the first risk analysis was introduced in 1961 [2].

The accident at Three Mile Island nuclear power plant (NPP), Harrisburg, in 1979 took us into a new era, “the age of human factors”. Technology was at this time considered to be safe, so the remaining cause for accidents were the humans. Faults were seen as people making mistakes, and if the behaviour of the employees could be controlled and limited, accidents could be reduced [2].

1986s’ accidents at the Chernobyl NPP and the explosion of the Challenger shuttle revealed that an accident is more complex than just the faults of humans. Organizations as a whole, and safety management, played an important part and many contributing factors were identified. Safety Culture as a concept was formed [2]. The safety culture concept was brought up again after the accident at Fukushima Daiichi, but also how the culture of the country as a whole influenced the workers at the plant. A systemic approach to safety have after the Fukushima accident been discussed as a new approach which is necessary for the organizations to apply to be able to increase safety standards.

Even though a systemic approach to safety is beginning to settle in the industry, research started study safety in a systemic way much earlier. In summary, 'systemic' means that organizations should be seen as a living organism whose prerequisites are always changing. The environment in which the employees work are dynamic and the goals are often conflicting or changing. The most common conflicting goals the industry today is struggling with are safety versus efficiency and profit. Both these goals are important for a business to blossom but blossom in different ways. The industry must find a good balance between these and the managers expectations of the employees must be clearly stated when this conflict becomes harshly real. As an employee, you sometimes face a situation when a job becomes critical for the progress of a project, or work order, as a whole, and you have to make a decision whether or not to take your time, benefiting the goal of safety or working faster, benefiting efficiency and profit. It might be hard for organisations in highly regulated industries to admit that goal conflicts actually exist, especially when most organisations proclaim overriding goals like "Safety First and Safety should and must always have the first priority". For a company to exist there must be other goals like sound economy, efficiency, productivity etc. It could be argued that as long as safety is the overarching goal, efficiency and productivity will follow. Unfortunately, this does not always play out in the messy reality of the daily work. Goal conflicts will often be the result when multiple goals are transpiring at the same time in complex work and constantly changing organisational settings.

The evolution of safety thinking has moved forward. Unfortunately, it is the big accidents that have made us realize these new aspects and approaches. The field of science studying the systemic age of safety has moved even further, but the safety critic organizations got stuck in the age of human factors and have had difficulties coping with a different kind of view of the human beings contributions to safety. Maybe one explanation is that the scientific field studying human behaviour in complex systems is a relatively new area. The area of technology has the upper hand. Maybe another explanation is the evolution of technology. The use of technology in our daily life, but also in the industries, has increased rapidly for the past 50 years and we have become so addicted to the aid of technology. We rely on it, we trust it and it is seen as safe.

The same is true for the system that we have built up around us. The term system in this context could mean everything from government legislation to organizational processes, procedures, manuals, instructions, checklists, etc. We put a lot of trust in our system. We trust that the legislative acts will lead us to safety. We trust that safety will be sustained as long as we follow our organizational procedures and process, etc. We do our very best to constantly follow and comply with the system we built up. We continuously audit our self to ensure that we fulfill the system requirements. Still accidents and mishaps occur, and it is necessary to ask ourselves why.

One explanation might be covered by the term "techno/system authority". This might illustrate the fact that we are slaves under the assumption that our systems and technology are safe and that the human factors are the unreliable element that must be constrained and harnessed. In short, we give our technology and the organizational systems we built up an authority. This creates an illusion, or in some cases even a stroke of complacency, in the infallibility of our systems. To move on and continue to increase our safety we must stop our belief in techno/system authority. It is important that we recognize that what seem to be perfectly safe systems are indeed prone to failure. It does not matter how much we try to eliminate error by building safer systems or more rigid technology. Our systems will continue to fail due to the high complexity of our operation and industry. This does not mean that we should stop trying to develop our system and technology to increase safety, but we must learn not to treat our system and technology as the final authority in a safe operation. An organizational system or a technical design can never substitute the human mind in dealing with the ever changing complex world we operate in. We must stop building the human out of the system and instead integrate our self in the same.

Homosapiens have looked more or less the same for the past 10 000 years but still we do not acknowledge the human being when designing new systems or new technology. We increase demands, change the surroundings, introduce new technology and believe the human being can cope. The revolution of technology has been, and still is, the centre aspect when it comes to new design. This approach has made it possible for people to be seen as bad apples. You might think you can solve your safety problems by telling your people to be more careful, by reprimanding the miscreants, by issuing a new rule or procedure and demanding compliance. But this is not the case. We have to start developing our surroundings, systems and new technology with the human mind and our cognitive functions as a primary target if we want to increase safety.

Even though we now have entered the age of safety management, and somewhat beginning entering the age of systemic safety, we are still seeing people as a problem, as a risk; a risk that should be constrained and, at fault, removed.

We have long searched for ways to limit human variability in – what we think are – otherwise safe systems. Performance monitoring, error counting and categorizing – these activities all assume that we can maintain our safety by keeping human performance within pre-specified boundaries. In fact, while we can make our systems safer, the human contribution to trouble remains stubbornly high. We have long put our hopes for improving safety on tightening the bandwidth of human performance even further. We introduce more automation to try to get rid of unreliable people. We write additional procedures. We reprimand errant operators and tell them that their performance is "unacceptable". We train them some more. We supervise them better, we tighten regulations.

Those hopes and ideas are now bankrupt. People do not come to work to do a bad job. Safety in complex systems is not a result of getting rid of people, of reducing their degrees of freedom. Safety in complex systems is created by people through practice – at all levels of an organization.

3. SAFETY THINKING

To be able to move forward, from the age of human factors into the age of a systemic view, a few things have to change. The industry today is very influenced by the things that go wrong. The accidents are analysed and countermeasures are set in place. But rather than treating accidents or "bad things" in the organization as a sequence of cause effect events, it should be seen as unexpected behaviour of a system resulting from uncontrolled relationships between its constituent parts. In other words, accidents are not created by a combination of latent and active failures; they are the result of human and technology operating in ways that seem rational at a local level but unknowingly create unsafe conditions within the system that remain uncorrected. From this perspective, simply removing a 'root cause' from a system will not prevent the accident from recurring. A holistic approach is required whereby safety deficiencies throughout the entire system must be identified and addressed. To further develop our safety culture, an understanding of this is significant.

The ultimate goal is to build a mature and proactive organizational culture, which does not merely react to unwanted events. To help keep this frame of mind alive, there are nine (9) attributes (or tools) for integrating state of the art safety in the outline for the future work within the field of safety culture [1].

- **Human error is seen as symptom and not as cause**. This does not cancel responsibility and accountability of workers and managers but we have to understand the prerequisites for our employees, the variability in the organization and accept this variability. *"Human error is a symptom of trouble deeper inside a system [not a cause]"* [3]. This means that the complexity in the system, and the prerequisites for the employee, influenced human performance [1].
- **Avoidance of hindsight bias**. We try to understand the course of events from the place of the actors and not as external observers. As an observer you have all the facts and you know the results of the decisions made, but we have to try to understand why the decisions made sense at that time. *"Hindsight means being able to look back, from the outside, on a sequence of events that led to an outcome you already know about"* [3]. *"Avoiding hindsight bias requires changing our emphasis in analysing the role of*

humans in accidents from what they did wrong to why it made sense for them to act the way they did" [4].

- **Shared responsibility**. Both good and adverse outcomes result from interdependencies and interactions of all organizational functions. An event can't be isolated. We have to look at other functions to see, identify and understand the complexity of the reality. *"The starting point for the Individual Blame Logic (IBL) is the assumption that people make mistakes because they do not pay enough attention to the task they are doing. It, therefore, adopts a causal linear model leaving the organizational context mostly in the background. The efforts to find the blame are as a result directed to people in the front line and the result of the approach is the attribution of the blame. If the guilty person is found, he or she can be held responsible for the accident. In practice this may mean that the 'bad apple' will be removed or prosecuted"* [6]. In contrast to IBL, the Organization Function Logic (OFL) *"/…/ reconducts the causal factors of an event to the whole organization [shared responsibility]. It acknowledges that accidents, incidents or mishaps are the result of mistakes made by individuals but these mistakes, however, are socially organized and systematically produced"* [5].
- **Focus on success rather than solely on failures**. We need to understand how employees perform well under constantly changing conditions and conflicting goals. *"Things basically happen in the same way, regardless of the outcome. The purpose of an investigation is to understand how things usually go right as a basis for explaining how things occasionally go wrong. Humans are seen as a resource necessary for system flexibility and resilience"* [6].
- **Feedback mechanisms**. System processes in addition to their planning and operation must be constantly monitored in order to allow adjustments. An organization is to be seen as a living organism and for it to work we have to rely on both feedforward and feedback.
- **Avoidance of folk models**. The use of abstract statements without further explanations (e.g., lack of motivation, boredom, and loss of awareness) does not support our understanding of why things do not go well. *"Folk models as used in human factors to explain large sequences of complex behavioural events seem to share the following characteristics: They explain by means of substitution instead of decomposition. They are immune against falsification. They tend to rely on overgeneralization"* [7]. *"Folk models are easily made because the concept of these terms is ill-defined. Often folk models offer a popular, but not necessarily helpful, characterization of difficult phenomena"* [3].
- **Non-counterfactual approach**. In addition to comparing performance with standards, we must explore the underlying reasons for non-adherence to procedures. Counterfactual could be explained as; *"They lay out in detail*

what these people could or should have done to prevent the mishap" [4]. When looking back at what happened, we cannot use words like "could" or "should" to point towards decisions not taken or actions not carried out. Such statement will not help us understand why people in fact did what they did.

- **Non-judgmental attitude**. Apart from comparing performance with norms and expectations, we need to both question established "norms" and explain why people do not act as expected. Judgmental could be explained a; *"Judge people (e.g. not taking enough time, not paying enough attention, not being sufficiently motivated) for supposed personal shortcomings"* [3]. Because humans are a part of our systems, it is very hard not to look or investigate what role the human plays contributing to the outcome, or the accident. But when doing so, we cannot judge the humans involved for doing or not doing something they should or should not have done. *The judgmental approach is the one that emphasizes mostly on the actions of the end user compared to what was expected according to some norm, either implied or explicit (e.g. training, role, qualifications, experience)* [1].
- **Systemic view**. Good and unwanted events result from continuous interaction among systems elements under variable conditions and multiple objectives. Up until today, we have focused almost solely on problems and why things don't work how they are supposed to. We analyse incidents and accidents to try improving the organization. But with this approach we are only looking and taking in consideration a very small part of the work carried out on a daily basis. When the outcome of a work process is as expected, we move on without reflecting on why we reached success. If we start looking at what, and why, things work out as expected, we can learn from the positive. These positive experiences could further be applied to other processes and help us increase safety. We still have to analyse and learn from the bad, but not looking at what goes right could be seen as a missed opportunity to learn.

4. MAKING SAFETY CULTURE INTO A CORPORATE CULTURE

These nine (9) attributes describe modern safety thinking and to be able to incorporate this view in an organization, it is important to recognize some general prerequisites that must be present in the organization.

Karanikas et al. [8] suggests that these prerequisites are:

- Management commitment,
- Leadership,
- Clear responsibilities and accountabilities of all management areas towards safety,
- Safety department visibly responsible and accountable for safety planning,

- Employee involvement,
- Non-reliance on past success,
- Risk management policy,
- Planning for buffers,
- Rewarding safety initiatives,
- Internal communication,
- External communication.

For a modern safety thinking to be successful, the management commitment is essential. The changes have to start at the top to further be incorporated down in the whole organization. This commitment should be clearly stated and written down, but it is equally important that the management shows this commitment visually throughout their daily work. With a strong commitment comes strong leadership that will help the organization navigate towards a strong safety culture. Even though the change has to start from the top, all employees have a responsibility regarding safety. For the employees to be able to personally strengthen the safety culture, they have to feel valued and involved. The employees have valued knowledge of the daily operation and should be involved in the day-to-day planning and decision-making. If the employees are engaged in planning, monitoring and improvement of the company, the success rate will increase. The employee's contribution to safety is important to acknowledge. The daily contribution is somewhat expected but the contributions that go beyond, such as new ideas and voluntary participation in safety plans, should be rewarded [8].

Safety is something that has to be discussed, and worked towards, every day. Safety is not something that we have, it is something we continually do, and it has to be tended at a daily basis. The environment in which we operate is constantly changing, and therefore, safety is not a goal we will reach someday. Because of this, we cannot rely on yesterday's safety. Every decision that is to be made that could influence safety needs to be assessed based on a risk management framework, tailored to each level of decision making. This will help in assessing and planning each work effort based on prerequisites present in specific situations. Further, it will help optimize resources and in the long run also create an organization that will be able to cope with the unexpected [8].

There are of course many aspects that are important to help us create an organizational climate which will promote the safety culture efforts. It is not as easy as just stipulating a number of values and expectations of behavior. This could be considered the foundation to succeed but to get a positive effect it is very important to have a certain frame of mind when it comes to safety and the development of a safety conscious organization.

5. CONCLUSION

Historically, failure is seen as people making mistakes. The human factor causing accidents, as if failure is a process separated from the one of success. Failure is when the organization goes from a safe to an unsafe state. Whereas today, safety should be seen as something that emerges from our daily work and the same is to be said about failure. Failure is introduced into the system when it fails to adjust to the dynamic reality in which it operates. If organizations are to be seen as living organisms whose prerequisites are changing, we have to understand that success and failure is the outcome of normal performance variability. And because this is the reality in which we operate, performance variability should be controlled rather than constrained. The ability to control this variability will be achieved through resilience and a systemic view of safety. The understanding of this is vital to integrate safety culture into a corporate culture.

ACKNOWLEDGEMENTS

A special thanks to Amsterdam University of Applied Sciences, Aviation Academy, by who's devoted and inspiring work have motivated Oskarshamn nuclear power station to advance in the ongoing work developing safety culture into a corporate culture. Especially worth mentioning are the dedicated researchers Dr. Nektarios Karanikas, Prof. Robert Jan de Boer, Dr. Alfred Roelen, Prof. John Stoop, Pedram Soltani and Prof. Sidney Dekker, by who's help and sharp minds have inspired OKG to improve within the state-of-the-art view on safety.

REFERENCES

[1] KARANIKAS, N., et al., "Evaluating Advancements in Accident Investigations Using a Novel Framework", Proceedings of the Air Transport and Operations Symposium, 20th-22nd July 2015, Delft University of Technology, Netherlands, 2015.

[2] HOLLNAGEL, E., "From safety -1 to safety-2: An introduction to resilience engineering", Presented at Human Factors Network in Sweden seminar on subject Resilience engineering – From safety 1 to safety 2, Linköping Sweden, 2013.

[3] DEKKER, S., The Field Guide to Understanding Human Error, 2nd edition, Ashgate Publishing Limited, (2006).

[4] LEVESON, N., Engineering a Safer World: Systems Thinking Applied to Safety, MIT press, (2011).

[5] CATINO, M., A review of literature: Individual blame vs. organizational function logics in accident analysis, Journal of Contingencies and Crisis Management (2008) 53-62.

[6] HOLLNAGEL, E., Safety-I and Safety-II: The Past and Future of Safety Management, Ashgate Publishing Limited, (2014).

[7] DEKKER, S., HOLLNAGEL, E., Human factors and folk models, Cognition, Technology & Work (2004) 79-86.

[8] KARANIKAS, N., et al., OKG Phase 2 Project Report (FUD Project Report – Safety Culture), internal report, OKG AB, Oskarshamn Sweden, 2015.

PERSPECTIVE ON HUMAN AND ORGANIZATIONAL FACTORS (HOF)
Attempt of a systemic approach

F. MEYNEN
Swiss Federal Nuclear Safety Inspectorate ENSI
Brugg, Switzerland
Email: friedrich.meynen@ensi.ch

Abstract

Human and organizational factors (HOF) neither constitute new issues nor are they just issues of the nuclear industry. As a result of increasing system complexity in the entire industry with high risk potential for humans and the environment, not only the requirements for technical systems increase but also the human and organizational demands rise (or even completely change) due to technical progress in such a way that these need to be redefined. In the presentation, the project will examine whether risks can be reduced with the "human factor" by systemic approach regarding the interaction between man, technology or organization and which further questions arise thereby.

1. INTRODUCTION

Many accidents – also in the non-nuclear industry – show that strong links frequently exist between the technical, human and organizational aspects. The so often associated, classic response in case of incidents/accidents etc. is, that in the end humans are (or were) always involved since they created, maintained, supervised and monitored the technical systems. Provocatively it can be concluded that therefore always the classic answer "human failure" applies. This statement carries the risk that analyses will not be carried out systematically or at great length. From this follows the necessity of intensive dealing with human and organizational factors (HOF), the interaction and in particular the interfaces between human, technology and organization, respectively. The following figure shows that the human factor follows a primeval concept, which depicts human individuals correlating with their surrounding and its corresponding interaction. Everyone exists in an environment. The interaction between humans and the environment exists at all times. Man can act through his behavior to his surrounding and himself. The influence of the environment on humans represents an external effect. The immediate effect of individuals to themselves is an inner influence. Each act of man upon environment or himself is called human factor(s) HF.

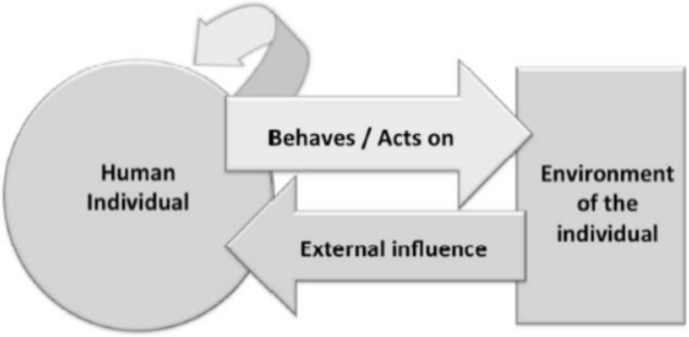


FIG. 1. Individual environment interference/interaction scheme [1].

In the first HF approaches in the nuclear industry after 1979 (Three Mile Iceland) the ergonomics and the human/technology interactions were intensely reflected. Whereas only the operation and monitoring of processes were brought into focus at that point. The maintenance procedures regarding plant operation were not observed since the systems are usually deactivated for this purpose and therefore the risk exposure is assumed to be much lower. Furthermore, in the nuclear industry it is common practice to use very detailed indications, leading to the erroneous opinion that one could thus prevent (human) errors. Besides, one cannot replace required know-how with detailed instructions. This is one of the widespread incongruities.

- **Example 1:** For the maintenance of special components such as pumps, valves, etc. are partially specialists of the manufacturers required to some extent. They must have the specific know-how of the components. How will this be ensured?
  Can a very precise maintenance instruction of a component replace the expertise and know-how of a maintenance specialist?
- **Example 2:** For the commissioning of systems and components well-trained operating personnel is required (in the control room and on-site). The necessary procedures became more specific nowadays. How can someone’s best attention be arrested, when everything is accurately described?
  Can a precise commissioning instruction replace the expertise and know-how of an operator?

The two simple questions already show the complexity of the interaction between technical, human and organizational aspects. It can be deducted that excellent in-depth knowledge and solid experience in the corresponding field(s) are required. Besides, one should not put only the focus on the control room personal, but take also into account the "support organizations" (maintenance, analysis, monitoring, etc.) and in parallel the various manufacturers. Since these "support organizations" are mainly responsible for ensuring the technical performance of the entire plant their significant role in the entire system should not be undervalued. This results in the following requirement:

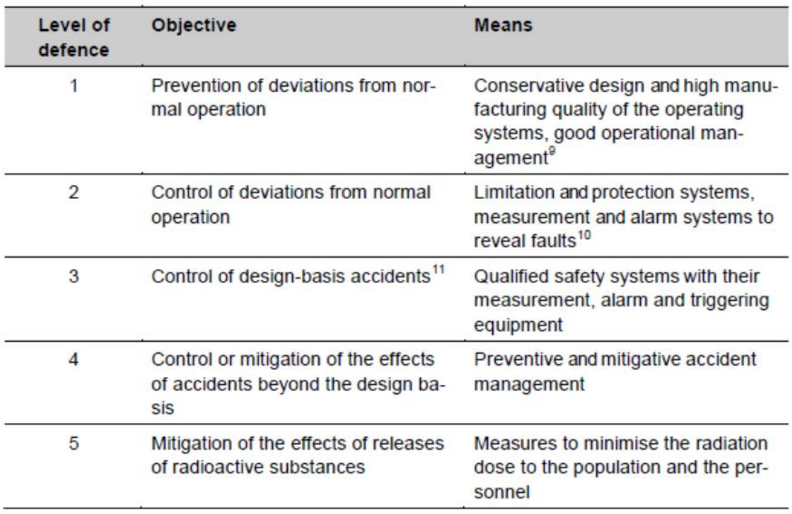
Trained and periodically checked expertise and solid experience in the respective fields are the basis for safety-oriented human actions.

This involves in particular the following two conditions:

- An organization appropriate for the requirements;
- Sufficient qualified and trained personnel.

The different requirements for the technical systems can be appointed to different levels of safety and thus to a staggered defense-in-depth assign. The resulting requirements are specifiable as "single fault detection", "redundancy" and "diversity". For the human and organizational requirements this division is not obviously definable to such an extent. The safety of a nuclear power plant depends on the technology used, its state of condition and the people operating it as well as the organizational structures and their tools.

Defense-in-depth



Level of defence	Objective	Means
1	Prevention of deviations from normal operation	Conservative design and high manufacturing quality of the operating systems, good operational management[9]
2	Control of deviations from normal operation	Limitation and protection systems, measurement and alarm systems to reveal faults[10]
3	Control of design-basis accidents[11]	Qualified safety systems with their measurement, alarm and triggering equipment
4	Control or mitigation of the effects of accidents beyond the design basis	Preventive and mitigative accident management
5	Mitigation of the effects of releases of radioactive substances	Measures to minimise the radiation dose to the population and the personnel

FIG. 2. Levels of defense-in-depth [2].

In addition to the staggered defense-in-depth provisions in the technical field with their related safety levels exist similar precautions in the organizational field. Some of the problems are the interfaces between the different organizational areas, people with different requirements and the different technology used in each case. From this follows that in different organizational areas different approaches apply. Furthermore, the particular culture of the country, the company, the nuclear installation, the department, the areas etc. play a significant role. Individual elements of the plant, many organizational structures and tools, but especially the people working in a nuclear power plant cannot be assigned uniquely to individual safety levels.

Hence the necessity arises to take action reducing the probability of errors and strengthen the barriers. This involves in particular the following two conditions:

- A strong corporate governance, which gives priority to nuclear safety at all times;
- An integrated management system that structures all safety-related activities.

A clear, well understandable management system for quality assurance and meaningful measures to promote a good safety culture helps the organization to reduce the likelihood of human error and to strengthen the people as a safety factor.

In the following figure the Swiss cheese model of Reason shows a few examples of measures that are possible in the context of a good work planning.

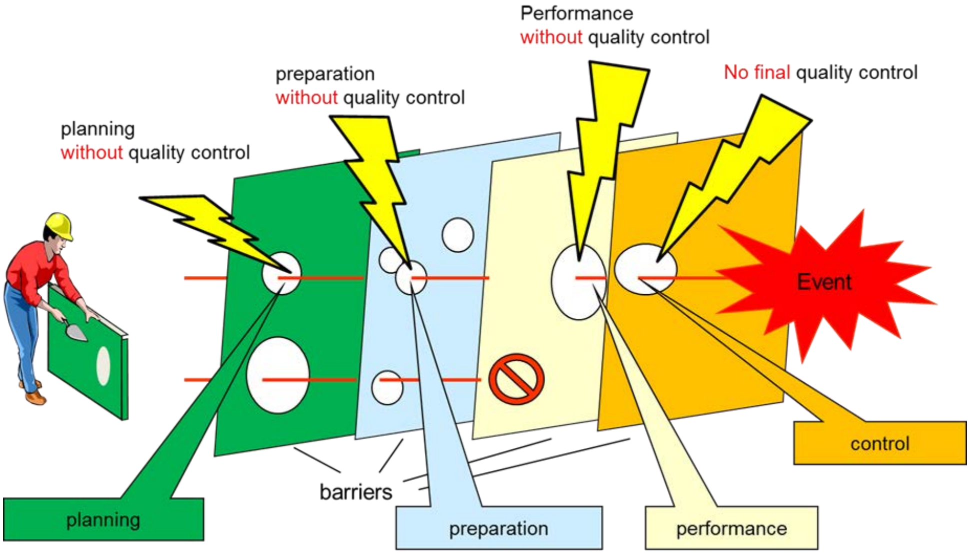


FIG. 3. Work practice in maintenance based on Reason model [3].

Stated below are some examples or methods to reduce chances of human errors in the field of work planning, preparation and performance:

- Four-eye principle
- Three-way communication
- STAR (Stop-Think-Act-Review)
- ODM (operational decision making)
- Peer-checking
- Pre-job briefing / debriefing
- Regulations
- Checklists
- Reporting system
- Training and qualification systems

These instruments or methods are used in many organizations and their use is supported by international organizations (e.g. WANO). These instruments also run frequently under the name of "human performance tools". They can essentially be divided into the three following groups:

(1) Duplication of control
(2) Decisions based on wide base
(3) Experience and expertise preservation

Still missing is the external influence on the actions of individuals. At this point group responsibility, producer responsibility and operational responsibility play a major role in terms of a safe and trustworthy operation. These responsibilities are influenced directly and indirectly by politics, society, the media and the surveillance to a greater or lesser extent. The following illustration tries to provide an overview of systemic dependencies and interrelationships.

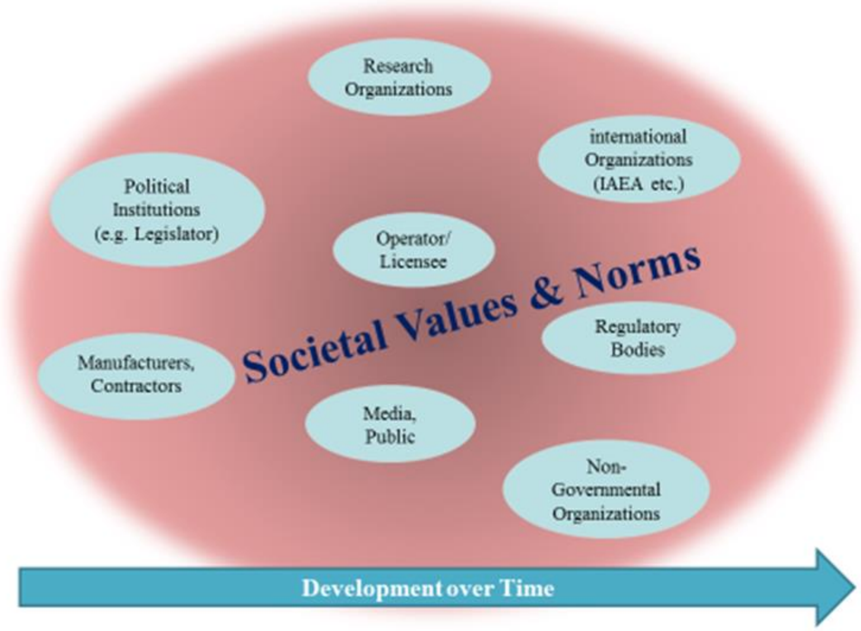

Research Organizations
international Organizations (IAEA etc.)
Political Institutions (e.g. Legislator)
Operator/ Licensee
Societal Values & Norms
Regulatory Bodies
Manufacturers, Contractors
Media, Public
Non-Governmental Organizations
Development over Time

FIG. 4. Overall system of stakeholders [4].

These dependencies should be examined more closely using some examples.

Is politically and medially a technique no longer recognized, will this risk decreasing motivation of employees affected and therefore the loss of the vital know-how of the application, the use and consequently the safety-related improvement of it.

If a technique is praised politically and medially as the best to achieve a goal, this entails the risk that not all resulting hazards from this technique are realized as such and that the safety development of this technology is not promoted.

These two examples show the importance of a corporate culture that promotes the handling of errors and learning from experience and wants and fosters a continuously improvement and takes as well into account the cultural related dependencies.

2. CONCLUSIONS

The technical systems will always be evolving and their reliability increases thereof. On the other hand, the question which impact occurs through this in the domain of organization and the individuals acting in this system will not always be analyzed as penetrative as may be necessary. To reduce the complexity, only single aspects such as "safety culture", "management system", "training", "organizational structure" etc. are verified but a systemic approach is ignored on a regular basis.

REFERENCES

[1] INTERNATIONAL JOURNAL OF PERFORMABILITY ENGINEERING, A Systematic Approach to Oversee Human and Organizational Factors in Nuclear Facilities, Vol. 10, No. 7. November 2012 (2012).

[2] SWISS FEDERAL NUCLEAR SAFETY INSPECTORATE ENSI, Oversight of Safety Culture in Nuclear Installations, ENSI Report on Oversight Practice, ENSI-AN-8980, ENSI, Brugg/Switzerland (2014).

[3] JAMES T. REASON,“Managing the Risks of Organizational Accidents” Aldershot, Ashgate (1997)

[4] SWISS FEDERAL NUCLEAR SAFETY INSPECTORATE ENSI, Oversight of Safety Culture in Nuclear Installations, ENSI Report on Oversight Practice, ENSI-AN-8980, ENSI, Brugg/Switzerland (2014).

REINFORCING DEFENCE IN DEPTH – A PRACTICAL SYSTEMIC APPROACH

JOZEF MISAK
UJV REZ A.S.
Husinec, Czech Republic
Email: Jozef.Misak@ujv.cz

GERMAINE WATTS
Intelligent Organizational Systems
Bayswater, Canada
Email: germainewatts@intelorgsys.com

Abstract

The concept of defence in depth for ensuring nuclear safety of nuclear installations is often oversimplified and interpreted as a set of physical barriers, whose integrity is ensured by safety provisions in the form of the plant systems implemented independently at various levels of defence. However, the provisions established at each level of defence should in general terms include not only hardware components (active and passive systems), but more comprehensively, also inherent safety characteristics, safety margins, operating procedures and guidelines, quality assurance, safety culture, staff training, and many other organizational measures as parts of management of safety. Many of the above mentioned provisions belong to the category of human and organizational factors. While various hardware components are typically specific for different levels of defence, human and organizational factors may have an impact on several levels of defence. These factors are associated with large uncertainties due to their emergent property and can result in latent weaknesses. This paper discusses how a strengthened focus on human and organizational factors, along with a systemic approach to safety, can enhance defence in depth in practice. In the first part it introduces a screening method developed by the IAEA as a tool for facilitating systematic assessment of the comprehensiveness of defence in depth. This method uses screening of safety provisions at five levels of defence to ensure integrity of the physical barriers and achievement of safety objectives at each level of defence. This part of the paper includes an example of how the method is applied to human and organizational factors. Opportunities for strengthening the role of human and organizational factors in defence in depth are also indicated. The second part focuses on how a systemic perspective can be used to understand the dynamics within and between organizations, making it possible to anticipate otherwise invisible challenges to safety. It uses the example of what changes when a situation shifts from level 3 to 4 of the defence in depth framework to show how a systemic perspective can reveal hidden vulnerabilities and concludes with a brief look at how leadership that builds shared space during normal operating conditions can ensure the resiliency required at levels 4 and 5.

1. INTRODUCTION

The defence in depth concept is based on hierarchical deployment of multiple physical barriers and five levels of complementary barriers that combined, are intended to ensure protection of workers, the public and the environment against the harmful effects of ionizing radiation. This is an essential strategy for ensuring safety of nuclear power plants, Ref. [1, 2].

This strategy should be comprehensively applied to all stages of a plant's life, from siting through construction and operation up to decommissioning. Defence in depth ensures that the safety functions are reliably achieved with sufficient margins to compensate for equipment failure and human errors. The importance of defence in depth is highlighted in a number of IAEA Safety Standards, e.g. Ref. [3,4,5] and the necessity of maintaining and strengthening defence in depth has been recognized within important international forums Ref. [6].

1.1. Objective tree method – screening comprehensiveness of defence in depth

In the late 1990's it was recognized by the IAEA that a practical tool aimed at facilitating assessment of the comprehensiveness of defence in depth was needed. While all NPPs have physical barriers and means to protect those barriers, their level of defence can be very different. It became also necessary to emphasize that the measures for protecting workers, people and the environment involve much more than just NPP technological systems and procedures.

These efforts resulted in the development of a screening method described in detail in IAEA Safety Report No. 46 on "Assessment of Defence in Depth for Nuclear Power Plants", Ref. [7] published in 2005. The method uses objective trees (Fig. 1) to screen the availability of safety provisions at five levels of defence. The provisions are aimed at preventing mechanisms from challenging safety functions, so that the integrity of physical barriers and safety objectives is maintained at each level of defence.

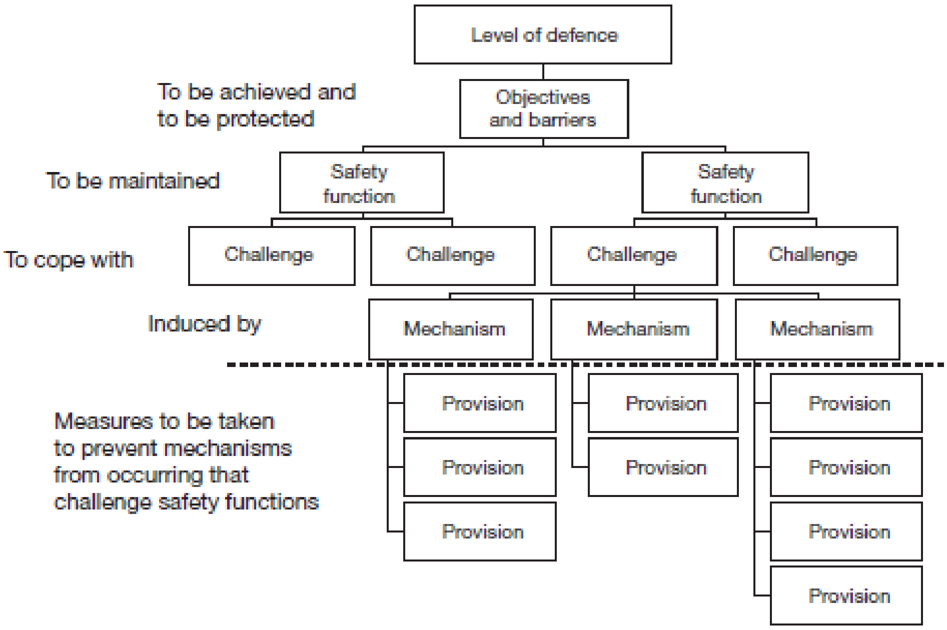


FIG.1. Structure of the objective tree at each level of defence.

A top down approach has been used for the development of objective trees, i.e. from stating the objectives and relevant safety functions for each level of defence, through identification of the challenges to performance of these safety functions composed of various mechanisms affecting the performance, ad ending up at the provisions which may be implemented to prevent challenges to the safety functions from taking place.

Graphical depiction of the links between safety objectives and safety provisions as an objective tree helps to identify weaknesses in defence in depth and supports the questioning attitude essential for nuclear safety. Screening by means of objective trees should be understood not only as a comprehensive tool for assessment, but also as a way of thinking about nuclear safety in very broad sense.

INSAG-12, Ref. [2] introduced a number of general and specific basic safety principles. These are shown in Fig. 2 below which provides useful guidance for ensuring the comprehensiveness of safety provisions, as well as the mechanisms and challenges to performance of the safety functions.

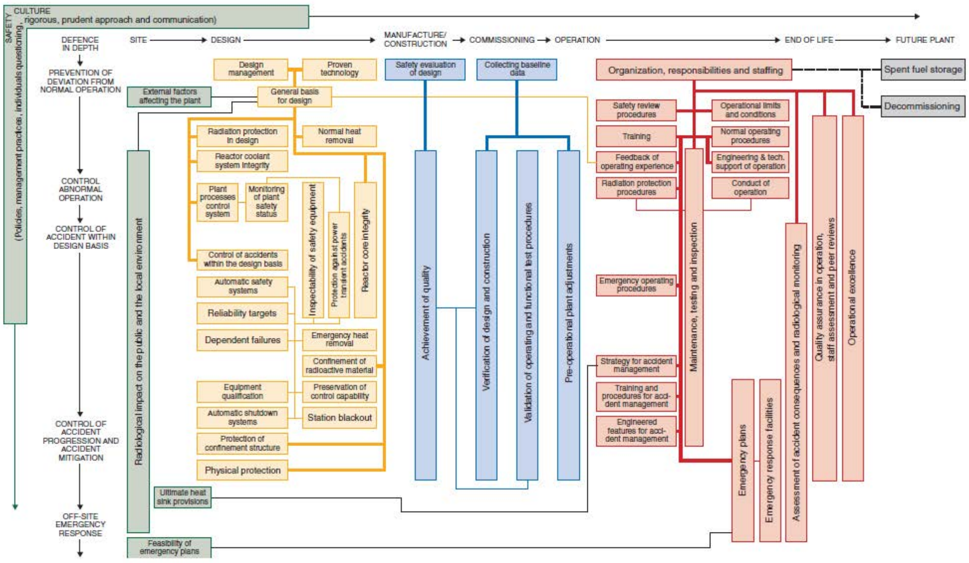

SAFETY CULTURE (Policies, management practices, individuals questioning, rigorous, prudent approach and communication)
DEFENCE IN DEPTH
PREVENTION OF DEVIATION FROM NORMAL OPERATION
CONTROL ABNORMAL OPERATION
CONTROL OF ACCIDENT WITHIN DESIGN BASIS
CONTROL OF ACCIDENT PROGRESSION AND ACCIDENT MITIGATION
OFF-SITE EMERGENCY RESPONSE
SITE
DESIGN
MANUFACTURE/ CONSTRUCTION
COMMISSIONING
OPERATION
END OF LIFE
FUTURE PLANT
External factors affecting the plant
Radiological impact on the public and the local environment
Ultimate heat sink provisions
Feasibility of emergency plans
Design management
Proven technology
General basis for design
Radiation protection in design
Normal heat removal
Reactor coolant system integrity
Plant processes control system
Monitoring of plant safety status
Inspectability of safety equipment
Protection against power transient accidents
Reactor core integrity
Control of accidents within the design basis
Automatic safety systems
Reliability targets
Dependent failures
Emergency heat removal
Confinement of radioactive material
Equipment qualification
Preservation of control capability
Automatic shutdown systems
Station blackout
Protection of confinement structure
Physical protection
Safety evaluation of design
Achievement of quality
Collecting baseline data
Verification of design and construction
Validation of operating and functional test procedures
Pre-operational plant adjustments
Organization, responsibilities and staffing
Spent fuel storage
Decommissioning
Safety review procedures
Operational limits and conditions
Training
Normal operating procedures
Feedback of operating experience
Engineering & tech. support of operation
Radiation protection procedures
Conduct of operation
Maintenance, testing and inspection
Emergency operating procedures
Strategy for accident management
Training and procedures for accident management
Engineered features for accident management
Emergency plans
Emergency response facilities
Assessment of accident consequences and radiological monitoring
Quality assurance in operation, staff assessment and peer reviews
Operational excellence

FIG. 2. Schematic of INSAG-12 specific safety principles and their interrelations.

The process for constructing an objective tree is illustrated in the following example:

Safety principle applicable for Levels 1-3: Protection against power transient accident

Safety function to be potentially affected: To prevent unacceptable reactivity transient

Challenge to the safety function: Insertion of reactivity with potential fuel damage

Mechanisms contributing to the challenge: 1). Control rod (CR) withdrawal; 2). CR ejection; 3). CR malfunction; 4). Erroneous start-up of a main circulation loop; 5). Release from the core of absorber deposits; 6). Incorrect refueling operations; 7). Inadvertent boron dilution

Provisions (examples only for 1st mechanism)

For Level 1:

Design margins minimizing need for automatic control
Operational strategy with most rods out

For Level 2:

Monitoring of control rod position
Limited speed of control rod withdrawal
Limited worth of control rod groups

For Level 3:

Negative reactivity feedback coefficient
Conservative set-points of reactor protection system
Reliable and fast shutdown system

The objective tree for this example at Level 1, is depicted in Fig. 3 below.

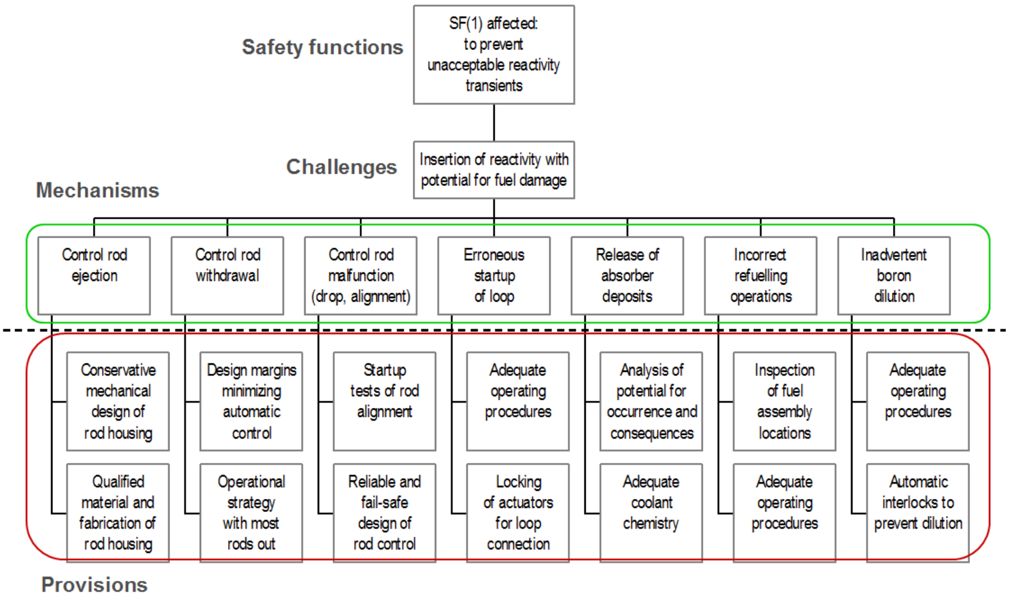

Safety functions
SF(1) affected: to prevent unacceptable reactivity transients
Challenges
Insertion of reactivity with potential for fuel damage
Mechanisms
Control rod ejection
Control rod withdrawal
Control rod malfunction (drop, alignment)
Erroneous startup of loop
Release of absorber deposits
Incorrect refuelling operations
Inadvertent boron dilution
Conservative mechanical design of rod housing
Qualified material and fabrication of rod housing
Design margins minimizing automatic control
Operational strategy with most rods out
Startup tests of rod alignment
Reliable and fail-safe design of rod control
Adequate operating procedures
Locking of actuators for loop connection
Analysis of potential for occurrence and consequences
Adequate coolant chemistry
Inspection of fuel assembly locations
Adequate operating procedures
Adequate operating procedures
Automatic interlocks to prevent dilution
Provisions

FIG. 3. Objective tree for Level 1 of defence in depth, corresponding to safety principle "Protection against power transient accidents".

Similar trees corresponding to the same safety principle have been developed for other levels of defence and for all other safety principles. In total, Safety Report No. 46 presents 69 objective trees with 95 identified challenges (some of them applicable for several levels of defence), 254 different mechanisms, and 941 different provisions.

1.2. Need to strengthen human and organization factors in defence in depth

The concept of defence in depth is often oversimplified and misinterpreted as a set of physical barriers whose integrity is ensured by plant safety provisions implemented at various levels of defence. However, it is important to emphasize that the screening method presented in Safety Report No. 46 recognizes the importance of considering the large variety of provisions necessary for ensuring plant safety, including not only technological but equally important human and organizational provisions, such as inherent safety characteristics, safety margins, active and passive systems, operating procedures, operator actions, human factors and other organizational measures, including safety culture aspects.

While plant technological systems are very important, they are not the only important components of defence in depth. Fig. 4 below illustrates a “soft” objective tree related to human and organizational factors. The challenge, mechanisms and associated provisions related to safety culture are highlighted by the red circle. There are many such ‘soft’ objective trees included in Safety Report No. 46.

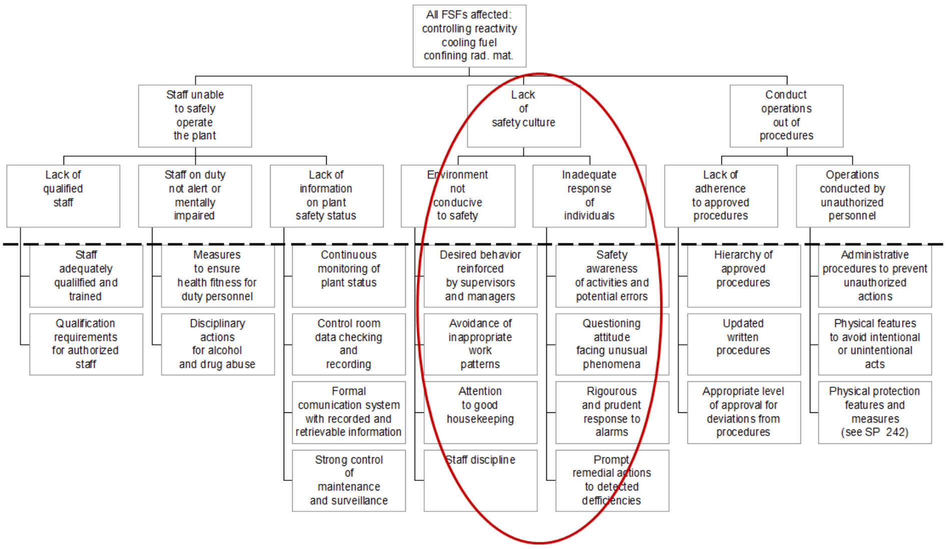

All FSFs affected: controlling reactivity cooling fuel confining rad. mat.
Staff unable to safely operate the plant
Lack of safety culture
Conduct operations out of procedures
Lack of qualified staff
Staff on duty not alert or mentally impaired
Lack of information on plant safety status
Environment not conducive to safety
Inadequate response of individuals
Lack of adherence to approved procedures
Operations conducted by unauthorized personnel
Staff adequately qualilfied and trained
Qualification requirements for authorized staff
Measures to ensure health fitness for duty personnel
Disciplinary actions for alcohol and drug abuse
Continuous monitoring of plant status
Control room data checking and recording
Formal comunication system with recorded and retrievable information
Strong control of maintenance and surveillance
Desired behavior reinforced by supervisors and managers
Avoidance of inappropriate work patterns
Attention to good housekeeping
Staff discipline
Safety awareness of activities and potential errors
Questioning attitude facing unusual phenomena
Rigourous and prudent response to alarms
Prompt remedial actions to detected defficiencies
Hierarchy of approved procedures
Updated written procedures
Appropriate level of approval for deviations from procedures
Administrative procedures to prevent unauthorized actions
Physical features to avoid intentional or unintentional acts
Physical protection features and measures (see SP 242)

FIG. 4. Objective tree for Level 1 of defence in depth (other levels covered separately), corresponding to safety principle “Conduct of operations”.

The IAEA Report on ‘Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant’, Ref. [8] renewed emphasis on the importance of assessing and strengthening human and organizational factors in support of defence in depth. Recommendations included:

— Strengthening mutual cooperation among all stakeholders (operators, vendors, regulators, contractors, TSOs, corporate organizations, international organizations) utilizing new communication interfaces and arrangements
— Strengthening interdisciplinary expertise through involvement of the social and behavioural sciences
— Continuously improving maintenance management and establishing closer cooperation with manufacturers and contractors
— Consideration of human and organizational factors in the planning, conduct and evaluation of emergency drills and exercises

- Identification of additional training, including understanding resilience, for operating personnel
- Enhancing the dialogue between the regulatory body and operating organization on topics beyond compliance and regulations, on safety practices and policies
- Enhanced efforts by the regulatory body to go out in the field and engage the licensee in conversations at the working level about safety practices and policies
- Establishing and maintaining the trust of local communities.
- Implementation of more practical ways for managers to strengthen safety culture supporting prioritization of nuclear safety (in particular, if a NPP is part of a non-nuclear utility)
- Strengthening leadership and management for safety, mainly for top-level managers
- Objectively assessing efforts to strengthen safety and widely informing staff about safety initiatives
- Demonstrating high priority to safety culture by proactively introducing actions and ensuring resources for safety upgrading
- Recognizing the efforts of personnel to protect and ensure the safety of the public, the workers and the plant
- Implementing improvements with regard to decision making and consideration of the use of tools to support decision making in emergency response

It is relatively straight forward to incorporate these recommended improvements into the series of ‘soft’ objective trees and in this way to make them a more practical and more comprehensive screening tool for ensuring defence in depth.

2. REINFORCING DEFENCE IN DEPTH – A PRACTICAL SYSTEMIC APPROACH

In addition to making recommendations on how to strengthen human and organizational factors within the defence in depth framework, IAEA Report Ref. [8] emphasized the importance of *adopting a systemic approach to safety that considers the interaction between individual, technical and organizational factors*. This recommendation takes us a step beyond the inclusion of human and organizational factors in ‘soft’ objective trees. It points to the need to investigate the non-linear interactions between the hard and ‘soft’ logic trees, and to look beyond organizational boundaries, in order to gain insight into otherwise invisible or latent challenges that can potentially affect each and all levels of defence in depth (including at the same time) across the nuclear programme.

This systemic approach to safety recognizes that human behaviour does not happen in a vacuum: rather that the goals, expectations and concerns of different parties (whether individuals, groups, or whole organizations), are influenced by relationships with, and perceptions and expectations of other parties. For example, how a regulator views a licensee and licensee views the regulatory body influences the nature of their interaction and their combined focus on safety. The same is true for other relationships including those with technical support organizations, suppliers, governmental bodies, professional associations, community groups, and more. What this means in practice is that the behaviour of the system is characterized by very high degrees of complexity and uncertainty.

It is an over-simplification to view nuclear power programmes as ‘complicated’ systems wherein expertise, logic, systematic planning, and finely tuned policies and procedures can be relied upon to ensure seamless operation. They are more accurately seen as ‘complex’ systems consisting of hundreds of interdependent parts, potentially thousands of networked actors, and no central point that orchestrates all these dynamic inter-relations with and fluid context.

The complexity results from the inter-relationship, inter-action and inter-connectivity of elements within a system and between the system and its environment over time. ‘Complex’ systems are dynamic: meaning they continuously adapt in and evolve with a changing environment. This fractal nature creates an emergent quality with high degrees of uncertainty that is a very different risk-management challenge from that of a ‘complicated’ system.

Designs, plans, strategies and top-notch managers are insufficient to getting these large, dynamic complex systems to function in predefined ways. Conflicts and gaps arise near randomly, as do modifications in design and action because of the interplay of independent and interdependent relationships that make up the web-like system.

Viewed from this perspective, defence in depth can be enhanced through the use of a screening process that looks at how the entire ‘complex’ system is responding to shifting conditions, handling conflicting demands, and learning. System mapping is a proven methodology for systematically identifying relevant parties; the relationships between the parties; the needs, goals and expectations shaping approaches by each of the parties, and the reinforcing cycles that shape dynamics across an entire system. It allows systematic assessment of the safety implications of various relationship patterns and thereby supports targeted improvement. Specifically, where interactive cycles are examined and found to be ‘virtuous’ i.e., they support the ultimate goal of safety conscious decisions and actions, they can be intentionally maintained and even reinforced if needed. In contrast, when ‘vicious’ cycles are identified, i.e., cycles that undermine the information flows, cooperation, and conservative decision-making that are the essence of safety consciousness, strategic interventions can be undertaken to reshape the interactive patterns so potential challenges to safety are mitigated.

In this way, senior and middle managers can proactively review their organization’s capacity to anticipate and mitigate risks, and take targeted actions to strengthen their culture for safety. In addition, by drawing focused attention to how these factors interact with physical barriers, it is possible to highlight potential contributions to mechanisms that can challenge safety functions at one or several levels of defence.

2.1. Organizational resilience

The defence in depth framework is a resilience model consisting of five levels as depicted in Fig 5 below. Each level is intended to control risks and minimize the consequence of failures at the preceding level. Each level, from 1 through 5, represents a reduction in the overall level of predictability of the situation. When human and organizational factors are screened as one aspect, or at discrete levels of defence within an organization, risk is only partially understood. *A systemic perspective enhances application of the defence in depth concept by screening interactions multi-directionally, and across many organizational boundaries.*

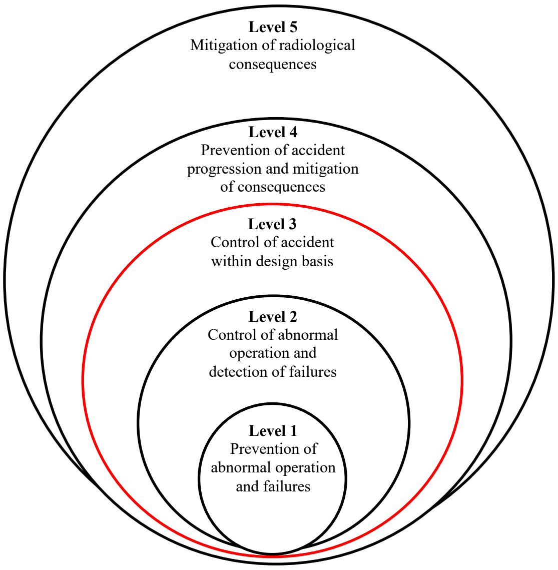

Level 5
Mitigation of radiological consequences
Level 4
Prevention of accident progression and mitigation of consequences
Level 3
Control of accident within design basis
Level 2
Control of abnormal operation and detection of failures
Level 1
Prevention of abnormal operation and failures

FIG. 5. Defence in depth framework.

Let us consider the example of the dramatic shift that happens between Levels 3 and 4 in terms of the demands placed on the organization's members. Up to and including Level 3, organizational members are still working within the framework of familiar working relationships, work methods, and tools. The overall level of trust in the predictability of the situation remains relatively high. This sense of stability supports prevailing levels of human performance. However, as an accident progresses and familiar controls and supports fall away, uncertainty grows, and the members of the organization and the broader emergency response system need to demonstrate progressively higher degrees of situational learning, logistical coordination, and mindful (safety conscious) inventiveness. When the situation reaches levels 4 and 5 reliance shifts almost entirely from known and reliable systems to the capacity of the human beings to function effectively individually and collectively in spite of unknowns, risks and confusion.

From this example, two demands for strengthening nuclear safety become clearer:

First, the need for resiliency born of relationships that are characterized by openness, trust, communication, and cooperation grows dramatically as severe accident management structures and practices are enacted.

From a traditional defence in depth perspective, human and organizational factors are often viewed as a potential source of undesirable variability and risk to nuclear safety. However, when viewed from a systemic perspective, the human capacity for situational learning and adaptive response can also been understood as a potential source of strength depending on the safety culture of the system. During peace time, behavioural norms such as adherence to standard operating practices and procedures serve to minimize unintended outcomes. However, during upset and accident conditions, the capacity to maintain focus on safety while problem solving and identifying alternative (novel) courses of action, is the unique strength of human beings.

This form of organizational resilience is a product of leadership practices that cultivate shared space and strengthen an organization's capacity to prioritize safety under all circumstances. Shared space is about more than simply sharing facts or participating in processes. It refers to a quality of relatedness between individuals and groups that support mindfulness, engagement and wellbeing. It is characterized by:

- Active trust-building
- Decreased power dynamics
- Mutual respect
- Openness – free flow in sharing of thoughts and ideas
- Interest in learning from each other and curiosity about differences in perspectives
- Willingness to express views related to inner thoughts and feelings that are not inhibited by fear of recrimination or exclusion
- Dialogue instead of discussion and argumentation.

Shared space cannot be created in the instant. It must be cultivated at every stage of a plant's life (and across the multi-organization complex system of which it is a part), as an integral aspect of the overall culture for safety of the nuclear power programme.

By using system mapping, leaders can begin to explore and anticipate system dynamics, including the quality of shared space, at the group and organizational level, and take steps to address 'vicious' cycles that threaten to undermine needed organizational resilience.

Second, the overall culture for safety and ultimate safety outcomes of a national nuclear programme are strongly influenced by system-wide dynamics that can only be systematically assessed and improved by a defence in depth screening process that involves multiple stakeholders.

Fig. 6. below depicts a partial high-level map of the parties involved in a nuclear power programme. Viewed in this way, the large number of relationships within the system that have an influence on safety decisions becomes readily apparent.

The nature of the relationships established within and between organizations influences not only how effectively the system shares information, learns and improves in peace time, but also how well it is likely to collaborate as a situation degrades. Lines of authority change, time pressure and confusion grows, and the number of parties involved in the response expands as a situation progresses from Level 1 through 5.

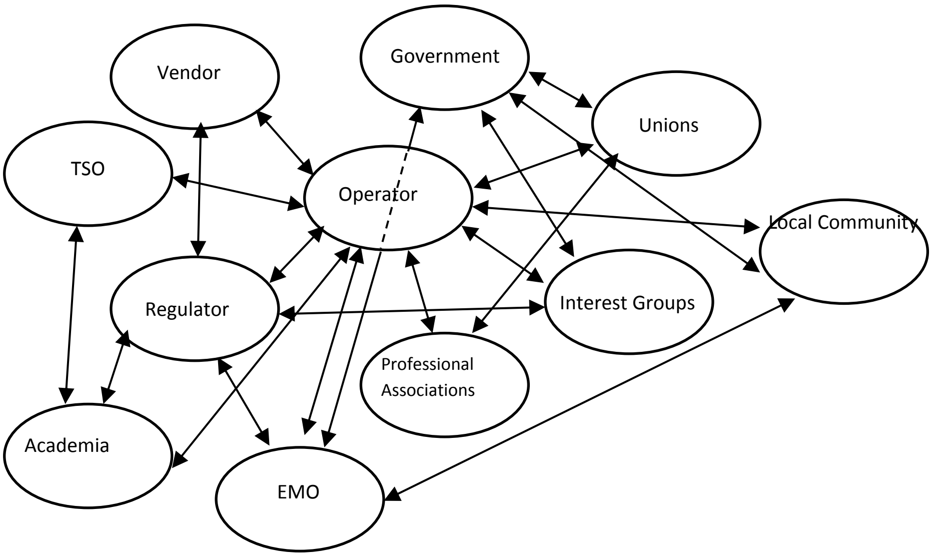


FIG. 6. High-level systemic view of a nuclear power programme.

By systematically exploring the primary drivers to the multitude of interactions between the many parties, it is possible for leaders from across the system to anticipate areas of strengths and latent challenges. If carried out with a blame-free focus, potentially ‘vicious’ cycles can be identified, brought into broader awareness, and specific actions taken to address the human and organizational factors that may otherwise inadvertently undermine defence in depth at a system-wide level.

3. CONCLUSIONS

Defence in depth is an essential strategy to ensure nuclear safety for both existing and new builds. The use of objective trees for screening the comprehensiveness of defence in depth provides a powerful tool for understanding links between technological and organizational provisions for ensuring safety of nuclear power plants. Defence in depth should not be oversimplified by reducing it to the capacity of barriers to protect against releases of radioactive substances. The large uncertainties associated with predicting human behaviour, alongside their sensitivity to organizational factors and societal influences, requires special attention to be given to 'soft' logic trees within the defence in depth framework and screening process. Defence in depth can be further strengthened by understanding nuclear power programmes as 'complex' systems, and by taking into account all the components of the system, from operators, through middle level managers, NPP managers, up to corporate, governmental and even international levels when assessing risk. Cross-correlation and mutual interdependence between all components of this complex system's defence in depth needs to be given considerable attention in the future.

The use of system mapping for exploring the non-linear interactions between individual, technical and organizational factors can enhance defence in depth by providing a method for screening the multiplicity of dynamics within and between organizations that drive the overall culture for safety within a national nuclear programme.

REFERENCES

[1] IAEA, Defence in Depth in Nuclear Safety, INSAG-10, International Nuclear Safety Advisory Group, Vienna (1996)

[2] IAEA, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1, INSAG-12, Vienna (1999)

[3] IAEA, Fundamental Safety Principles, Safety Standards Series No. SF-1, Vienna (2006)

[4] IAEA, Safety Assessment for facilities and Activities, Safety Standards Series, GSR Part 4, Vienna (2008)

[5] IAEA, Safety of Nuclear Power Plants: Design, Safety Standards Series, SSR-2/1 Rev. 1, Vienna (2015)

[6] IAEA International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety held in Vienna, 21-24 October 2013

[7] IAEA, Assessment of defence in depth for nuclear power plants, Safety Report Series No. 46, Vienna (2005)

[8] IAEA Report on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, International Experts Meeting, 21-24 May 2013, Vienna, Austria

OPERATIONAL HUMAN AND ORGANISATIONAL FACTORS PRACTICES IN THE AREVA GROUP TO FACE NEW CHALLENGES

Internal and external new challenges: Practices and open questions

T. COYE DE BRUNELIS
AREVA
Paris, France
Email: thierry.coye-de-brunelis@areva.com

E. BACHELLERIE
AREVA
Paris, France
Email: eric.bachellerie@areva.com

J.-F. SIDANER
Paris, France
Email: jean-francois.sidaner@areva.com

Abstract

The first generation of operators started up the facilities and optimized their operation. This first phase gave them a better understanding of operations and related limits, particularly through testing and start-up operations and the responses that had to be found for all of the technical issues that arose. All of these interactions offered opportunities to make the safety challenges of processes and facilities tangible and directly perceptible. The young operators of those bygone years are now the ones who are “in the know” in the organizations, the ones with unique technical know-how and a multi-layered perception of the risks involved.

Those first generations of operators, with their unique operational knowledge and know-how, are gradually leaving the industrial world. Replacing those skills creates a new set of challenges.

The first part of the article presents specific training measures, qualification programs and organizations to ensure that all of these developments are under proper control.

Concomitantly, the French nuclear safety authority also benefitted from these facility start-ups to increase its skills by sharing in the learning process concerning the facilities’ operational realities and in the construction of a safety configuration program, and by gaining a concrete perception of risk. This fostered the mutual trust that is vital and integral to facility safety.

The setting for this work is characterized by a proliferation of regulatory requirements, even though the facilities themselves have integrated in their process some benefits from continuous safety improvement. Whereas previously safety resulted from a weighted balance between managed safety and regulated safety, we are seeing regulated safety assume an increasingly dominant role. The sharp upward trend of regulatory requirements in France makes one wonder about their real impacts in terms of continuous safety improvement.

The second part of the article questions (a) the efficiency of the overall process of safety governance and (b) the different biases and pitfalls that safety faces. A link with generational renewal is made trying to explain a part of the causality.

1. INTRODUCTION

The construction and operation of the first fuel cycle facilities in France began in the 1960s and continued until the 1990s. Their design and operation have involved several generations and age groups of engineers and operators up to the present.

The first generation of operators started up the facilities and optimized their operation. This first phase gave them a better understanding of operations and related limits, particularly through testing and start-up operations and the responses that had to be found for all of the technical issues that arose. All of these interactions offered opportunities to make the safety challenges of processes and facilities tangible and directly perceptible. The young operators of those bygone years are now the ones who are “in the know” in the organizations, the ones with unique technical know-how and a multi-layered perception of the risks involved.

Those first generations of operators, with their unique operational knowledge and know-how, are gradually leaving the industrial world. Replacing those skills creates a new set of challenges. Today, AREVA must manage the departure of skilled personnel with unique knowledge. It is therefore vital to ensure the capitalization and transmission of those skills and knowledge to new generations. Transmission and appropriation are not a simple matter, for the distinctive features of new generations must be factored into the equation: their value systems, their risk perception and the image they have of facility reliability.

AREVA has created specific training measures, qualification programs and organizations to ensure that all of these developments are under proper control.

From another hand and concomitantly, the French nuclear safety authority also benefitted from these facility start-ups to increase its skills by sharing in the learning process concerning the facilities’ operational realities and in the construction of a safety configuration program, and by gaining a concrete perception of risk. This fostered the mutual trust that is vital and integral to facility safety. As for AREVA it could be hypothesized that the French regulators should face the same challenges regarding generational renewal. Some day-to-day facts support our hypothesis.

Indeed facilities operation is characterized by a proliferation of regulatory requirements, even though the facilities themselves have integrated in their process some benefits from continuous safety improvement. Whereas previously safety resulted from a weighted balance between managed safety[3] (defined based on best practices from experience and recognized by all) and regulated safety[4] (defined based on regulatory requirements) [1], we are seeing regulated safety assume an increasingly dominant role. The sharp upward trend of regulatory requirements in France makes one wonder about their real impacts in terms of continuous safety improvement. In fact, applying this volume of requirements to operations is a heavy burden for operators. The appropriation of each of these new measures is an issue, and finding and getting acceptance of responses proportionate to the stakes involved in the operational application of all these requirements remains a challenge.

Added to this change of generation (both for nuclear operators and safety authorities) are constraints such as the acceptability of risk-related activities to society, requiring transparency and the need for ongoing nuclear operations to be carried out in an acceptable economic framework, which in turn requires assurance of an appropriate level of industrial performance while ensuring that safety levels remain in line with prescribed standards.

We will first present the specific training measures, qualification programs and organizations set up by AREVA to ensure that all of these developments are under proper control.

We will then attempt to explain the link that may exist between generational change and the greater proceduralization of safety, which paradoxically can sometimes occur to the detriment of safety. These explanations, based on daily observations, are supported by the theory of social regulation of J.-D. Reynaud [2] and the work of De Terssac [3]. The proposed line of questioning is forward-looking in its examination of how safety governance functions, both at the meta-organizational level and at the operator level. Its prime purpose is to open discussion on the status and performance of safety governance. Following Bourrier and Bieder [4] and Rolina [5], we will try to reexamine the proceduralization of safety by questioning the underlying causes, which sends us back to the process itself and to those involved in it.

[3] Managed safety: avoid all foreseeable deficiencies through formalism, rules, automatic controls, protective measures and equipment, training in “safe behaviors”, and ensure regulatory compliance management [1].

[4] Regulated safety: ability of the organization to anticipate, perceive and respond to unforeseen deficiencies. It relies on human expertise, quality initiatives, the functioning of collectives and organizations, and on management that is attentive to real-life situations and that promotes interaction among different types of knowledge useful to safety [1].

2. TOOLS DEPLOYED BY AREVA TO MEET THE CHALLENGES RAISED BY GENERATIONAL RENEWAL

2.1. Context and issues

As indicated in the introduction, several generations of operators have contributed to the creation, development and operation of the French nuclear industry. Through their interaction with processes and facilities and the development of operative procedures, some of which are intimately tied to safety, operating personnel have had the opportunity to develop highly specific and unique knowledge and know-how.

Thus, based on prerequisite, formal, declared safety (one also speaks of "regulated safety" [1]), the operators have built what makes for effective safety (also called "managed safety" [1]), a set of rules of use based on experience and know-how. This set of rules is built in particular during qualification and start-up tests and in operational situations. It transforms formal/prescribed safety into a shared obligation which gives birth to individual commitment to a program to enhance safety, to the appropriation of formal rules, to the understanding of incidents and events (without looking for the person responsible), and to the pooling of knowledge concerning risk [3].

This illustrates that the management of jobs and skills in safety and radiation protection (for the protection of protected interests and the management of technological risk) for key operational positions is an essential component of safety management. These key positions are those of the operational chain of command first of all, but also those of the independent safety network.

Skills self-assessment, awareness raising and training programs and actions have thus been implemented by AREVA with the goal of strengthening knowledge.

2.2 The Safety Excellence Program

The Safety Excellence Program was set up in early 2012 in response to a request from the Chairman of the Executive Board of AREVA to "work on a comprehensive inventory, by operational level, of the skills of managers involved in safety-health-security-environment (SHSE[5]) implementation in the facilities."

Today, this program covers all of the site directors, production directors, duty officers, facility managers, project managers for the owner-operator and for the group's engineering entities, as well as the SHSE managers of the sites. This population represents some 500 employees, mainly in France.

For each population, the program consists of four parts:

— Identification of the jobs and employees concerned;
— Definition of requirements at the start and mid-point of the job;

[5] SHSE: Safety Health Security Environment

- A self-assessment or assessment campaign based on a single areva safety configuration program for shse skills in key operating positions;
- Implementation of dedicated shse training and awareness-raising programs for populations covered by the plan based on the results of self-assessments.

In 2014, SHSE self-assessment campaigns were carried out by duty officers (126 employees) and SHSE managers (100 employees). Following an analysis of the results, an action plan was set up to:

- Strengthen their awareness of nuclear safety issues;
- Provide suitable training on hazardous materials transportation, nuclear materials control, human factors and "on-the-floor practices".

For site directors (MSSE program) and facility managers (SAFI program), a special program of support based on a body of mandatory training courses was set up to assist them in their duties. At the end of 2015, more than 70% of the site directors in France and abroad had taken the MSSE program and close to 85% of the facility managers in France had completed the SAFI program.

Based on the positive feedback on the training and overall program, AREVA decided to continue it and include it in a triennial initiative. In 2016, in addition to carrying out five to six training sessions, including a pilot session for project managers, the priority will be to define a program to support project manager duties and to conduct a second self-assessment/assessment campaign among site directors, including line management members of the Business Units' management committees.

2.3. Other training to strengthen safety skills

In addition to mandatory SHSE training and awareness programs on nuclear and occupational safety risks and culture, training programs specific to nuclear safety, human and organizational factors (HOF) and emergency management are in place for target populations:

- Nuclear safety engineers, with a General Nuclear Safety Engineering module (General Inspectorate – Nuclear Safety Department) (five days);
- Local managers, with a module on HOF tools and work reliability (two days);
- Persons involved in harvesting operating experience, with a module on event analysis from the HOF angle (two days);
- Members of the Management Committees, with an awareness module on emergency management and organization (one day).

In 2015, nearly 300 employees completed these training and awareness programs.

In addition, to meet the requirements of the INB Order of February 7, 2012 on the supervision of subcontractors performing protection-related activities, an action plan was deployed to identify and support some 500 supervisors in their new duties.

The professional training of these key players is based on raising awareness of the requirements of the INB Order as concerns the supervision of subcontracted activities connected with protected interests and safety culture. It also includes a training program on supervision tools, designed by the operators with support from corporate departments, which is offered by the group's training entity, TRIHOM. This one-day program is based on case studies and includes a test of knowledge at the end.

In 2014, more than 7,000 hours of training were dispensed to 540 AREVA employees identified for assignments as supervisors. The program was adapted to be extended to supervisors in charge of engineering and operating entities that provide services and work to other operators.

3. FUTURE CHALLENGES FOR SAFETY AND SAFETY GOVERNANCE

3.1. Context and issues

In his 2014 annual report, the Inspector General of AREVA stated that "The number of regulatory requirements has seen unparalleled growth since the beginning of 2012. This situation is accompanied by real challenges associated with their proper operational implementation and their appropriation by the operators.

In these times of new long-term requirements and changing safety configuration programs, the quality of the relationship with the nuclear safety authority ASN is more than ever a decisive factor. In the forest of complex requirements, which could demotivate those who do the work and cause them to lose their way, it is important to keep our sights trained on the primary objective of improving safety. The difficulties encountered in the operational implementation of the 2005 order on pressurized nuclear equipment (ESPN) alert us to the real challenges of this type of regulatory change. All of the lessons must therefore be drawn from the misunderstandings that arose from implementation of this order so that 1) proper operational measures are ultimately defined in this regard and 2) procedures for implementing any new requirements remain the first concern of their authors. It is on the floor that safety is won first. To be met, a requirement must first be well understood and correspond to a clearly identified and accepted issue." [6].

This excerpt is quoted to call attention to a chronic situation: the growth of the prescriptive safety configuration program, which increasingly neglects the objectives to be met in favor of focusing on the details of processes. At each stage, the burden of proof and compliance with the requirement must be presented. As a result, operators are confronted each day with the proceduralization of safety governance.

How can one explain this reinforced proceduralization and its corollary, the growing difficulties for operators constrained to apply an evolving safety configuration program? Our hypothesis is that part of the explanation lies in generational renewal, not only at AREVA, but at other actors in safety governance.

3.2. Generational renewal: a lead for explaining the growth in regulations and in the difficulties of their implementation

3.2.1. Challenges for new generations

In terms of safety governance, the French nuclear safety authority was built at the same time as the design and construction of facilities by French nuclear actors. Thus, the safety authority's corps of inspectors in charge of the fuel cycle was also forged, built and grew in skills through contact with the first operators. From its interactions with them, it drew shared knowledge of the facilities and an accurate appreciation of the risks. The interactions between industrial companies and safety authorities (ASN, IRSN) were propitious to the movement of personal skills and knowledge which benefitted the growth of knowledge and risk perception by all actors. Incidentally, the first generations of operators contributed to the training and building of skills of the safety authority.

Relations between operations and the authority have changed considerably due to generational features, in particular the weakening of technical knowledge of operations and of the relationship to risk. The weakening of technical knowledge contributed to the weakening of technical authority. Thus, a migration of technical authority towards disciplinary authority based solely on compliance with the rule is observed at the safety authority. How to narrow this distance from risk and ensure its management in this situation? At first glance, prescribing rules and regulatory requirements appears to be an efficient way to encapsulate risk in a set of rules (on the model of defence in depth, comparable to a stack of barriers) whose superposition is postulated to cover every aspect and control all facets of risk in the end. This approach seems all the more efficient in that for each regulatory requirement not followed there is a sanction, such as a formal demand or even a daily penalty. The power to sanction is substituting for technical authority capable of an accurate assessment that draws on knowledge and is proportionate to the issues. Very quickly, there follows the logic that the more the safety requirements, the safer the operation of the facilities. Does this logic stand up to scrutiny? It may seem satisfactory intellectually, for it gives one the feeling that the risk is controlled and safety is ensured. But the operational application of a repository of requirements shows that things are not so simple and that, by itself, formulating rules does not guarantee risk management.

3.2.2. Legitimacy of rules and their construction

De Terssac[6] [3] notes that the work of organizing safety is paradoxical in that it associates trust in the tranquility of regulated safety with the uncertainty of an action adjusted to a situation and a context.

Philippe Bernoux [2] observes that in the theory of social regulation of J.-D. Reynaud, *the expression of the rule does not determine its efficiency*, “for it is only valid by the consent of the actors and the ability of institutions to have it enforced. The rule is a collective reality that *systems and institutions cannot by themselves bring into existence*, for commitment by the actors is necessary.” Yet as De Terssac (*Ibid*.) underscores, the rule as requirement on which action is based “is activated only if the subject decides to mobilize it.” Thus, again per [3], “sociology (Friedmann, Simon, Crozier, Touraine, Reynaud, Friedberg, Thoenig, et al.) has shown that rules do not apply themselves and are mobilized only by the decision of an individual to act (or to decipher the context).”

The excerpt from the annual report of AREVA’s Inspector General [6] accurately shows the difficulty of operating personnel to commit to a system of rules whose legitimacy may be questioned. This loss of legitimacy is implicit in the difficulty of new generations to appropriate operational realities, related constraints and an accurate perception of risk. Because of this distance from reality, the system of rules loses its impact. Moreover, it can cause a loss of prioritization of preventive actions to be taken because experience and culture are the most robust supports for instituting a hierarchy of safety issues. Today, an increasingly inflexible system of rules can lead to the feeling that each one has equal weight, which is of course not the case when it comes to major risks. By way of example, environmental protection could be put on the same level in some persons’ minds as criticality control. The requirements are put on the same level, although they are not.

3.3. Appropriation of the rule as a process for its implementation

Once again following the theory of social regulation [2], the fabrication of a rule is not completed by the expression that makes it visible; it continues through its implementation. This point is of the greatest importance. To understand its reach, it is necessary to consider safety governance as a whole (as a meta-process for

[6] De Terssac [3] calls up the theory of social regulation of J.-D. Reynaud and applies it to security to demonstrate how usage rules are built and to explain the transition from regulated safety to effective security. His work of analysis focuses on the rule as object of regulation and mobilizes safety as the framework of application. Indeed, it appears methodologically acceptable to us to transpose his analysis to the framework of application of safety. Moreover, while there is a difference between security and safety in French, this difference is less pronounced in English, where the word “safety” covers both French words “securité” and “sûreté”.

generating rules), a whole consisting of (distinct) sub-processes for generating rules, both from the side of the safety authorities (ASN, DSND, etc.) and from that of the nuclear operators.

A rule produced by a safety authority is, in general, retranscribed and transposed in the safety configuration program of the operator, which must apply the prescribed rules. This process, internal to the operator, is akin to a process of "digestion". Each rule is analyzed, dissected into as many units of meaning as necessary, and its import measured, such as the impacts on operating procedures and activities. This digestive process enables the operator to appropriate the rule.

For operators such as AREVA, this appropriation process is generally broken down into two levels. The first level of analysis takes place in the corporate departments in charge of "translating" rules issued by the authorities for the operators in a set of documentation (guidelines, directives, instructions, etc.). The second level of analysis is then deployed at the level of each site, entity or operator which, in turn, appropriates the set of documentation issued by the corporate departments in response to the regulations in order to translate it into its own safety configuration program. The third and last stage of the AREVA group's internal appropriation process is provided by the operators themselves during operations, in the operating actions in which these rules are implemented.

Thus, a rule is the fruit of several continuous and contiguous processes which are institutional first and then operational, and which may be summarized as follows:

(a) Development of the rule by the authorities
(b) Transcription of the rule
    (i) At the AREVA group corporate level
    (ii) Then at the central site / entity / operating level
(c) Implementation by the operators

De Terssac (*Ibid.*) adds that "during its construction, the rule solidifies and becomes institutionalized in an expression which has a life of its own, and during its implementation it is transformed and enriched by its uses... It is not that there are rules on one side and action on the other, but a process of adjustments between declared rules on the one hand and their implementation in real-life conditions on the other." In the end, the conception of a rule should not be thought about from a single viewpoint alone – that of the regulator – but from multiple viewpoints: independent safety network, regulator, operating company, operators at the facility. Its development requires the integration of all processes (and their constraints), going from the safety authorities' internal processes to the processes by which operators in charge of its application in the facilities appropriate it.

Various places exist for exchanges and communication between authorities and operators for the development of rules and safety configuration programs. Points for meeting and discussion are set up to facilitate convergence towards formulations of rules that are as satisfactory as possible to the parties involved. This supposes, first of all, that the words used have the same meaning for the regulator and the operators, that everyone understands the same things, the same obligations, the same evidence… Moreover, this understanding must be valid and ensured for all generations to come. Yet several situations have supported the observation that generational renewal leads to understandings that may be different for new generations, in particular due to appropriation that is disconnected from the context and initial exchanges that led to the consensus reached on the system of rules.

In certain respects, these processes of exchange and communication tend to close the decision-making loop and to ensure that everyone's viewpoint has been put forward. The operators (often through the corporate departments) are asked to give opinions as part of an iterative process. Through this loop, the operators translate or try to translate the operability of the rule. But this involvement sometimes does not enable the authorities to integrate it, contributing to the production of safety configuration programs that are difficult if not impossible to apply.

In operation, the safety rules are taken in a field of constraints that are much more complex that the safety field alone. In operations, production is always the fruit of a balance struck among all the fields of constraints. Thus, "the effectiveness of a safety rule is not summed up in its formal expression or its inclusion in systems, even though without this expression one cannot speak of safety." [3]

The first two process (*Cf. supra*) remain chiefly of an administrative order in the sense that they only generate rules without any of the actors having to apply to rule in practice, operationally.

Only the third operational mechanism deals with it, makes it effective. De Terssac identifies three features to make a rule effective by operating personnel on the floor.

(1) The decision must be made to mobilize it, to refer to it before a third party and to show that it can be used in a real-life situation. Effectiveness is the result of its existence as a mobilizable system. Even if a rule were not to be mobilizable in the situation observed, the decision to mobilize it shows that it exists, that it is applicable and that *it comes to life only through the use made of it*.

(2) Effectiveness is having the possibility of making use of it to act or to direct the action… The rule opens up an area for consideration to decide whether to apply it or not; *it is not an operating procedure whose execution would guarantee the functioning of safety*; rather, it serves to correctly proportion the action.

(3) Thirdly, effectiveness is its descriptive nature: it serves as a marker to qualify a reality. The use of a formal rule gives it meaning due to the interpretation of the text debated in the particular context of that reality and due to the choices it makes possible between contradictory constraints (which may be safety constraints that contradict each other).

Faced with the complexity of this appropriation process and the constraints that must be integrated, the question arises: how to know, in advance of the development of a rule, how that complexity and those constraints are in fact taken into account by the regulator? This question is all the more justified in that the appropriation of a rule is governed, in the end, by the conditions of its acceptance in the facilities.

3.4. Conditions of acceptance of the rule

De Terssac also sheds light on the conditions for the acceptance and implementation of rules. For him, "the fact that the rules are co-constructed, both at the knowledge level and at the authority level, gives them a certain consistency, a density and thickness: the construction of the declared rule is integral to negotiated safety, giving it legitimacy not only in terms of the rule itself, but also in the work of supervision that accompanies its constitution and implementation." The challenge in its development is in fact its co-construction, which enables negotiation as part of a "fair compromise" process to be attained where the interests of all parties are taken into account. The attainment of a fair compromise is also a lever for creating trust between actors and involving them in the operational transcription. The most salient point put forward by De Terssac is the *mobilization of knowledge and authority*. This relationship lights the way for the balance that must be found in the comprehensive governance of safety. Naturally, knowledge is more the domain of the nuclear operator than the legislator, whereas authority is more the domain of the legislator than the operator.

These keys for understanding call for a just balance to be found between consideration of operating constraints and the position of the safety authority. An imbalance between the two leads to the deterioration of trust and of the ultimate acceptance by the operating personnel, to difficulties in transcribing the rule and to difficulties in mobilizing operating personnel for application of the rule. The more debatable the technical value of the rule, the greater these difficulties. In fact, among the conditions for acceptance of the rule, justification of the need for it plays an important role. Acceptance will be all the greater if justification of the need is built on operating experience, on compliance with a wider obligation and on an explanation of how it will contribute to improving safety or limiting risk.

Without it, this rule may be perceived as dogmatic and compulsory.

3.5. Dogmatism in safety: another trap for new generations

3.5.1. Expression of the rule

A safety dogma identified by Amalberti [7] posits that "the expression of the rule is the condition of safety and one can trust this regulated safety from both a standards viewpoint and a cognitive viewpoint." That dogma could be qualified as "safety expression dogma". De Terssac [3] reformulates the dogma by positing that "*confidence in standards postulates that the simple application of the rule guarantees safety, and it precludes any gap between the rule and the action*." This is very common dogma for the standards aspect and is present trans-organizationally. It is not uncommon to see corrective actions like "create a procedure to establish guidelines for operator activity" in event reports. This point corroborates the position of Bourrier and Bieder (*Ibid.*): "Although it is well documented that procedures do not guarantee in themselves a safe performance, reinforcing proceduralization remains a widely spread reflex action when safety is perceived to be insufficient."

While this dogma appears to exist at the lowest level of the safety organization (i.e. at the level of facility operators), it also appears to be very much alive in the highest strata of safety governance. It underlies the logic we mentioned earlier in this article: the higher the number of safety requirements, the safer the operations. Underlying this logic is the fact that the operators cannot escape from the application of the rules decreed by the authorities. So the simple fact of expressing a rule appears to be enough for its implementation and efficiency, since the operators must apply it once it has been expressed.

In view of the foregoing, this dogma appears to be one of the explanations for the growth of regulatory requirements, for it justifies the logic of safety improvement by increasing the number of rules and regulations. At the same time, the number of rules fills the deficit of safety-related knowledge and learning resulting from generational renewal. The greater the number of safety rules, it seems, the lower the chances of safety gaps. Nevertheless, the more technical knowledge decreases, the more the distance to risk increases. Too large a distance to risk leads to reliance on dogma.

The existence of this dogma reinforces the integration of safety governance in a vicious circle of over-specification or over-legislation in the hopes of an overall improvement in safety.

3.5.2. Masking mechanisms at work in the dogma

This dogma also helps mask the complex processes of rule development and operational deployment mentioned earlier. It unconsciously avoids having to think about the complexity of safety governance with all the finesse this requires while at the same time remaining involved in the safety development process.

This is echoed in the words of Bourrier and Bieder [4] in particular. They note that, indeed, "the scope of public oversight, enacted by regulatory bodies, grew together with these successive proceduralization areas. Regulatory agencies progressively extended their fields of intervention along these lines, but oftentimes lacking operational knowledge, experience, manpower and resources. Hence, promoting procedures and processes offered a feasible option to stay on board, probably at the expense of losing sight of a more in-depth understanding of the conditions under which safety was concretely achieved and socially produced.”

Another effect resulting from this dogma is the deformation or even the disappearance of the human dimension of safety, and yet it is preponderant. By postulating that the expression of the safety rule is necessary and sufficient to the operational implementation of safety, human and organizational factors are disposed of *ipso facto*. The understanding of human behavior and its involvement in the development of the rule as conveyed by the dogma is mistaken. The bases for the construction of an applicable rule (revolving around the interests of each of the actors, underpinned by the fact that each party knows the concessions made by everyone, the adjustments necessary to satisfy each field of constraints, understanding by the parties of all of the issues, trust between individuals and between organizations, construction of the legitimacy of the rule, etc.) are clearly the factors with a direct impact on individuals, on their activities and in the end on safety. One of the fundamental aspects is the need for the persons who have to apply a rule to understand its usefulness and proportionality to the circumstances. Yet all too often the rules are perceived as additional constraints to the detriment of a line of defense against risk. If a hazard has potential in the work situation, the rule to protect against it will be applied without deviation (e.g. the rules applied by flight deck personnel on an aircraft carrier); the awareness of risk is acquired in the field. Likewise, when a rule multiplies additional measures in relation to a hazard that has already been perceived and controlled without those additions, the rule loses its effectiveness and legitimacy. Individuals carry out their duties and apply the rules (no matter what they are) only when they are convinced that they are well-founded. The rule must therefore have the ability to engage individuals in action, and explanation of its utility is certainly the most effective way to secure support.

Once again, the dogma of safety expression, by the fact that it erases these mechanisms for the construction and appropriation of the rule and offers a mistaken and hollow view (model) of human behavior, carries within it the seed of weakness for development of the rule, for its rejection by the recipient, and for the creation of important roadblocks to its implementation.

The enduring consequences of this dogma with the operators appear to be the same with the safety authorities, for whom the rule sometimes seems to remove a responsibility that could come back to them in the event of an accident. These consequences at the level of the authorities most certainly have more impact, for their weight in the rule development process is greater than that of the operators.

3.5.3. Means and resources: a partial or even ineffectual response

The mobilization of this safety dogma and the gaps in the related representations also avoid having to think about the problem of resources (in particular human) needed to develop rules and to make them operational, and enabling them to be applied effectively in the facilities. Moreover, this avoidance is reinforced by the fact that the operators have an obligation to achieve results versus a best-efforts obligation, it being the responsibility of the operators to put in place the means of achievement. This dogma seems to act as permission to free oneself from the precautions necessary to the facilitation of rule production and to their ultimate quality.

Regarding all of the mechanisms analyzed (generational renewal, comprehensive governance process, existence of dogmas, unparalleled growth of regulations, etc.), the following hypothesis may be formulated: the final cost (financial, in time, human, etc.) of the functioning of safety governance is significantly higher that it should be, yet this does not improve the overall level of safety of the facilities. In fact it could be lower. Some explanatory factors are proposed hereunder.

The operators (corporate departments and sites) must appropriate the system of rules according to the process described above and moreover must manage the additional roadblocks they cause (lack of legitimacy of the rules, etc.). This is the first source of extra costs. In addition, these extra costs, which consist of mobilizing personnel, do not allow the personnel to focus on other aspects of routine safety, which does not contribute to the continuous improvement of safety.

In that situation, and rather instinctively, the actors could be asked to mobilize additional resources in order to deal with the excess costs and the resulting workload. Aside from the fact that the energy market is particularly competitive and leaves industry little room to maneuver, the mobilization of additional personnel does not deal with the problem.

In fact, the growth of regulations coupled with problems of inconsistency between rules automatically increases complexity, both organizationally (human, technical resources, etc.) and cognitively (complexity of safety configuration programs, word complexity, semantic complexity, etc.), raising it to a level that is impossible to grasp. This cognitive complexity in the safety configuration programs is such that it is increasingly difficult for the operators (central departments and sites) to understand them, to transcribe them, to make them applicable and to apply them. Moreover, mobilizing additional resources to analyze and deploy these safety configuration programs (i.e. deal with cognitive complexity) creates the side effect of an increase in the number of actors and interactions, which creates even more complexity to be dealt with. To this should be added the need to recruit personnel, to train them, to raise their skills level, to ensure their level of safety culture... Once again, all these points create additional organizational complexity. The complexity causes by the growth of regulations is polymorphous: it is quantitative (going from 200 rules in 2006 to a projected 1,200 rules by the end of 2016), qualitative (emergence of concepts such as Items Important for Protection, Activities Important for Protection, etc.), and scope-related (expansion of the regulated scope, making rules specific to environmentally regulated facilities applicable to regulated nuclear facilities). And this growth of complexity is not linear: complexity is going critical due to the interactions between the rules themselves and the repercussions of those rules on organizations (recruitment, difficulty understanding the safety standards, etc.).

It therefore does not appear that the development of rules by the governing safety bodies includes all of the above-mentioned repercussions on the actors and on safety itself. And yet they are fundamental components which ultimately contribute to the effectiveness of the system of rules and thus to safety.

3.6. The paradoxes of safety

On the other hand, as De Terssac says, "this dogma of regulated safety makes deviation from the standard the source of the deterioration of regulated safety." The underlying premise is that the rule as formulated effectively contributes to safety. Yet a paradox of safety, observed in operations, resides in the fact that some rules do not further safety, others are contradictory (on this point, see the quotation of De Terssac hereunder)… Intrinsically, they generate an additional complexity and, de facto, potentially contribute to the deterioration of safety. That being the case, how can it continue to be maintained that all rules contribute effectively to safety and that deviation from the rule degrades safety?

Up to now, we have only broached the standards side of the safety expression dogma. Let us now consider the cognitive side. De Terssac indicates that "cognitive confidence in a rule relies on the idea that we know the events that could alter the system." Yet this premise of "exhaustive" knowledge of operating scenarios (normal and incidental) does not allow assertion of the completeness of the rule that could make it effective and applicable in all situations. The rule is developed based on cases, on a necessarily incomplete set of scenarios. As De Terssac says, "the incompleteness of the rule is one of its characteristics," and goes further by asserting that a rule is "necessarily incomplete and contains inconsistencies or contradictions, limits and implicit understanding which make application variable." Thus, behind this cognitive confidence hides an additional trap for safety dogma. Not only is the expression of the rule not the only necessary condition of safety, but the application of the rule does not guarantee safety in its entirety.

In the end, this safety dogma, if taken as it stands and considered true by those in charge of developing the rules, leads to only one safety, which is fragmentary on the one hand (caused by the incomplete nature of the rule) and on the other does not completely guarantee safety.

4. CONCLUSION

Like any industrial company confronted with the implementation of complex systems, the AREVA group faces challenges for the management of its skills and knowledge. The group has set up conventional means to meet them (on-the-job training programs, mentoring system). It is our hypothesis that this endogenous issue also exists within the regulator, partly explaining the proceduralization in which

French safety is increasingly imprisoned. This hypothesis may even be extended to all French regulatory systems.

On the other hand, the safety dogma is a reality inside the AREVA group. Work on safety culture is one of the drivers for defusing this dogma to enhance safety. The safety self-assessments done by AREVA are a step in this direction.

The hypothesis here is that this dogma governs a large share of the rules issued by the system of governance. It is therefore just as necessary for the governing bodies to guard against this as it is for any other operator.

The themes raised in this article demonstrate that all actors – the regulator as much as the nuclear operators – are likely to face their own internal HOF issues (generational renewal, technical skills management, safety culture management, etc.), which contribute directly to safety, safety being the result of a long and complex process integral to each phase in the lifecycle of the facilities, from their design and manufacture to their operation, maintenance, modification, shutdown and dismantling. This process is not limited to simple application of rules to a process by operators at the end of a chain, but must intervene well in advance in the organization of safety governance. Safety improvement is achieved by effective and suitable handling of the internal HOF issues of each actor in safety governance. What means are used today by each of the safety actors to cope with these problems? More generally, and this is the most important point, how does safety governance as a whole incorporate HOF to provide effective, long-lasting solutions for root causes that chronically disrupt its functioning (HOF training, raising of technical skills, raising of risk/safety culture, etc.)?

By reconsidering the proceduralization of safety at work in the organizations of the safety actors, through the filter of the internal issues that AREVA encounters, we wish, following Bourrier and Bider, to stress the need "to stay alert and vigilant in front of constant re-engagement towards more rules and regulations." [4] The first victim of this phenomenon is safety. By means of a questioning attitude, safety culture invites us to ask ourselves about the path safety is taking. Can we still draw real benefits from the direction taken? Effective measures should be taken to get out of the traps described in this article.

To conclude, Bourrier and Bieder are even more adamant about questioning ourselves: "The idea that organizations might kill as surely as bombs and terrorist attacks is no novelty (Adams and Balfour 1998, Clarke 2006, Vaughan 1999) […] The distributed sense-making activities (Weick 1995) that take place daily in order for actors to adequately respond to uncertainties, increased workload, new maintenance activities and new business constraints are largely left unaccounted for (Roe and Schulman 2008, Van Fenema 2005). The real conditions under which safety is produced, maintained, enhanced, enforced, supported or disturbed, ruined, and further destroyed are left in the limbo (Bourrier 1999)… The risk is to lose track of the exact conditions under which safety is daily produced by many different categories of actors, in different parts of the overall system."

How can the entire process of safety management be enhanced and even renewed?

REFERENCES

[1] DANIELLOU, F., SIMARD, M. et BOISSIERES, I. Facteurs humains et organisationnels de la sécurité industrielle : un état de l'art. Numéro 2010-02 des Cahiers de la Sécurité Industrielle, Fondation pour une Culture de Sécurité IndustFrance, Toulouse, France (2010).

[2] BERNOUX, Ph., La théorie de la régulation sociale, compte rendu, Sociologie du travail, 47, (2005) 277-279.

[3] DE TERSSAC, G., De la sécurité affichée à la sécurité effective : l'invention des règles d'usage, Annales des Mines, Gérer et comprendre N°111 (2013) 25 – 35.

[4] BOURRIER, M. and BIEDER, C., "An introduction", Trapping Safety into Rules, How Desirable and Avoidable is Proceduralization of Safety?, Ashgate, Farnham, (2013).

[5] ROLINA G., Sûreté nucléaire et facteurs humains – La fabrique française de l'expertise, Presses des Mines, Collection Economie et Gestion, Paris (2009).

[6] Annual report of the AREVA General Inspector (2014), available on AREVA's website (www.areva.com)

[7] AMALBERTI, R., La conduite des systèmes à risques, PUF, Paris (1996).

THE APPLICATION OF SYSTEMIC SAFETY FOR SMALLER NUCLEAR INSTALLATIONS

J. WARD
Australian Radiation Protection & Nuclear Safety Agency
Sydney, Australia
Email: john.ward@arpansa.gov.au

Abstract

This paper describes the approach taken by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) to develop and promote a systemic approach to safety from its licence holders. It provides the development of the approach, which the ARPANSA calls holistic safety, and how it has been implemented. The paper then proceeds to explain the ARPANSA inspection programme and how inspection findings can be related to the same common contributing causes of accidents on which the holistic approach to safety is founded.

1. INTRODUCTION

This paper describes the approach taken by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) to develop and promote a systemic approach to safety from its licence holders. This approach encourages stakeholders to take into consideration the impact on safety of technological, human and organisational factors. Whereas systemic safety approaches are being advanced and introduced in many countries that use nuclear power, the ARPANSA approach, which it calls ‘Holistic Safety’, is graded to apply to the less hazardous smaller nuclear installations found in Australia.

The development of the ARPANSA holistic safety approach was undertaken by the Regulatory Services Safety Analysis Section comprising of Mr John Ward, Mr Vaz Mottl and Mr Jordan Lock. Ongoing responsibility for the approach is now implemented by the Regulatory Services, Continuous Improvement Section under the leadership of Mr John Ward.

2. BACKGROUND

The role and functions of the ARPANSA CEO are set out in the Australian Radiation Protection and Nuclear Safety Act 1998 (ARPANS Act). One of the more important functions is the regulation of radiation sources, radiation facilities, and nuclear installations of Australian government entities and contractors. This function is performed by the ARPANSA’s Regulatory Services Branch (RSB). The RSB has the fundamental objective to ensure that licensed facilities and sources are operated in an acceptably safe manner at all times. To meet this objective it is a requirement of the ARPANS Act that the applicant satisfy the CEO that they have taken into consideration international best practice (IBP) in nuclear safety and radiation protection in regards to the conduct of the controlled activity.

In 2011 ARPANSA reviewed its approach to human and organisational factors and safety culture as part of the licence assessment process. It was clear that academic work was highlighting that the safe use of technology was underpinned by good human performance, supported by an organisation having a good safety culture and supportive organisational structures. In this context it was clear that IBP included the recognition that safety was a function of a complex socio-technical environment. Much of the guidance being undertaken by IAEA member states in this area concentrated on nuclear power programs rather than smaller facilities such as those present in Australia.

ARPANSA established a small regulatory group to develop a holistic approach to safety; the Safety Analysis Section (SAS). It was recognised early on that 'measurement' of human and organisational factors was not practical in a regulatory compliance sense. Therefore, this group was set the challenge of developing methods to promote the holistic safety approach and influence its use as best practice in the absence of traditional regulatory tools to ensure effective compliance to the principle.

3. DEVELOPMENT OF THE ARPANSA HOLISTIC SAFETY APPROACH

3.1. Basis for approach

There is a variety of sophisticated work being undertaken by nuclear power regulators and operators around the world in the areas of safety culture and systemic safety. The scale and complexity of this work may not be justified for smaller nuclear installations such as those operating within Australia. However, within these large and complex approaches, there were features that could be adapted to the Australian context.

Staff from ARPANSA reviewed research on systemic safety approaches and engaged with the international community through the attendance of meetings and conferences principally organised by the IAEA and NEA. From this a number of observations were made that influenced the approach to the holistic safety project for Australia:

Reviews of accident investigations into major disasters pointed to common contributing causes. A number of studies have been undertaken that highlighted similar findings. ARPANSA focused on research by Prof Richard Taylor from the University of Bristol (UK) Safety Systems Research Centre [1], [2], that identified eight common contributing causes, namely:

- Leadership issues
- Operational attitudes and behaviours
- Business environment

- Competence
- Risk assessment and management
- Oversight and scrutiny
- Organisational learning
- External regulation

Whilst these common contributing causes were seen in accidents internationally, there is often a human tendency for people to distance themselves from a disaster by highlighting differences in the situation or environment that led to the disaster when compared to the local situation, i.e. ‘it couldn’t happen here’. If, however, it can be shown that a local operator has similar vulnerabilities associated with a contributing cause, this becomes a powerful incentive to introduce improvement.

There are a variety of published academic works on safety approaches that may be used to address the contributing causes of disasters. A list of references used in the development of the holistic safety approach for Australia is provided on the ARPANSA website [3].

3.2. The approach

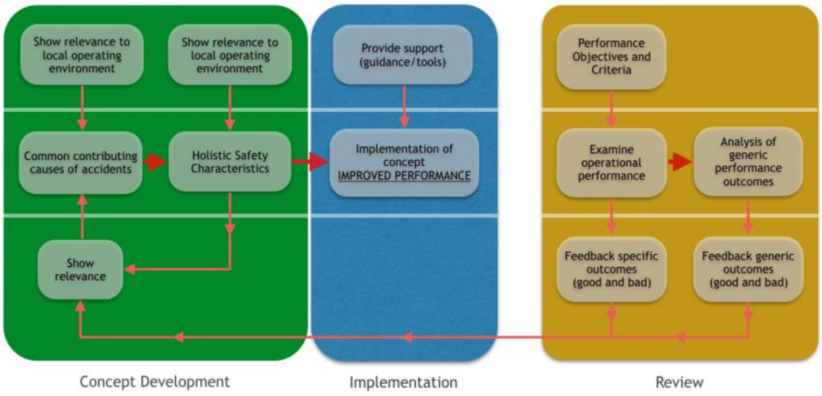

Show relevance to local operating environment
Show relevance to local operating environment
Provide support (guidance/tools)
Performance Objectives and Criteria
Common contributing causes of accidents
Holistic Safety Characteristics
Implementation of concept IMPROVED PERFORMANCE
Examine operational performance
Analysis of generic performance outcomes
Show relevance
Feedback specific outcomes (good and bad)
Feedback generic outcomes (good and bad)
Concept Development
Implementation
Review

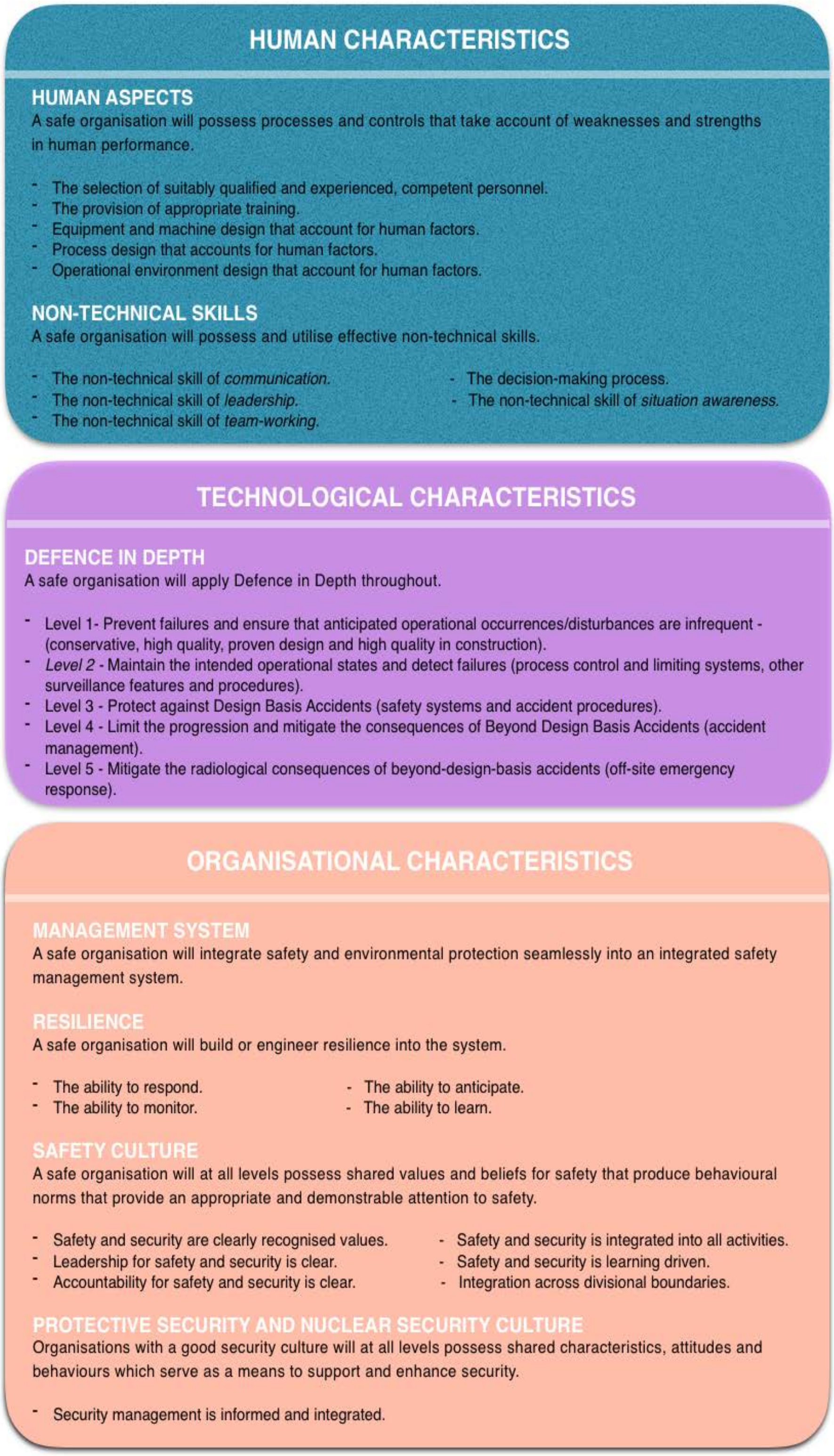
FIG. 1. Strategy for Implementation of Holistic Safety.

Figure 1 presents the strategy used in developing and promoting the holistic safety approach. An initial challenge was to show that the common contributing causes of accidents are relevant in the local environment. Australia has experienced major disasters that have been the subject of extensive investigations. From the reviews of these it was clear that the causes fit closely to the common contributing causes described above. Examples include the 1994 Moura mine disaster, the 1998 Longford gas explosion, the 2003 Waterfall train disaster, and the 2009 Black Saturday bush fires. A number of smaller accidents were also reviewed, sometimes from court proceedings. The outcomes of the findings again correlated well with the common contributing cause model and could be used to demonstrate that the model was good for a range of smaller incidents and accidents as well as major disasters. Importantly, the analysis showed that despite a well-educated workforce and high quality workplace health and safety regimes, Australia could not be distanced from the types of accidents that are seen elsewhere by claiming that Australia is somehow different. This demonstrated local relevance of the contributing cause model.

ARPANSA has selected seven ‘characteristics’ from modern safety approaches and methods to address the common contributing causes of accidents. These are shown in Figure 2. Each characteristic has positive attributes and guidelines that can be found in organisations with good safety performance. One purpose of the holistic characteristics is to encourage operators, and regulatory staff, to look at safety from different angles. There is an overlap between the characteristics but their collective aim is to achieve a comprehensive consideration of safety and to encourage a questioning attitude to adequacy of current practices.

ARPANSA stakeholders represent a wide range of operating risk and consequently a balance needed to be found to provide a useful amount of detail for all of its stakeholders. A decision was taken to encourage a widespread use of the holistic safety approach through a concise (18 page) guide which is supplemented with other support materials where needed. The ARPANSA website is a key feature of this strategy and provides extensive information on the approach, guidance, samples of assessment tools and an extensive list of references used to develop the approach. (See arpansa.gov.au/Regulation/Holistic).

Stakeholder engagement was actively pursued during development of the holistic safety approach through a number of forums and other meetings. All stakeholders also had the opportunity to input the materials developed before its formal launch in January 2012.



HUMAN CHARACTERISTICS

HUMAN ASPECTS

A safe organisation will possess processes and controls that take account of weaknesses and strengths in human performance.

- The selection of suitably qualified and experienced, competent personnel.
- The provision of appropriate training.
- Equipment and machine design that account for human factors.
- Process design that accounts for human factors.
- Operational environment design that account for human factors.

NON-TECHNICAL SKILLS

A safe organisation will possess and utilise effective non-technical skills.

- The non-technical skill of *communication.*
- The non-technical skill of *leadership.*
- The non-technical skill of *team-working.*
- The decision-making process.
- The non-technical skill of *situation awareness.*

TECHNOLOGICAL CHARACTERISTICS

DEFENCE IN DEPTH

A safe organisation will apply Defence in Depth throughout.

- Level 1- Prevent failures and ensure that anticipated operational occurrences/disturbances are infrequent - (conservative, high quality, proven design and high quality in construction).
- *Level 2* - Maintain the intended operational states and detect failures (process control and limiting systems, other surveillance features and procedures).
- Level 3 - Protect against Design Basis Accidents (safety systems and accident procedures).
- Level 4 - Limit the progression and mitigate the consequences of Beyond Design Basis Accidents (accident management).
- Level 5 - Mitigate the radiological consequences of beyond-design-basis accidents (off-site emergency response).

ORGANISATIONAL CHARACTERISTICS

MANAGEMENT SYSTEM

A safe organisation will integrate safety and environmental protection seamlessly into an integrated safety management system.

RESILIENCE

A safe organisation will build or engineer resilience into the system.

- The ability to respond.
- The ability to monitor.
- The ability to anticipate.
- The ability to learn.

SAFETY CULTURE

A safe organisation will at all levels possess shared values and beliefs for safety that produce behavioural norms that provide an appropriate and demonstrable attention to safety.

- Safety and security are clearly recognised values.
- Leadership for safety and security is clear.
- Accountability for safety and security is clear.
- Safety and security is integrated into all activities.
- Safety and security is learning driven.
- Integration across divisional boundaries.

PROTECTIVE SECURITY AND NUCLEAR SECURITY CULTURE

Organisations with a good security culture will at all levels possess shared characteristics, attitudes and behaviours which serve as a means to support and enhance security.

- Security management is informed and integrated.

*FI*G. 2. The ARPANSA holistic safety characteristics.

4. IMPLEMENTATION

4.1. Basis for approach

In January 2012, ARPANSA published a guide providing the characteristics, attributes and positive guidelines that describe what it expects to see in an organisation with a good approach to holistic safety. This was accompanied by a publication providing more detailed questions to allow both regulatory officers and licence holders to better examine operational safety.

Parallel to publication of the guidance a programme of socialising and promoting the concept was undertaken. Stakeholder engagement has been through meetings, information sharing seminars and conferences with its licence holders. A number of talks and presentations have also been given nationally and internationally, mostly through the IAEA.

In the period since publication ARPANSA has published tools based on its guidance which may be adapted by other users to suit individual applications. These tools ask a series of questions that outline an approach which can highlight areas of strength and weakness associated with the holistic safety characteristics. The basic principle of the tools is to allocate a qualitative performance value for each of the characteristics, attributes and, for larger installations, the guidelines. The results of these can then be shown pictorially to provide informed advice on where additional safety resources may be directed. Examples of these tools are available on the ARPANSA website.

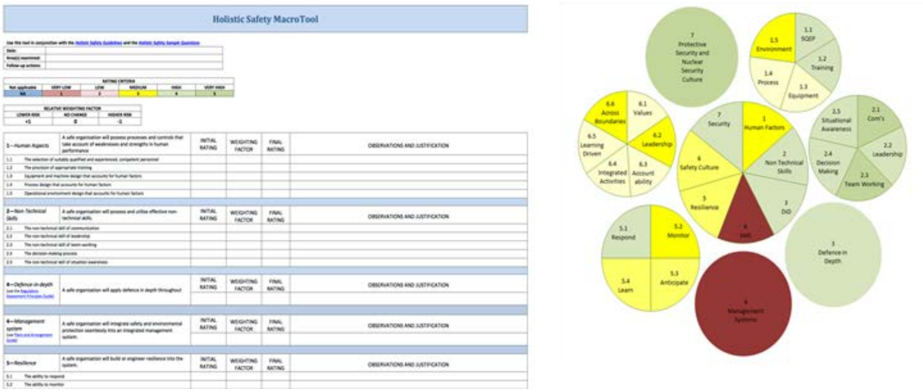


FIG. 3. Screen shot of Holistic Safety tool available from the ARPANSA website and example of output highlighting areas of strength and weaknesses.

4.2. Regulatory compliance

It is not the ARPANSA intention to inspect directly against the holistic safety characteristics but rather to promote improved regulatory compliance by the voluntary adoption of the approach. In 2013 a number of “thematic” inspections were undertaken focusing on the specific services across one large licence holder. These inspections provided some useful information to the licence holders on aspects of holistic safety and received some positive feedback. However, during these inspections, it was difficult to differentiate between the holistic approach to safety and the review of compliance. Ultimately the thematic inspection programme was suspended following a review and alterations to the ARPANSA general inspection programme which are described below.

4.3 The ARPANSA inspection programme

In 2014, ARPANSA undertook a major review of its inspection programme and introduced significant changes that are described in its Regulatory Delivery Model. Inspections are now undertaken against specified performance objectives and criteria (PO&Cs) which support a consistent, transparent and rigorous approach to inspection that is consistent with the risk of a facility, source or controlled activity. PO&Cs provide a comprehensive list of features, controls and behaviours that contribute to safety and, when considered with relevant codes and standards assist the detailed planning and conduct of each inspection and support a qualitative assessment of safety.

The PO&Cs have been developed in consideration of the requirements of the ARPANS Act, international standards and best practices. They are informed by the holistic approach to safety and each of the holistic safety characteristics are carefully wrapped into the PO&Cs. Together, they describe what ARPANSA expects from licence holders. When the PO&Cs are met the organisation will achieve high levels of regulatory compliance and safety standards. When the PO&Cs are not met, ARPANSA will consider the implications for regulatory compliance and safety performance. As well as findings relating to compliance with the Act and Regulations, ARPANSA inspections now include findings of performance deficiencies (PD). A PD does not warrant a finding of non-compliance, but instead highlights a weakness in safety that it expects licence holders to address. This provides a mechanism to highlight any weaknesses in holistic safety performance to a licence holder. The inspections may also highlight areas of good practice where a licence holder goes above and beyond what ARPANSA would normally expect and which can be used to promote improved practices throughout the ARPANSA licence holder community

There are eight PO&C baseline inspection areas, known as ‘baseline modules’ and three cross cutting areas associated with safety culture, human performance and performance improvement (see Figure 3). The scope of individual inspections is determined by the safety risk of the facility. An individual inspection may cover from one to all eight baseline modules with a three year rolling inspection programme ensuring that each module is inspected at least once in a three year period. Whilst elements of the holistic safety approach can be found throughout the whole set of the PO&Cs, the cross cutting inspection areas are particularly associated with the behavioural and organisational aspects of holistic safety. In recognition of the importance of these aspects to an organisation's safety performance, the cross cutting areas are reviewed at all inspections.

A more concise single set of PO&Cs is used for the inspection of a source recognizing that the inspection of sources is usually less complex than a facility. The ARPANSA Regulatory Delivery Model and interactive files of all PO&Cs are available from the inspection page of the ARPANSA website.

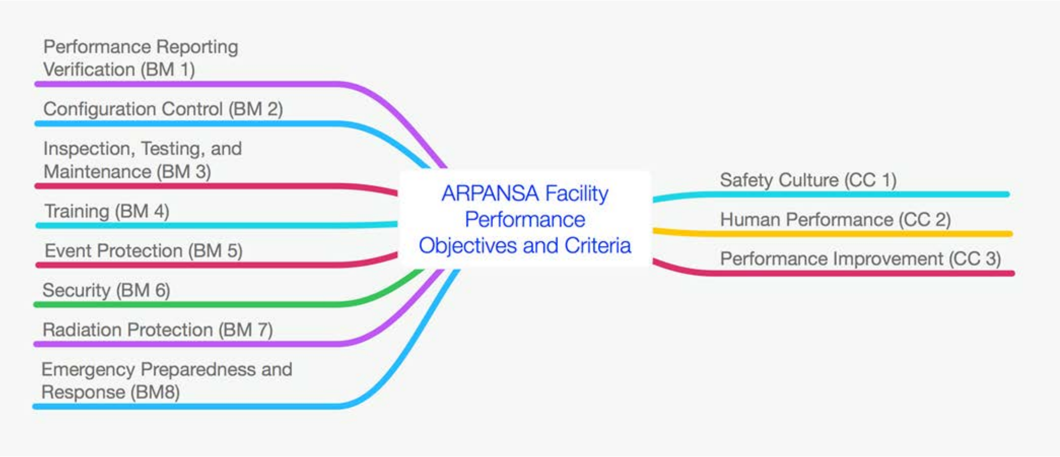

Performance Reporting Verification (BM 1)
Configuration Control (BM 2)
Inspection, Testing, and Maintenance (BM 3)
Training (BM 4)
Event Protection (BM 5)
Security (BM 6)
Radiation Protection (BM 7)
Emergency Preparedness and Response (BM8)
ARPANSA Facility Performance Objectives and Criteria
Safety Culture (CC 1)
Human Performance (CC 2)
Performance Improvement (CC 3)

FIG. 4. The ARPANSA inspection performance objectives and criteria subject areas.

5. REVIEW

One benefit of the ARPANSA inspection programme is consistency between the various inspections that take place. This enables a review for general trends and emerging issues. In the period from March to December 2015, 41 inspection reports were written containing 108 performance deficiencies. A review of the inspection findings is currently being conducted. Whilst more work is required, its initial results are highlighting a number of similarities in the inspection findings which are shown in Figure 5. Many of these findings may be linked to vulnerabilities associated with the contributing causes of accidents on which the ARPANSA holistic approach to safety is founded. For example, roughly 31% of the performance deficiencies are associated with a failure to properly apply internal or external standards. Failure to meet standards may be linked to poor leadership, unhealthy operational attitudes and behaviours, or an organisational (business) environment which does not support or reinforce safety. A further 32% of performance deficiencies were associated with weaknesses in the systems for internal reviews. These may be linked to problems with internal oversight and scrutiny including risk assessment and management.

ARPANSA will continue to collect and review regulatory data which will be shared with licence holders. The objective of this review will always be to highlight vulnerabilities in safety performance for its licence holders to consider and address where needed.

It should be mentioned that the review of inspection findings is also important to the continuous improvement of the regulatory inspection programme. Some aspects of inspections need to be improved in terms of the consistency of conduct; depth of review and reporting outcomes. These findings are actively fed back to the regulatory inspection team and are the basis of ongoing development and training for regulatory staff.

.

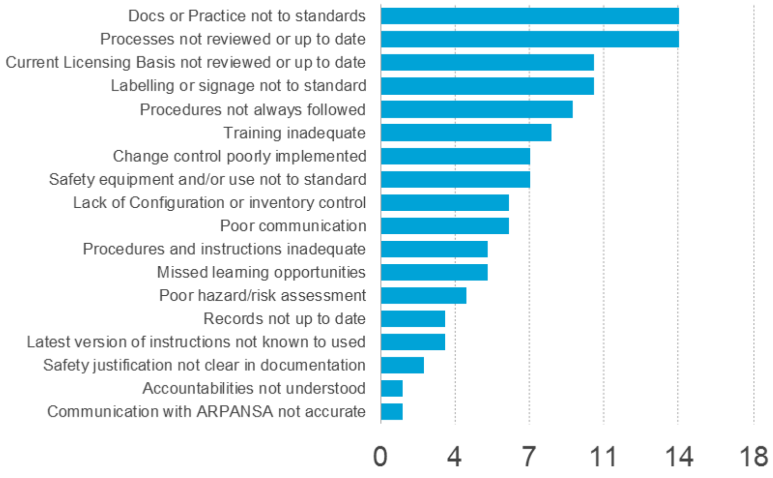


FIG. 5. Chart showing the number of similar performance deficiencies identified during inspection undertaken in 2015.

6. CONCLUSION

The ARPANSA holistic safety approach aims to make licence holders more mindful of the importance to safety of human and organisational factors in addition to technological factors. ARPANSA has endeavoured to make this relevant to its licence holders by developing guidance that will lead to improved controls associated with the common contributing causes of accidents within Australia and elsewhere. Whilst not used directly as a compliance tool, holistic safety characteristics have been wrapped into its inspection performance objectives and criteria so that weaknesses in human and organisational factors may become the subject of performance deficiencies. ARPANSA expects performance deficiencies to be corrected by its licence holders. To further emphasise the importance of this, ARPANSA has begun to review and assess inspection findings cumulatively. This has highlighted a number of common or emerging issues that are associated with accident causation and which can become the subject of improvement.

ACKNOWLEDGEMENTS

The author acknowledges the support of Mr Vaz Mottl and Mr Jordan Lock of the ARPANSA Safety Analysis Section in their support for the development of the holistic safety approach and associated regulatory guidance.

REFERENCES

The ARPANSA holistic safety approach has been developed in consideration of a large number of publications relating to accident causes and modern approaches to safety. A comprehensive list of references is available from the Holistic Safety page of the ARPANSA website, see arpansa.gov.au/Regulation/Holistic.

[1] TAYLOR, R., Learning from disasters – Understanding the cultural and organisational precursors, presented at NEA/IAEA workshop on oversight of, and influencing, licensee leadership and management for safety, including safety culture, Chester UK, 2011.

[2] TAYLOR, R., Managing the organisation and cultural precursors to major events – Recognising and addressing complexity, IAEA international conference on human and organisational aspects of assuring nuclear safety: Exploring 30 years of safety culture, Vienna Austria, 2016.

[3] ARPANSA Website – List of useful references used during development of holistic safety approach - www.arpansa.gov.au/Regulation/Holistic.