NKS-482
ISBN 978-87-7893-578-6

Internal nuclear safety oversight as part of organizational defence-in-depth – Lessons learned for the Nordic nuclear industry
Intermediate report from the NKS-R INSOLE activity

Kaupo Viitanen[1]

Teemu Reiman[2]

Sami Karadeniz[1], Merja Airola[1]

Fredrik Jakobsson[3], Carin Sylvander[3], Sara Lind[3]

[1]VTT Technical Research Centre of Finland Ltd

[2]Lilikoi

[3]Risk Pilot AB

January 2024

Abstract

The NKS-R INSOLE activity aimed to contribute to the development of independent internal nuclear safety oversight functions at Nordic nuclear power plants. This intermediate report describes the findings from the first year of implementing the activity.

Five organizational failures in safety-critical industries where deficiencies in oversight were one of the contributing causes were examined to identify lessons learned for Nordic INSO.

Examples of INSO practices were reviewed in the global nuclear industry. The INSO functions have been introduced in different times and due to different reasons, and under different labels. Their goals included ensuring nuclear safety and excellence, independently challenging the line organization, and providing information to senior management and board of directors.

Preparations for Nordic INSO case studies were described. This involved the identification of Finnish and Swedish cultural characteristics, overview of the respective regulatory frameworks, and areas of interest for the Nordic INSO.

Finally, a draft version of the independent nuclear safety oversight framework was developed and used to guide data collection and analysis. It contains four overall dimensions (system perspective, context, management and organizing, and outcome), several subcategories for each dimension, and example questions for each subcategory, which can be utilized, for example, in self-assessments of the INSO function, guiding the self-improvement of the INSO function, and external evaluation of the INSO function.

Key words

independent oversight, internal oversight, nuclear safety, INSO

NKS-482
ISBN 978-87-7893-578-6
Electronic report, January 2024
NKS Secretariat
P.O. Box 49
DK - 4000 Roskilde, Denmark
Phone +45 4677 4041
www.nks.org
e-mail nks@nks.org

Internal nuclear safety oversight as part of organizational defence-in-depth – Lessons learned for the Nordic nuclear industry

Intermediate report from the NKS-R INSOLE activity

(Contract: AFT/NKS-R(23)138/5)

Kaupo Viitanen[1]
Teemu Reiman[2]
Sami Karadeniz[1], Merja Airola[1]
Fredrik Jakobsson[3], Carin Sylvander[3], Sara Lind[3]

[1]VTT Technical Research Centre of Finland Ltd
[2]Lilikoi
[3]Risk Pilot AB

Table of contents

1 Introduction 3
2 Research Approach and Methods 5
3 Oversight-related Lessons Learned in Safety-Critical Industries 6
3.1 Boeing 737 MAX Crashes and Grounding 6
3.2 NASA Space Shuttle Crashes 10
3.3 Nimrod XV230 16
3.4 Enron scandal 21
3.5 Tokaimura criticality incident 24
3.6 Key lessons learned for INSO 26
4 Independent Internal Nuclear Safety Oversight Globally 32
4.1 Methodology and dataset 32
4.2 Examples of INSO practices globally 33
4.3 Summary 40
5 Formulation of Nordic Case Studies 41
5.1 Nordic cultural context 41
5.2 Nordic regulatory frameworks 43
5.3 Areas of interest for the Nordic INSO 44
6 Independent Nuclear Safety Oversight Framework (draft) 48
6.1 Management and organizing 48
6.2 Context 51
6.3 System perspective 55
6.4 Outcome 59
7 Conclusions 62
8 References 63

1 Introduction

A recent development in the nuclear industry is the **increase of attention towards licensees' self-regulation and internal nuclear safety oversight arrangements**. It becomes increasingly important for the licensees to recognize, how the different ways to organize and implement their internal nuclear oversight function affect their safety performance and how to overcome systemic challenges such as ensuring independence, integration with other processes, cultural contexts, etc.

In the nuclear industry, **oversight** refers to the industry function that "verifies that the utility has the full capability to perform in a manner which achieves fundamental nuclear safety functions through appropriate staffing, processes, activities, actions and monitoring" (WANO & IAEA, 2018, p. 4). WANO and IAEA (2018) have identified four layers of oversight:

- In-process oversight (e.g., peer checking and self-assessment)
- Functional oversight (performed by senior managers)
- Independent oversight (performed independently of the line organization)
- External oversight (e.g., regulator, WANO, IAEA)

The former three are performed internally by the licensee organization (internal oversight). This research activity focuses primarily on **independent internal oversight** but also considers the interactions between the other layers of internal oversight when appropriate.

These oversight layers form an "**organizational defence-in-depth**" structure which serves as an organizational control mechanism for assuring nuclear safety. As with technical defence-in-depth that involves multiple, independent and redundant systems (IAEA, 1996), organizational defence-in-depth involves the use of multiple layers of oversight that may or may not be independent and redundant. The extent to which they are (or can be) independent and redundant, and how this affects the ability of the oversight function to assure nuclear safety serve as examples of open questions related to designing an effective internal oversight function.

Previous research focusing on organizational aspects of internal independent oversight is scarce and there is little prior peer-reviewed research specifically on internal independent nuclear safety oversight. NKS-R INSOLE contributes to the scarce scientific body of knowledge on internal oversight by collecting the **experienced best practices** of nuclear and non-nuclear organizations operating in different sociotechnical contexts and examining the reasons for choosing certain configurations of internal oversight. These findings are analysed in light of the sociotechnical approach to risk management (Le Coze, 2015; Leveson, 2011; Rasmussen, 1997) in order to establish their nuclear safety, organizational and safety culture implications.

The **overall goal** of the activity is to contribute to the development of internal nuclear safety oversight functions at Nordic NPPs by applying a participatory approach.

The **specific goals** of the two-year activity are:

- To study how internal oversight function has been implemented in the global nuclear industry and in non-nuclear safety-critical organizations

- To examine the different ways to organize and implement internal nuclear safety oversight function in nuclear power companies from a sociotechnical perspective

- To develop normative framework for internal nuclear safety oversight function in Nordic NPP context

- To facilitate participative development of internal nuclear safety oversight in Nordic NPPs

In this report, we will describe work done within NKS-R INSOLE during its first year of implementation, focusing primarily on the first three goals. During the first year, the focus was on establishing research approach and methods (chapter 2), reviewing lessons learned from case studies of organizational failures where oversight deficiencies were a contributing cause (chapter 3), reviewing ways of implementing INSO function globally (chapter 4), formulating Nordic case studies (chapter 5), and defining a draft independent nuclear safety oversight framework (chapter 6).

2 Research Approach and Methods

NKS-R INSOLE activity integrates cutting-edge organizational and safety scientific theories, existing knowledge concerning independent oversight, and participative case studies in Nordic nuclear power plants. The overall structure of the activity is summarized in Figure 1.

The principal tool and outcome of the project is the **Independent Nuclear Safety Oversight Framework**. In the first phase of the project (2023), the framework is used to guide data collection and analysis and can take the form of a question battery. The draft framework is based on researcher workshops, theory integration as well as discussions held with representatives from Nordic nuclear power companies during case study preparation. The draft framework is described in detail in chapter 6.

In the second phase of the project (2024), the framework takes a normative form and describes lessons learned and best practices for independent nuclear safety oversight. The normative framework integrates the findings from all previous research activities, including accident case studies (see chapter 3), reference case studies about INSO practices and lessons learned in non-Nordic nuclear and non-nuclear safety-critical domains, and case studies in Nordic nuclear power plants (see descriptions of the case study topics in chapter 5).

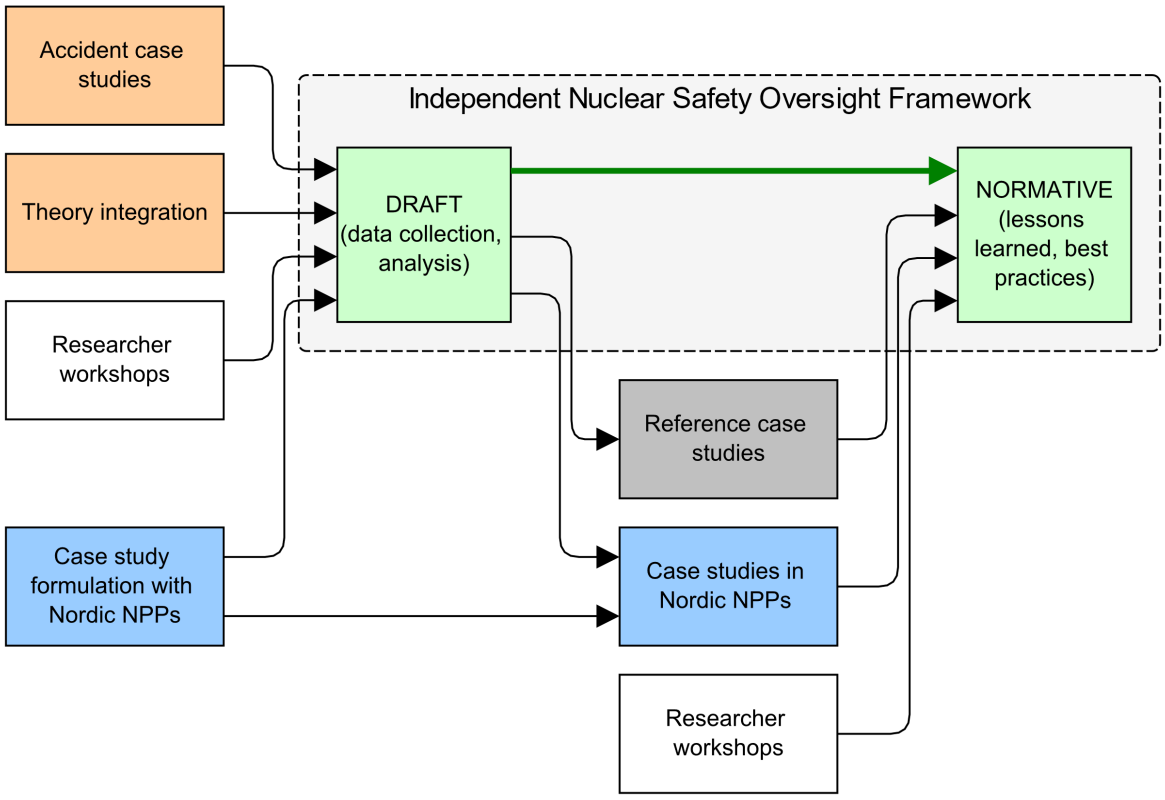

Figure 1. Overall structure of NKS-R INSOLE

3 Oversight-related Lessons Learned in Safety-Critical Industries

3.1 Boeing 737 MAX Crashes and Grounding

3.1.1 Summary of the two crashes

This subchapter summarizes the two Boeing 737 MAX crashes based on the official investigation report (Defazio & Larsen, 2020).

Boeing 737 MAX aircraft was **grounded** worldwide on March 13, 2019, after two crashes, one in Indonesia in 2018 and the other in Ethiopia in 2019. The crashes killed a combined total of 346 people. Apart from the human tragedy, it was a huge blow to Boeing's business, since the company had thousands of 737 MAX orders on its books.

On October 29, 2018, **Lion Air flight 610** dove into the Java Sea shortly after takeoff from Jakarta, Indonesia, killing 189 people. That aircraft was almost brand-new, having arrived at Lion Air three months earlier.

Problems began immediately after the plane had left the ground. The nose mysteriously dipped, and the crew compensated. The nose lifted, but then dipped again. The flight crew repeatedly commanded nose-up trim over the final ten minutes of the flight, not knowing that due to the erroneous angle-of-attack (AoA) data, **Maneuvering Characteristics Augmentation System (MCAS)** was continuously activating and commanding an automatic nose-down trim. Unbeknownst to the pilots, an angle-of-attack sensor was misaligned.

The Indonesian National Transportation Safety Committee published its final report on the Lion Air crash (KNKT, 2019). The report identified nine factors that contributed to the crash, but largely blamed the MCAS. Before crashing, the Lion Air pilots were unable to determine their true airspeed and altitude, and they struggled to take control of the plane as it oscillated for about 10 minutes. Each time they pulled up from a dive, the MCAS pushed the nose down again. “The MCAS function was not a fail-safe design and did not include redundancy”, the report said. The investigators also found that the MCAS relied on only one sensor, which had a fault, and flight crews had not been adequately trained to use the system. Improper maintenance procedures and the lack of a cockpit warning light for the AoA sensor disagree alert contributed to the crash, as well.

The second crash occurred on March 10, 2019, when **Ethiopian Airlines flight 302** departed Addis Ababa Bole International Airport bound for Nairobi, Kenya. Just after takeoff, the pilot radioed a distress call and was given immediate clearance to return and land. But before the crew could make it back, the aircraft crashed 60 kilometers from the airport, six minutes after it left the runway. Aboard were 149 passengers and eight crew members. The aircraft involved was only four months old.

In both accidents, the crews were **unaware of the existence of the MCAS** and **faulty information from the AoA sensor**, which resulted in not-commanded activation of the MCAS. After the accidents, all Boeing 737 MAX aircraft were grounded worldwide for 21 months.

3.1.2 History of Boeing and the 737 MAX development

Boeing was founded by William Boeing in 1916. The Boeing Company developed from military and government supplier to civil aviation market and prided itself on its **engineering-driven and product-focused way of operating**. It designs, manufactures, and sells airplanes, rotorcraft, rockets, satellites, telecommunications equipment, and missiles worldwide.

The story of Boeing is also a story of **competition** with Douglas Aircraft Company (later McDonnell Douglas), and Airbus Industrie, for customers in the growing civil aviation field. The original Boeing 737 grew out of these struggles (then with Douglas DC-9 and the British BAC-111). It was not expected to be profitable – it was designed to be an entry-level model targeting those airlines that are small or are not able to buy larger models (Robison, 2021; Serling, 1991).

The **Boeing 737** first flew in 1967. Against the initial expectations and the company's financial crisis of the late 1960s and early 1970s, it slowly became one of Boeing's most sold airplanes. The 737-100, along with a slightly longer version, the 737-200, were the original generation.

In 1979, Boeing began to develop a **major revamp** of the 737. Making their debuts in the 1980s and early 1990s, the 737-300, 737-400, and 737-500 were introduced. They came to be known as the 737 Classic series. The 737-300, introduced in 1984, had the latest high-bypass-ratio engines designed specifically for the airplane, having engine nacelles with then unusual flat-shaped bottoms. The 737-300 "was a transport designed for the era of deregulation and became a stunning sales success, although the McDonnell Douglas MD-80 was a powerful competitor" (Serling, 1991, p. 401). Thirty years after its development, the Boeing 737 was the best-selling jetliner in the world (Rodgers, 1996, p. 229).

In the early 1990s, Boeing began working on **another 737 update**. These planes, which entered service in the late 1990s and early 2000s, were known as the 737NG ("Next Generation"). The performance of the 737NG meant it was essentially a whole new aircraft family compared to the Classic, but it kept enough important commonality with the Classic that upgrading or operating mixed fleets would be easier and more cost-effective for customers. The airframe received upgrades, the wings were redesigned, and the flight deck and cabin were improved.

In August 1997, **Boeing and McDonnell Douglas merged**. The new company was called Boeing, incorporating logos of both McDonnell Douglas and Boeing. The CEO of McDonnell Douglas, Harry Stonecipher, became the president and COO of Boeing. Stonecipher had started at McDonnell Douglas in 1994, being the first outsider to run the then family business. Stonecipher came from General Electric, where he learned the "art" of reducing costs and increasing shareholder value (Robison, 2021).

In 2001, Boeing **moved its headquarters** from Seattle to Chicago, into a "new, leaner corporate center focused on shareholder value" instead of "how-do-you-design-an-airplane stuff", as the CEO of Boeing who implemented the merger and the relocation, Philip Condit, succinctly put it (Robison, 2021, p. 79).

Boeing's **new business model** relied on heavy **outsourcing** and a strong **focus on efficiency and costs**. For example, the simulator training department was established as its own company, selling its services to Boeing as well as airlines. Harry Stonecipher boasted in an interview: "When people say I changed the culture of Boeing, that was the intent, so it's run like a business rather than a great engineering firm. It is a great engineering firm, but people invest in a company because they want to make money." (Callahan, 2004)

The first new civilian airplane developed with the **new, streamlined business model**, was the Boeing 787 Dreamliner, the development of which was approved by the board of directors in April 2004. That project was marked by serious cost overruns and many outsourcing-related problems foreshadowing the challenges faced by the Boeing 737 MAX project (Robison,

2021)[1]. Originally targeted for a 2008 release, the Dreamliner entered commercial service in late 2011. The delays and cost overruns of the 787 project also affected the next product Boeing was considering: the successor for the 737NG. For a while, Boeing considered both replacing the 737 with a brand-new airplane, or re-engining the 737NG with more efficient engines and other features. A team to consider the options was established in 2006, but in 2010 they still had not reached a decision. Then, in December 2010, rival Airbus announced their A320neo family, which was a re-engined, more efficient version of A320, and the main competitor to the 737. Some major American airlines started to lean towards ordering from Airbus if Boeing could not offer something similar.

In 2011, Boeing finally ditched the idea of designing a whole new airplane and instead decided on **re-designing the 737**.

There were several advantages of the redesign of the 737. It could take up to 10 years to get a new design in the air, and the costs of a redesign were estimated as $2.5 billion compared to $20 billion for a new design. Also, the fact that it was an existing, already certified airframe, meant that Boeing would not have to undergo the same lengthy certification process it would for an all-new airplane. Further, as with the transition from the 737 Classic to the 737NG, the 737 MAX retained a great degree of commonality with its predecessors, which meant that **one pool of pilots and ground staff could work on both planes, with some supplementary training**, rather than having to be certified on a new aircraft type. Boeing promised its customers that the pilots will only be required to take a brief tablet-based course, rather than full simulator training, like they would for a new plane.

3.1.3 The Maneuvering Characteristics Augmentation System

When Boeing designed the 737 MAX, it made the **engines larger** to increase fuel efficiency and positioned them slightly forward and higher up on the plane's wings. Early testing revealed that the relocated engines caused the plane's nose to pitch upward in some situations (e.g., low-speed flight, or flight with a high angle-of-attack when the plane is being flown manually). Both software and hardware fixes (such as redesigning the tail) were considered for these undesirable aerodynamic changes, but eventually Boeing settled on a software solution.

The Maneuvering Characteristics Augmentation System (MCAS), a piece of software, was designed to **improve the airplane's handling characteristics and to decrease the pitch-up tendencies at elevated angles of attack**. The objective was to avoid stalling (loss of lift), which can happen if the plane flies at too steep an angle. MCAS activates automatically, without the pilot's input – and in the two accident cases, without the pilots' knowledge.

Originally, the MCAS was designed to activate only in high velocities and high angle-of-attack situations. In 2016, one year prior to the FAA's certification of the 737 MAX, when Boeing test pilots were finally able to fly the actual plane, they found that it was not handling well when nearing stalls at lower speeds. As a solution, Boeing **redesigned the MCAS** to enable its activation at lower speeds. Moreover, the new version of the MCAS could move the horizontal stabilizer a maximum of 2.5 degrees (as opposed to 0.6 degrees as originally designed).

[1] The lithium battery fires in several Dreamliners in 2013 uncovered similar deficiencies at Boeing and the FAA as the 737 MAX accidents. Among the NTSB's findings, it found inadequate FAA oversight, a failure by both FAA and Boeing's Authorized Representatives (ARs) to identify critical deficiencies, and flawed safety assumptions by Boeing that it made into the airplane's System Safety Assessment. (Defazio & Larsen, 2020)

Boeing was worried that the **Federal Aviation Administration** (FAA, the regulatory authority) would treat the MCAS as a new function and required simulator training for the pilots – a condition that Boeing had promised its customers would not happen. In 2013, Boeing made a decision to downplay the significance of MCAS externally, and to present it as just a part of the old system (Robison, 2021, p. 140). Thus, Boeing did not include any information on MCAS in the pilots' training material and its redesign was never communicated to FAA. (Defazio & Larsen, 2020; Robison, 2021)

3.1.4 Oversight of safety issues during the Boeing 737 MAX certification

The official investigation of the two crashes concluded that they resulted from a culmination of faulty technical assumptions, lack of transparency in Boeing's management and "grossly insufficient" oversight by the regulator (Defazio & Larsen, 2020). The investigation discovered the following root causes of the two accidents:

- Production pressures leading to update the Boeing 737 design swiftly and inexpensively.
- Faulty design and pilot performance assumptions.
- Culture of concealment.
- Conflicted representation in the system that deputizes Boeing employees to act on behalf of the government.
- Boeing's influence over FAA's oversight structure.

In this report, we will deal with the two last ones in more detail. Other factors, important as they are, will only be considered superficially.

The Boeing 737 MAX was approved under the FAA's "**Organizational Designation Authorization**" (ODA) program. FAA created the ODA program in 2005 and finalized in 2009 to standardize its oversight of aircraft manufacturers that have been approved to perform certain functions on the Agency's behalf, such as determining compliance with aircraft certification regulations (Office of Inspector General, 2015). The ODA program effectively allows the aircraft manufacturers to certify parts of their own designs with limited federal oversight. According to Boeing data, as of March 2017, FAA delegated all 91 certification plans to Boeing's ODA (Gotcheva & Ylönen, 2021).

The ODA program **enhanced the authority that FAA granted to aircraft manufacturers to perform FAA-mandated certification activities**. Before 2009, FAA selected the authorized representatives (ARs) at the aircraft manufacturer who were authorized to act on FAA's behalf. After 2009, the selection of the ARs was done by the manufacturers, in this case Boeing. (Robison, 2021)

Under the ODA program, Boeing served as a buffer between the ARs and FAA technical experts to help **funnel the information regarding certification issues to the FAA in a more effective and efficient manner**. While this change relieved FAA of an administrative burden, it limited the interactions between ARs and FAA staff, which prevented free communication of issues and concerns. If there had been more fluid and frequent communication between Boeing's ARs and FAA officials in the FAA offices overseeing the certification of Boeing 737 MAX, FAA's knowledge of the ARs concerns might have dramatically improved safety of the

airplane and enhanced FAA's certification scrutiny of the 737 MAX program. (Defazio & Larsen, 2020)

There were indications that Boeing employees who were supposed to be **representing the interests of the FAA** under the ODA program were instead representing the interests of Boeing. Further, Boeing designees involved in critical issues regarding the certification of the 737 MAX program failed to keep the FAA adequately informed of key issues, although these same designees did attempt to raise these issues internally at Boeing. FAA's own employees reported in a survey that they perceived too much external influence on FAA and that the delegation of certification responsibilities to "external FAA designees" (e.g., Boeing employees) has not been done adequately.

After the Lion Air crash, FAA learned about the redesigned MCAS and its vulnerability to a single point of failure in the angle-of-attack sensor. FAA conducted an analysis and estimated that without a software fix to the system, there might be as many as 15 similar accidents during the lifetime of the Boeing 737 MAX. Despite this analysis, FAA did not ground the airplane, but rather gave Boeing ten months to come up with a software fix. A few months after the accident, FAA's Associate Administrator for Aviation Safety described it as a "one-off" caused by poor pilot performance at Lion Air (Defazio & Larsen, 2020, p. 238). A month later, the second crash occurred. Regulators in China, EU, India, Australia, Singapore, and Canada grounded the 737 MAX. Three days later, the FAA followed suit. Under the ODA program, **FAA did not prioritize oversight of "the highest-risk areas"**, such as new aircraft designs, and it did not have an adequate system for determining whether the teams that were overseeing certifications were sufficiently staffed. The lack of independent design verification by experts also contributed to the "**crash of the regulatory system**" (Sgobba, 2019).

3.2 NASA Space Shuttle Crashes

3.2.1 Introduction

National Aeronautics and Space Administration (NASA) **Space Shuttle Program** was first envisioned in late 1960s as part of Space Transportation System, which was supposed to provide an easy and convenient access to space. The system aimed to reduce the cost of spaceflight by replacing expendable rockets with reusable spacecraft and to support other programs such as space stations and a human landing mission to Mars.

The Space Shuttle was marketed as **safe and cost-effective transportation to space** with one flight every week. NASA had settled on the basic layout of the Space Shuttle in 1972. It would consist of two solid rocket boosters and three main engines burning hydrogen and oxygen for the eight-minute flight to orbit. The fuel and the oxidizer for the main engines were to be stored in an external fuel tank attached to the orbiter. The orbiter would be the manned and winged shuttlecraft that would return to earth. To keep space travel costs down, NASA sought to develop a fully reusable vehicle.

The **two accidents, Challenger, and Columbia**, happened in 1986 and 2003, respectively. In the case of Challenger, the technical failure was erosion of seals (O-rings) between segments of the solid rocket booster shortly after launch. In the Columbia Space Shuttle accident, the physical cause of the accident was a breach in the thermal protection system on the leading edge of the left wing, caused by a piece of the insulating foam that struck the wing immediately after launch.

Columbia Accident Investigation Board concluded that both accidents were "**failures of foresight**", and that their similarity demonstrated that "the causes of the **institutional failure** responsible for Challenger have not been fixed" (CAIB, 2003, p. 195). The board identified attributes of an organization that could more safely and reliably operate the inherently risky Space Shuttle (CAIB, 2003, p. 9):

- A robust and independent program technical authority that has complete control over specifications and requirements.
- An independent safety assurance organization with line authority over all levels of safety oversight.
- An organizational culture that reflects the best characteristics of a learning organization.

After the Challenger Space Shuttle accident in 1986, **NASA reorganized** its activities to put more emphasis on safety issues. For example, they opened a confidential hotline for reporting safety problems, trained engineers in quality control, increased use of statistical risk and trend analysis, and standardized procedures for tracking significant problems. With its contractors, NASA moved away from cost-plus-incentive-fee and cost-plus-fixed-fee contracts that subordinated quality standards to cost and schedule requirements. Instead, they sought to enhance safety and quality by using cost-plus-award-fee contracts that had specific quality requirements and incentives, as well as by putting quality experts on Award Fee Boards. (Dunar & Waring, 1999, p. 410)

After the Challenger accident, the Space Shuttle Program went into an "increasingly ritualistic set of reforms that temporarily increased safety consciousness as the system geared up for a return to flight program that would have a scope far beyond what was advised by commissions and panels." (Farjoun, 2005, p. 27). Despite many reforms, **the powerful space flight culture and institutional practices largely remained intact** and before the Columbia accident, issues such as normalization of deviances, silent safety program and schedule pressure had returned (CAIB, 2003, p. 101).

In 1992, the government made cuts to NASA's budget. As a response, a new philosophy "**Faster, Better, Cheaper**" was introduced. Major cuts were made in safety programs and personnel and safety function was downsized. During the 1990s, NASA reduced its workforce by 25 percent. There was a perception in NASA that they had overreacted to the Challenger Accident investigation report recommendations by introducing too many layers of safety inspections in launch preparation and that it had created a bloated and costly safety program. (Farjoun, 2005, p. 30)

NASA's culture had developed over a long time, which made it very **resistant to change**. The Apollo era had introduced an exceptional "can-do" culture expressing tenacity in the face of seemingly impossible challenges. This culture highly valued interaction among research and testing, and hands-on engineering experience. It was dependent on the exceptional quality of its workforce and leadership. As such, the organization possessed in-house technical capability to oversee the work of its contractors. **Risk and failures were accepted as inevitable** aspects of operating in space, even though at the same time the culture held as its highest value attention to detail to lower the chances of failure. (CAIB, 2003, pp. 101–102)

Success of the Apollo missions created an influential image of the space agency as a "perfect place". The organization saw itself as "the best organization that human beings could create to

accomplish selected goals." According to the Columbia Accident Investigation Board report, this vision, based on **glories of an earlier time**, did not change with times even though the world and consequently, the context within which the space agency operated, changed around NASA's organization (CAIB, 2003, p. 102).

Instead of keeping up with changing times and demands of a new operational environment, NASA found new incentives to **hold on to problematic cultural attitudes**. Obviously, NASA as an organization was anything but an island isolated from society around it – how strongly outside pressures and constraints affected every aspect of it being proof that. More likely than the idea of NASA as a walled city cut off from the world around it, is that despite everything that changed in the world around NASA, that world still managed to produce new incentives and encouragement to hold onto unrealistic, overconfident, and overoptimistic views about NASA's ability to perform as expected. These expectations changed remarkably little, even though the resources allocated to NASA dwindled steadily. This, in turn, led NASA into setting itself **impossible goals**.

According to the Columbia Accident Investigation Board, external criticism and doubt reinforced the will to "impose the party line vision on the environment, not to reconsider it". This in turn led to **flawed decision making, self-deception, introversion, and a diminished curiosity** about the world outside the perfect place. The NASA human space flight culture the Board found during its investigation manifested many of these characteristics. In particular, the Board noted a self-confidence about NASA possessing unique knowledge about how to safely launch people into space (CAIB, 2003, p. 102).

Furthermore, against all the evidence that had accumulated over time, it appears that NASA (and everyone else as well) **failed to grasp the basic nature of the Space Shuttle System**. Consequently, NASA's understanding of its organizational core task in developing the Space Shuttle System was compromised. In 1995, the Kraft Committee, established to examine NASA contractual arrangements and opportunities for privatization, characterized the Space Shuttle Program as a well-run program and the Space Shuttle as "a mature and reliable system ... about as safe as today's technology will provide" (Kraft, 1995). This was a mischaracterization, but it allowed NASA to continue to believe that it could turn increased responsibilities for Space Shuttle operations over to a single prime contractor and, as a result, reduce its direct involvement in ensuring safe Space Shuttle operations and instead monitor contractor performance from a more detached position. NASA also thought that the "maturity" of its Space Shuttle meant the ability to carry out operational missions without continually focusing engineering attention on understanding the mission-by-mission anomalies typical for vehicles considered to still be in developmental stage (CAIB, 2003, p. 118).

In 1984, President Reagan announced the goal to build a **space station** enabling a permanent human presence in space within a decade. Deliveries of cargo and personnel necessitated an operational space shuttle for the new International Space Station (ISS). The ISS project itself was competing for the ever-decreasing resources within NASA, and the project experienced delays and cost overruns. By 1988, the project's total cost estimate had tripled, and the first scheduled launch was bumped from 1992 to 1995. (Farjoun, 2005)

Because the Space Shuttle was now tied to ISS's needs (e.g., crew rotation), the urgency of maintaining a **predictable launch schedule was emphasized**. Any delays in the Space Shuttle's schedules would also impact the ISS schedule. During 1998, an international agreement made the ISS project an international cooperation project. Service flights to the station were viewed by external observers, such as scientists and space policy experts, and by

people within NASA, as a distraction from the science and technology goals of the NASA project (Farjoun, 2005).

The combination of **financial constraints and overambitious goals** meant that NASA was unable to address adequately the fact that its **Space Shuttle fleet was aging**. Maintenance costs for the Space Shuttles were rising, in sharp contrast with demands to cut costs. There were plans to replace the Space Shuttles with newer vehicles, but in the 1990s, the planned date for replacing the Space Shuttle shifted first from 2006 to 2012 and then to 2015 or later. Aging and increasingly expensive Space Shuttles were simply expected to continue safe performance for some 10 years past what had been originally planned, because there was no money to replace them, even though they had become invaluable to ISS, and they were the only means of getting to the ISS in addition to Russian Soyuz. (CAIB, 2003)

3.2.2 Oversight and quality assurance at NASA

The Commission investigating the Challenger accident called for **centralizing of safety oversight** (Presidential Commission on the Space Shuttle Challenger Accident, 1986). The Commission recommended a new Shuttle Safety Panel to be formed, that would report to the shuttle program manager. Also, an independent Office of Safety, Reliability and Quality Assurance (SR&QA) was to be established, headed by an associate NASA Administrator, with independent funding and direct authority over all safety bodies throughout the agency. It should report to the NASA Administrator, rather than program management, as a way of keeping safety separate structurally from the part of NASA responsible for budget and efficiency in operations. NASA initiated the recommended Headquarters Office of Safety, Reliability and Quality Assurance (renamed Safety and Mission Assurance, S&MA) but instead of the direct authority over all safety operations, as the Commission recommended, **each of the centres had its own safety organization**, reporting to the centre director, and the various centre safety offices in its domain remained **dependent because their funds came from the very activities that they were overseeing** (CAIB, 2003; see also Vaughan, 2005).

Thus, one of the things that did not change between Challenger and Columbia Accidents was the **weak position and authority of safety and oversight in the NASA organization** (CAIB, 2003). The Columbia Accident Investigation Board report noted surprise that safety was not deeply engaged at every level of Space Shuttle management: “Safety and mission assurance personnel have been eliminated, careers in safety have lost organizational prestige, and the program now decides on its own how much safety and engineering oversight it needs” (CAIB, 2003, p. 181).

Columbia Accident Investigation Board (2003) criticized the organizing of safety assurance at NASA as **overly bureaucratic and confusing in terms of authorities and responsibilities**. The position of the Space Shuttle Division Chief was described as a critical node in NASA’s Safety and Mission Assurance architecture that seems to the Board to be plagued by conflict of interest. It is a single point of failure without any checks or balances. Many other positions were also such that their holders simultaneously performed duties on both the centre’s and program’s behalf.

In response to the Rogers Commission Report (Presidential Commission on the Space Shuttle Challenger Accident, 1986) after the Challenger accident, NASA established what is now known as the **Office of Safety and Mission Assurance** at Headquarters to independently monitor safety and ensure communication and accountability agency-wide. The Office of

Safety and Mission Assurance focused on monitoring unusual events like "out-of-family" anomalies and establishes agency-wide Safety and Mission Assurance policy[2].

The Office of Safety and Mission Assurance also screened the Space Shuttle Program's Flight Readiness Process and signed the Certificate of Flight Readiness. The Space Shuttle Program Manager, in turn, was responsible for overall Space Shuttle safety and was supported by a one-person safety staff. The Space Shuttle Program was permitted to organize its safety program as it saw fit, which resulted in a **lack of standardized structure** throughout NASA's various centres, enterprises, programs, and projects. The **level of funding** a program was granted impacted how much safety the Program could "buy" from a centre's safety organization. In turn, Safety and Mission Assurance organizations struggled to anticipate program requirements and to guarantee adequate support for the many programs for which they were responsible. (CAIB, 2003, p. 186)

The Columbia Accident Investigation Board concluded that the safety system structure left the Office of Safety and Mission Assurance **ill-equipped to hold a strong and central role in integrating safety functions**. NASA Headquarters had not effectively integrated safety efforts across its culturally and technically distinct centres. In addition, the practice of "buying" safety services established a relationship in which programs sustain the very livelihoods of the safety experts hired to oversee them. These idiosyncrasies of structure and funding prevented the safety organization from effectively providing **independent safety analysis**. (CAIB, 2003, p. 186)

Leveson et al. (2005) also noted that the organizational changes made after the Challenger accident to increase the independence of safety activities had the **opposite result**, as the program manager decided how much safety is to be "purchased" from this new separate function, making the safety experts dependent on the programs.

The Columbia Accident Investigation Board believed that although the Space Shuttle Program had effective safety practices at the "shop floor" level, its operational and systems safety program was flawed by its dependence on the Space Shuttle Program. Its conclusion was that the **safety apparatus, suffering from a cumbersome organizational structure, chronic understaffing, and poor management principles, was unable to fulfil its mission** (CAIB, 2003, p. 186).

The structure and process placed Space Shuttle safety programs in the unenviable position of having to choose between rubber-stamping engineering analyses, technical efforts, and Space Shuttle program decisions, or trying to carry the day during a committee meeting in which the other side almost always has more information and analytic capability (CAIB, 2003, p. 187; see also Leveson et al., 2005, p. 273).

Leveson et al. (2005) discussed the challenges associated with assigning safety responsibility to an assurance organization (S&MA): "One core aspect of any matrix structure is that it only functions effectively if the full tension associated with the matrix is maintained. However, once one side of the matrix deteriorates to a "dotted line" relationship, it is no longer a matrix – it is just a set of shadow lines on a functionally driven hierarchy. The post-Cold War Systems Approaches to Safety period, with the new mantra of "faster, better, cheaper," has created new stresses and strains on this formal matrix structure, relegating the safety organization to the role

[2] An out-of-family event is an operation or performance outside the expected performance range for a given parameter or which has not previously been experienced.

of providing "safety services" to engineering and operations. Over time, this has created a misalignment of goals and inadequate application of safety in many areas." (Leveson et al., 2005, pp. 274–275)

Having all the safety engineering activities in a quality assurance organization with a weak matrix structure that provides safety expertise to the projects turns **safety into an after-the-fact or auditing activity only**. Furthermore, assurance groups in NASA did not have the **prestige necessary to influence decisions**. This was evident in the Challenger accident, where the safety engineers were silent and not invited to be part of the critical decision-making groups and meetings, and in the Columbia accident, when they were a silent and non-influential part of the equivalent meetings and decision-making (CAIB, 2003, p. 275).

The organizational structure also affected **information flow regarding observed deviations and their potential safety consequences**. Edmondson et al. (2005, p. 232) stated in their analysis of the Columbia accident that the rigidity of communication protocols inhibited exchange of ideas, questions, and concerns, and encouraged the reporting of packaged, or summarized, results up the hierarchy. Uncertainties related to the information were lost when the information moved through the organizational boundaries.

The Space Shuttle Independent Assessment Team (SIAT) board was formed because of increases in Space Shuttle failures in 1999. It released its report in March 2000 (NASA, 2000). The report identified systemic issues involving the **erosion of key defensive practices** – a shift away from the rigorous execution of pre-flight and flight-critical processes[3]. The reasons were many: reductions in resources and staffing, a shift toward a "production mode" of operation, and the optimism engendered by long periods without major mishap. However, the major factor leading to concerns was the reduction in resource allocations and staff devoted to safety processes. Although not all its recommendations were implemented, NASA took this report seriously and moved to stop Space Shuttle staffing reductions, added safety inspections, and sought more resources. In response to the SIAT there was a presidential initiative in 2001 to finance safety upgrades, but cost growth in Space Shuttle operations forced NASA to use funds intended for Space Shuttle safety upgrades to address operational needs. (Farjoun, 2005)

3.2.3 Changes after the Columbia accident

The Columbia Accident Investigation Board (CAIB, 2003, p. 193) noted that the responsibility and authority for decisions involving technical requirements and safety should rest with an independent technical authority. These findings resulted in a recommendation to establish a **Technical Engineering Authority funded directly from NASA Headquarters**, with no connection to or responsibility for schedule or program cost.

Second, NASA's headquarters office of Safety and Mission Assurance (formerly SR&QA) would have **direct authority and be independently resourced**. To assure that problems on one part of the Space Shuttle (e.g., the foam debris from the external tank) considered ramifications for other parts (e.g., foam hitting the orbiter wing), the Space Shuttle Integration Office would be reorganized to include the orbiter, previously not included.

Several other developments have taken place at NASA after the Space Shuttle accidents, but these will not be discussed here. Only one example is given that is directly relevant to independent oversight. Clearfield and Tilcsik (2018, p. 214) described how NASA's Jet

[3] The report explicitly relied on Reason's Swiss Cheese model (see Reason, 2000)

Propulsion Laboratory (JPL) sought to combat the normalization of deviance by relying on "outsiders' views". They created the **Engineering Technical Authority (ETA)**, a cadre of outsiders within JPL. Every project is assigned an ETA engineer, who makes sure that the project manager does not make decisions that put the mission at risk. In case of disagreements between the project manager and the ETA manager, there is a clear escalation channel to the ETA program manager, and finally to JPL's chief engineer. According to Clearfield and Tilcsik (2018, p. 215) ETA engineers are "skilled enough to understand the technology, close enough to understand the group, but detached enough to bring a different perspective."

3.3 Nimrod XV230

3.3.1 Introduction

Nimrod XV230, a maritime reconnaissance aircraft, suffered a **catastrophic fire and explosion in mid-air** over Afghanistan in September 2006, killing all 14 service personnel on board. The accident happened minutes after air-to-air refueling and was proximally caused by a fuel leak and an ignition source on board. A comprehensive independent review carried out by Queen's Counsel Charles Haddon-Cave and his team (2009) outlined three major themes on the factors that led to the accident: aircraft design flaws, failures in risk and safety assessment of the aircraft, and organizational causes, such as organizational changes and financial pressures.

The Nimrod was a **modified version of De Havilland Comet**, a commercial jet plane that had its maiden flight in 1949 (Haddon-Cave, 2009, p. 16). 20 years later, XV230 was the first Nimrod to enter military service (Haddon-Cave, 2009, p. 17). The Royal Air Force (RAF) of United Kingdom used Nimrod aircrafts especially for monitoring Soviet maritime activity during the Cold War, but they were also used for maritime search and rescue operations (Haddon-Cave, 2009, p. 23). During the war in Afghanistan, Nimrods were used to gather intelligence over land. It was in such an operation, while supporting NATO and Afghani ground forces that the XV230 caught fire and exploded on the 2nd of September 2006 (Haddon-Cave, 2009, p. 5).

The conversion of commercial airliners to military aircraft required numerous physical modifications to the planes that subsequently **introduced potential sources of ignition**. Moreover, during the Falkland war in the 1980s, air-to-air refuelling capability was added to the Nimrods. According to Haddon-Cave's investigation, these modifications introduced design flaws that were the underlying physical causes of the accident. Specifically, it is believed that the air-to-air refuelling system modifications were to blame in the fuel leak, whereas a hot air duct rupture in the modified aircraft's fuelling system was the source of the ignition on board (Haddon-Cave, 2009, p. 15).

According to Haddon-Cave, the accident could have been prevented if due attention had been paid to the **safety assessment of the aircraft** (Haddon-Cave, 2009, p. 10). Hazards were overlooked even though there were several documented cases where similar factors had caused incidents in other Nimrods (Haddon-Cave, 2009, p. 149).

To understand how such an incident came about, it is necessary to start from the organizational level, examining the background conditions that eventually produced a failed safety assessment of the XV230 and led to the fatal accident.

3.3.2 Background

In 1998, UK Government published a white paper called Strategic Defence Review outlining multiple **organizational change initiatives** in the Ministry of Defence (MOD) aimed at increasing efficiencies and savings in operations. Changes related to military system acquisition and in-service support processes were especially relevant in light of the XV230 accident.

Procurement in MOD in the 1990s had failed in purchasing and developing major military systems, as the processes repeatedly suffered from major delays and cost overruns (Haddon-Cave, 2009, p. 12). An external consulting firm was hired by MOD to review military procurement procedures and to come up with alternative operational models with the aim of increasing efficiencies, shortening procurement times and increasing savings (Haddon-Cave, 2009, p. 361).

The Defence Logistics Organisation, responsible for the management of XV230, was tasked with a strategic goal of a 20% saving in the output costs between the years 2000 and 2005 (Haddon-Cave, 2009, p. 357). According to Haddon-Cave, the financial targets set after the Strategic Defence Review caused an organizational **shift from a safety culture to a business culture**, which distracted especially the senior staff's attention away from safety matters to financial ones.

These suggested changes also had a direct impact on the **in-service support processes** that determined aircraft safety. Changes relevant to the XV230 accident were especially the following ones (Haddon-Cave, 2009, p. 356):

- A shift from function-oriented organizational lines to project-oriented ones that had started in the early 1990s but intensified after the Strategic Defence Review.
- Creating larger, multi-service organizational units.
- Increased outsourcing of service functions to industry partners.

To better understand the implications and consequences of the organizational changes listed above, let us compare the airworthiness structure before and after the publication of the Strategic Defence Review in 1998.

3.3.3 Airworthiness structure before the Strategic Defence Review

In the 1990s, Royal Air Force (RAF) had rather **coherent procedures regarding aircraft airworthiness** – a term used in the aviation industry that refers to the safe operational condition of an aircraft or its parts. Overall responsibility for the fleet airworthiness resided with the Chief Engineer under the RAF Logistics Command organization, which provided support, repair and overhaul services for the aircraft (Haddon-Cave, 2009, p. 384). Chief Engineer was a high-ranking officer who answered to the Chief of the Air Staff. Chief Engineer's tasks included setting the airworthiness policy, drafting regulations, carrying out airworthiness review processes and maintaining airworthiness audits of multidisciplinary groups, which were engineer-led units responsible for the servicing and safety of each aircraft type (Haddon-Cave, 2009, p. 343). Chief Engineer delegated responsibility to Director General of Support Management, who then delegated responsibility further to officers in charge of the multidisciplinary groups.

Chief Engineer and Director General of Support Management had an **airworthiness audit team** which was solely dedicated to auditing multidisciplinary group airworthiness processes (Haddon-Cave, 2009, p. 385). Aircraft safety was monitored via periodic Airworthiness Audits and Support Authority Reviews, which were highly meticulous processes where multidisciplinary group team leaders had to demonstrate aircraft safety in the presence of an active and cross-questioning Chief Engineer (Haddon-Cave, 2009, p. 392).

RAF also employed an internal, **independent safety oversight unit** called the Inspectorate of Flight Safety, whose director visited different RAF stations to talk with personnel, carried out inspections, monitored RAF occurrence reports and conducted Airworthiness Reviews of the aircraft (Haddon-Cave, 2009, p. 386). These activities provided information and advice to commanders.

3.3.4 Airworthiness structure after the Strategic Defence Review

After the publication of the Strategic Defence Review, **RAF Logistics Command was disbanded**. RAF service organization, along with the service organizations of the navy and the army, were merged into the larger tri-service Defence Logistics Organisation, with the hope of increased savings, elimination of overlaps and increased leverage over suppliers (Haddon-Cave, 2009, p. 346). The role of Chief Engineer was removed, and the representation of the air force in the Defence Logistics Organisation was headed by Director General of Equipment Support (Air) (DG ES(Air)), whose military rank was lower than that of Chief Engineer. DG ES(Air) delegated responsibility to leaders of Integrated Project Team, which replaced multidisciplinary groups (Haddon-Cave, 2009, p. 351).

In 2005, the DG ES(Air) role was removed, producing a larger **gap in the chain-of-command** between the Integrated Project Team leaders and the more senior staff and weakening the support and supervision available for Integrated Project Team leaders (Haddon-Cave, 2009, p. 395). This proved to be a lamentable change, as the Nimrod Integrated Project Team leaders, who were increasingly occupied with achieving their financial goals instead of attending to the technical and safety aspects of the aircraft, felt they were abandoned by their superiors (Haddon-Cave, 2009, p. 358).

Changes after the Strategic Defence Review had significant effects on the **airworthiness regime**. Inspectorate of Flight Safety, which had previously provided independent airworthiness inspections, was folded into the newly formed Defence Aviation Safety Centre, which was another tri-service organization that had officers from all the services (i.e., the navy, the army, and the RAF). Auditing authority in the new organization was insufficient to inspect Integrated Project Teams, which resulted in the **loss of an important independent airworthiness audit structure** (Haddon-Cave, 2009, p. 386). Previously, the keen interest in airworthiness matters displayed by Chief Engineer had a positive influence on the thoroughness of safety inspections. With the dismantling of Chief Engineer role, the number of full Airworthiness Audits decreased and Support Authority Reviews disappeared altogether (Haddon-Cave, 2009, p. 392). Integrated Project Team audits focused mostly on compliance matters.

To summarize, the simple and effective airworthiness structure along with its scrupulous airworthiness review processes disappeared with the organizational changes and they were replaced with convoluted and less effective alternatives. Even the Defence Aviation Safety Centre itself produced a report concluding that **the new airworthiness structure was confusing and dysfunctional** (Haddon-Cave, 2009, p. 387).

Furthermore, change initiatives did not end at the immediate aftermath of the Strategic Defence Review. On the contrary, there were further waves of organizational changes and manpower reductions in the Defence Logistics Organisation throughout the period between 2000 – 2006, which further accelerated the dilution of the strict airworthiness regime of the era preceding the Strategic Defence Review (Haddon-Cave, 2009, p. 357).

3.3.5 The Nimrod Safety Case

Since the early 2000s, UK military regulations demanded that the safety assessments of the aircraft, including the Nimrods, were carried out by drawing up Safety Cases, which were **structured arguments demonstrating that an aircraft was safe to operate in a given environment**.

The **Nimrod Safety Case** was prepared between the years 2001 and 2005. Reflecting the organizational changes and financial pressures outlined earlier, Nimrod Integrated Project Team – which carried the responsibility for the airworthiness of the Nimrods – outsourced the preparation of the Safety Case to industry partners. BAE Systems was the design authority for the Nimrods and was formally tasked with preparing the Nimrod Safety Case, whereas QinetiQ was supposed to provide an independent assessment of the Nimrod Safety Case to ensure that the assessment was up to the safety standards as outlined in military regulations.

The Nimrod Safety Case was implemented in **three phases** (Haddon-Cave, 2009, p. 189). The first phase took place between 2001 and 2003. Beginning with the scoping and formalization of the task, BAE Systems carried out zonal inspections of the Nimrods and produced a hazard identification report of the aircraft. The second phase (2003 – 2004) focused on hazard analysis and hazard mitigation, producing six written reports to the Nimrod Integrated Project Team. The third and final phase took place between 2004 and 2005, QinetiQ supported the sign-off of the task and the Nimrod Safety Case was declared satisfactorily completed by the Nimrod Integrated Project Team.

The Nimrod Safety Case had significant flaws that eventually played a major role in the XV230 accident. To begin with, the general attitude among Nimrod Integrated Project Team and BAE Systems seems to have been that the Nimrods are safe aircrafts and that the Safety Case is a mere formality done to comply with the regulations (Haddon-Cave, 2009, p. 263). The assessment itself was poorly implemented. The zonal inspections and hazard identification, carried out in the first phase of the Nimrod Safety Case, were superficial and lacking in detail (Haddon-Cave, 2009, p. 190). The final reports produced in the second phase contained numerous factual errors. Moreover, in the final reports, 70% of the hazards identified during the Nimrod Safety Case were marked as either ‘Open’ or ‘Unclassified’ with vague recommendations that further analyses were needed. These included the hazards that were implicated in the XV230 accident, whose risk was misclassified as ‘Tolerable’ whereas the evidence would have suggested otherwise (Haddon-Cave, 2009, p. 261). In his review, Haddon-Cave outlines in detail various problems in Nimrod Integrated Project Team’s and BAE Systems’ project management and competence in implementing the Safety Case.

Even though the Nimrod Safety Case was riddled with errors, a proper **independent safety review** could have identified the flaws and possibly prevented the succession of events that culminated in the fatal accident.

Nimrod Integrated Project Team leader was responsible for appointing an **Independent Safety Auditor** who would audit the compliance of the Nimrod Safety Case with the Nimrod safety management plan and carry out a technical evaluation of the Nimrod Safety Case (Haddon-

Cave, 2009, p. 318). Independent Safety Auditor would be responsible for producing an Audit Report to ensure that the Nimrod Safety Case satisfied the relevant military safety standards and regulations. An industry partner, QinetiQ, was tasked with auditing the safety analyses carried out by BAE Systems.

It can be argued that the **Nimrod Integrated Project Team was dependent on QinetiQ** to ensure that the Nimrod Safety Case was carried out properly. Nimrod Integrated Project Team leader was occupied with meeting financial objectives, and thus he delegated the majority of the project practicalities to an inexperienced safety manager who was, according to Haddon-Cave, out of his depth in the project (Haddon-Cave, 2009, p. 255). Thus, Nimrod Integrated Project Team lacked competence and resources in assessing BAE Systems' work itself.

Interestingly, **QinetiQ was never formally appointed as the Independent Safety Auditor of the Nimrod Safety Case**. In other words, no formal terms of reference or audit plans were agreed upon between Nimrod Integrated Project Team, BAE Systems and QinetiQ (Haddon-Cave, 2009, p. 318). QinetiQ was tasked to act merely as an independent advisor to the Nimrod Safety Case. In his review, Haddon-Cave suggested that the lack of formalization was due to a careless oversight of formalities, assumptions about the relationship having already been formalized, and reluctance by the Nimrod Integrated Project Team to have QinetiQ closely involved with the Nimrod Safety Case. Apparently, Nimrod Integrated Project Team leader and the safety manager had suspicious attitudes towards QinetiQ and their financial motivations. As QinetiQ was never formally tasked to be the Independent Safety Auditor, it was not required to produce a full Audit Report on the Nimrod Safety Case.

Despite the role ambiguity, the QinetiQ representatives were regularly involved in the Nimrod Safety Case proceedings; they attended the relevant project meetings, participated in the discussions concerning the processes and content of the Safety Case, and offered advice to Nimrod Integrated Project Team throughout the process (Haddon-Cave, 2009, p. 324). However, **QinetiQ failed to properly follow through that the advice they were giving were actually acted upon** (Haddon-Cave, 2009, p. 326). QinetiQ also failed to ensure that the hazard and risk assessments carried out by BAE Systems were based on sufficient and correct data and procedures during the Nimrod Safety Case preparation.

Another crucial independent assessment failure happened at the **Customer Acceptance Conference**, where BAE Systems presented the results of the Nimrod Safety Case at the end of Phase 2 of the project to demonstrate that the Safety Case was satisfactorily carried out. The QinetiQ representative who had been involved in the Nimrod Safety Case was unavailable at the last minute and thus the company sent his colleague to the Conference. Unfortunately, the colleague was not familiar with the project and had not been properly briefed before attending the meeting (Haddon-Cave, 2009, p. 326). Moreover, the colleague did not have access to the Phase 2 reports produced by BAE Systems on the Nimrod Safety Case. It is important to note that these reports contained numerous hazards whose status had been left as 'Open' or 'Unclassified', implying that there was insufficient information to complete the Nimrod Safety Case in good faith. In the interview carried out by Haddon-Cave during the preparation of the Nimrod review, the QinetiQ representative said that he had tried to inform the meeting attendees that he could not support the completion of the Nimrod Safety Case as he was only standing in and had not seen any of the relevant documents (Haddon-Cave, 2009, p. 327). He admitted succumbing to the pressure, however, describing that the mood in the meeting was clearly in favour of accepting the work. In other words, **QinetiQ supported the sign-off of the Nimrod Safety Case despite not having read any of the documents** describing the results of the work

carried out by BAE Systems. As such, clearly an independent assessment of the Nimrod Safety Case did not effectively take place.

Considering the suspicious attitudes towards QinetiQ in Nimrod Integrated Project Team, it is questionable how much **actual influence** QinetiQ could have had on the safety matters regarding the Nimrod Safety Case. One QinetiQ representative interviewed by Haddon-Cave commented on the influence of QinetiQ on Nimrod Integrated Project Team and BAE Systems by stating that "…we couldn't insist on them doing anything. We could only advise them." (Haddon-Cave, 2009, p. 330)

Another interesting tension in the relationship between Nimrod Integrated Project Team and QinetiQ is related to the **nature of independence between the entities**. QinetiQ, as a separate organization, was obviously culturally and administratively independent from Ministry of Defence. However, as a defence company, the Ministry was an important client, and the organization was financially dependent on Ministry. It seems that QinetiQ was eager to please the Ministry to ensure the continuity of future business (Haddon-Cave, 2009, p. 333). A QinetiQ representative who was interviewed by Haddon-Cave's team for the review had following to say about the nature of the relationship between QinetiQ and Integrated Project Teams (IPT):

> *"…In my view [QinetiQ project managers] were always stressed and on the back foot with the IPTs. This always seemed to stem from the fact that the IPTs had an inherent belief that QinetiQ were 'robbing them'. I felt that they went to extraordinary lengths to keep their IPT Leaders happy. I also felt that QinetiQ generally was on occasion prepared to modify its position for the same reason." (Haddon-Cave, 2009, p. 333)*

3.4 Enron scandal

3.4.1 Introduction

Enron was a Houston-based **energy, commodities and services company founded in 1985** after the merger of two energy companies, InterNorth and Houston Natural Gas (HNG). In the beginning, Enron specialized solely in the energy business, pursuing its vision of becoming the number one natural gas pipeline company in the USA. However, beginning from the late 1980s, Enron increasingly focused on **widening its operations** by focusing especially on growing its energy trading business and expanding its operations outside of the United States. The company saw multi-digit growth numbers on several years throughout the 1990s and it was hailed as a great innovator in the energy sector by the financial industry and the public at large. Despite the lavish and successful image the company presented outwards, its success was built upon **questionable accounting and finance practices** that veiled the poor actual financial performance of its operations. As Enron's businesses grew increasingly unsustainable, accelerated by several nationwide and organizational crises in the late 1990s and early 2000s, the company finally declared **bankruptcy in 2001**.

In the aftermath of the bankruptcy, attention was also turned to Enron's auditing firm **Arthur Andersen**. How was it possible that Andersen had allowed Enron's questionable financial practices to continue for so long?

Two insightful books, written with extensive contributions from insiders at Enron (Swartz & Watkins, 2003) and Arthur Andersen (Squires et al., 2003), serve to illuminate these questions in the following subchapters.

3.4.2 Background

Enron started as a **financially struggling natural gas pipeline company**. Despite being the largest natural gas company in the USA at the time and the owner of the second largest gas pipeline system after the merger of InterNorth and HNG, the company was **heavily in debt**, as InterNorth had paid a large premium when acquiring HNG (Swartz & Watkins, 2003, p. 30). Moreover, profits in the gas industry were rapidly diminishing because of a series of orders by the Federal Energy Regulatory Commission in 1984. These actions by the Commission were a consequence of a larger wave of deregulation in gas markets that was underway in the USA. Enron's CEO, Ken Lay, had pushed for deregulation of gas markets before taking the lead of the company, but he had not anticipated the unreliability of gas prices and supply that ensued from deregulation.

Lay knew he had to find ways to improve Enron's financial situation if the company was to survive. He sought **help from an external consulting company** and met a consultant called Jeff Skilling. Skilling's background was in the financial industry, and he proposed adopting practices from the finance sector to Enron's gas business. Lay liked Skilling's ideas and hired him to found and lead **Enron Gas Services**, a gas trading unit within Enron. Influenced by Skilling, Enron's business emphasis shifted from physical gas pipeline and power plant operations to a financial trading model applied to the energy sector. The move turned out to be lucrative and company finances improved.

In the early 1990s, the company adopted an accounting practice called **mark-to-market**, which was used in the financial sector but had not been used in the energy industry before Enron (Swartz & Watkins, 2003, p. 47). Mark-to-market practice allowed Enron to book unrealized future earnings at deal completion date. As a result, closing deals would improve the appearances of the company's financial performance even when no actual cash flow was generated from the deals. This mode of operation would work as long as the deals and projects would succeed in the future, which however proved to be challenging in the long run.

Enron's **high-energy and aggressive culture** supported mark-to-market accounting which required high trading volumes to keep booking profits. Enron's top executives, such as Lay and Skilling, encouraged creativity and risk-taking as long as it increased Enron's earnings (Swartz & Watkins, 2003, p. 102). As staff rewards were often tied to the stock price of the company, performance in the stock market became a high priority in organizational decision-making. Employee performance was evaluated by how much earnings people were bringing to Enron, which caused traders and finance personnel to regularly outperform employees working in the conventional pipeline or gas storage units (Swartz & Watkins, 2003, p. 60).

The main challenge with mark-to-market accounting was the **divergence of company's finances on the books and its actual cash flows**. Energy markets are inherently volatile. On several occasions, Enron's projected earnings failed to materialize because of either bad investments or global fluctuations in the energy prices (Swartz & Watkins, 2003, p. 110). Consequently, the company was regularly having issues with the scarcity of cash with which to fund its operations. To survive and grow its operations, Enron had to take on debt. However, the company had already been heavily in debt since its inception in 1985, and its credit rating was hindering its ability to borrow money from the banks.

In mid-1990s, the company's chief financial officer came up with the idea of using **special purpose entities (SPEs)** that helped Enron overcome the issues of cash scarcity and growth challenges (Swartz & Watkins, 2003, p. 63). SPEs were financial vehicles that were legally

separate entities from the main company. An SPE was legal as long as it fulfilled the following criteria: Enron could not own 100% of SPE stock, Enron could not control the SPE and Enron was not responsible for any loans or losses of the SPE (Squires et al., 2003, Chapter 1). Enron created SPEs by grouping specific assets and transferring them under an SPE. By doing so, the assets – and debts – were removed from Enron's main balance sheet and transferred to the SPEs (Swartz & Watkins, 2003, p. 63). Effectively, **Enron was hiding its debt** from its main balance sheets, and occasionally the company even booked profits from transferring assets to the SPEs that it created. As a result, Enron was able to expand its business without growing its debt in its main balance sheets, giving an illusion of healthy and strong financial performance and growth. It was later discovered that there were several SPEs that failed to fulfill the criteria that they were supposed to.

Enron's aggressive risk-taking culture, combined with dubious financial practices such as mark-to-market accounting and heavy use of SPEs, allowed the company to **soar and rise back from pushbacks** throughout the 1990s, while eventually creating the foundation for its failure. Although the seeds of Enron's downfall were especially sown by its accounting methods, the decline was accelerated by a few failed large investments internationally and failed attempts in expanding to the IT sector in late 1990s (Swartz & Watkins, 2003). Moreover, Enron's reputation was damaged especially by its role in exploiting the electricity crisis in California which increased public scrutiny into the details behind Enron's financial statements.

One consequence of increased attention to Enron was a Fortune magazine article that questioned Enron's stock price and raised the possibility of Enron being **overvalued**. This was followed by crude public remarks uttered by Jeff Skilling, which further contributed to Enron's weakening public reputation. In the summer of 2001, Skilling resigned abruptly from Enron. His resignation raised waves of suspicion in the public about the company's performance.

The final blows came in autumn 2001 when Enron reported **significant financial losses** and a statement that it had overstated its earnings for several years by almost 600 million USD. Around the same time, several articles exposing Enron's questionable use of SPE's came out in different financial magazines (Swartz & Watkins, 2003, pp. 305–306). Eventually, Securities and Exchange Commission (SEC), the US financial sector regulator, launched an official investigation into Enron. Enron's stock price crashed, and its credit rating plummeted, and the company was unable to complete its financial obligations. Enron filed for bankruptcy in December 2001, leaving thousands of employees without jobs and savings, as many had put their savings in Enron stock. Moreover, during the investigations carried out as part of the bankruptcy process, Department of Justice declared that Enron had committed **accounting fraud**.

3.4.3 Arthur Andersen's failures in auditing

Before the 1990s, Arthur Andersen had the reputation of being **one of the most respected accounting firms in the USA**. Founded in early 20th century, the firm became recognized in the field for providing faithful auditing for the shareholders instead of company executives (Swartz & Watkins, 2003, p. 94). However, **in the 1980s, the company was facing major challenges**. Auditing industry had changed with the advent of automated bookkeeping that allowed clients to manage their own accounting processes. Andersen's consulting business was continuously growing compared to its more traditional auditing business, whose revenue curves had flattened in the 1980s, and the auditors were facing pressure from internal competition to contribute to the company's bottom line (Squires et al., 2003, Chapter 5; Swartz & Watkins, 2003, p. 95). Andersen was also facing external competition as its competitors were becoming

bigger via ongoing mergers in the industry. Andersen's tough standards made it an unattractive firm for mergers (Swartz & Watkins, 2003, p. 94).

Organizational culture in Andersen shifted to a **strong sales culture as the company adapted to the internal and external pressures** (Squires et al., 2003, Chapter 6). The change had already started with the divergence of organizational cultures of the consulting and auditing divisions, the former being more sales-driven from the start. As the consulting division grew bigger, the hiring, training and retention strategies of auditing division also changed to form staff who was strong in bringing in and keeping clients. Moreover, Andersen's clients were themselves becoming increasingly risk-taking as a result of a wider deregulation of the business environment in the USA at the time (Squires et al., 2003, Chapter 10; Swartz & Watkins, 2003, p. 95). Traditional accounting values of stewardship and public trust slowly resided in the company, with emphasis shifting to pleasing clients to stay competitive. Power was transferred to local offices run by independent partners, which enabled increased complexity of operations and organizational structure, thus facilitating company growth. However, this also made the firm more **vulnerable to adverse actions** caused by rogue partners.

Ken Lay used Andersen's auditing services in InterNorth, and being a satisfied customer, he continued the business relationship after the merger and founding of Enron. Being its auditor, Andersen was responsible for making sure that Enron's accountants and financial officers were managing Enron's finances properly (Squires et al., 2003, Chapter 1). Over the years, the **relationship between the companies tightened**, as Andersen hired Enron's internal audit team when Enron outsourced the team to cut down on costs. Moreover, there was a regular flow of talent from Andersen to Enron, such as Rick Causey who moved to Enron and eventually became the company's chief accounting officer. Andersen also had their own floor in Enron headquarters. As Andersen was billing Enron about 1 million USD by mid-1990s, the business relationship was growing increasingly more enmeshed (Swartz & Watkins, 2003, p. 95).

Having Enron as a client raised **dissonance within Andersen**. David Duncan, who was the local partner responsible for Enron and Enron's chief accounting officer Rick Causey's friend and ex-colleague, received criticism in Andersen for being too inexperienced and timid when dealing with aggressive Enron executives and their intimidation tactics (Squires et al., 2003, Chapter 1). Andersen's internal Professional Standards Group had warned Duncan several times about the conflicts of interest in the use of SPE's in Enron. However, because of Andersen's management system that gave great decision-making power to local partners, Enron was kept as a client.

In the aftermath of Enron's bankruptcy, **Andersen was sued**. Initially, the company was accused of obstruction of justice because they had shredded documents related to Enron during the autumn of 2001, around the time of SEC investigations. Eventually, the shredded documents turned out to be largely unimportant and no criminal intent was found in the shredding. However, the court found an internal memo from an Andersen lawyer to Duncan which suggested an attempt to cover up Andersen's lenient standards in reviewing Enron's financial practices (Squires et al., 2003, Chapter 1). This was enough for the company to get convicted, and **Arthur Andersen collapsed along with Enron**. Andersen's downfall caused a crisis in the accounting industry and eventually led to the Sarbanes-Oxley Act (2002), which tightened the accounting rules around record keeping, imposed harsher penalties for violating regulations and clarified standards around maintaining auditor independence.

3.5 Tokaimura criticality incident

3.5.1 Event description

On September 30, 1999, a **criticality accident occurred at a uranium processing plant** operated by JCO Co., Ltd. (hereinafter referred to as JCO) in Tokai village, in Japan. The operation to produce uranyl nitrate solution was performed by three JCO workers. The government-approved procedure required the workers to dissolve uranium powder with added nitric acid in a dissolution tank. Instead of this procedure, they dissolved uranium powder in a 10-liter stainless steel bucket. In violation of the operation manual as well as of an approved procedure, they seem to have fed seven batches of uranyl nitrate solution into the precipitation tank which was designed to limit the mass to one batch, using a 5-liter stainless steel bucket and a funnel. Because of these actions, **the uranyl nitrate solution in the precipitation tank reached a criticality**. This criticality consisted of a very short period in the initial stage in which a large number of nuclear fission reactions took place and the later stage in which the fission reaction continued for approximately twenty hours. (Tsuchiya et al., 2002)

The accident resulted in **three JCO workers suffering acute radiation syndrome and two of them died within months**, and several workers and members of the public receiving radiation doses. Some 161 people were evacuated from within about 350 m of the facility, and some 310 000 people were advised to stay indoors for about 18 hours as a precautionary measure. The accident was essentially an 'irradiation' accident; it was not a 'contamination' accident as it did not result in a radiologically significant release of radioactive materials. (IAEA, 1999)

However, the accident had substantial **psychological and economic impacts** on the local population. News sources reported that JCO expects to pay at least $93 million in compensation to nearby residents and businesses (NRC, 2000). The compensation was not just due to evacuation and indoors shelter recommendations but the adverse effects like rapid fall of prices, boycotts of the agricultural and marine products in the whole region and the decline of tourism. (IAEA, 2000)

3.5.2 Contributing causes

IAEA report concluded that the accident at the nuclear fuel processing facility at Tokaimura seems to have resulted primarily from **human error and serious breaches of safety principles**, which together led to a criticality event. The accident was classified by the Japanese authorities as Level 4 on the IAEA International Nuclear Event Scale (INES), indicating an event without significant off-site risk. (IAEA, 1999)

Economical pressure as a root cause of the accident was evident. Within the year prior to the accident, profits dropped significantly because of competition, and JCO laid off about one third of its work force. After the layoff, JCO received an order for the 18.8 percent enriched specialty fuel, which is produced in small amounts on an infrequent basis, and the company was under pressure to meet the order schedule. (NRC, 2000) In addition, there were **implicit assumptions** both by the operators and by the regulatory authorities that such severe accidents could not happen and thus enough attention had not been paid to preparedness for the accidents (IAEA, 2000).

In the Tokaimura criticality accident **all four layers of oversight failed** (cf. WANO & IAEA, 2018). They either did not exist or were inadequate. At the first layer (individuals and work groups), the workers were not aware of the safety relevance of their work and there were no training nor qualification on the criticality hazards of their work. The second layer (management and supervision) failed because change management of the fuel process was lacking, and

management involvement was ineffective and insufficient. Management was also either ignorant or condoned operating outside licensed controls. (Tsuchiya et al., 2002)

The third layer of oversight, **independent internal oversight**, was also ineffective. The operational procedures used by the operators had **not been reviewed by the safety division** or the Japanese regulatory authorities to assure that they could be performed as written or that they would maintain the required criticality safety controls. For example, JCO made a revision of their operational procedure, which was internally reviewed by the manufacturing and quality assurance divisions, but it was not reviewed or approved by their safety management division. Apparently, there was no review and approval process provisions for verification and validation of procedures to assure that they could be performed as written and that the operators interpreted the procedural steps in a manner consistent with the plant's safety function. One of the reasons behind these choices was improving production efficiency. The failure to involve the safety management group chief and/or the chief technician of nuclear fuel in the review and approval process contributed to the degradation of independent internal oversight layer of oversight. (NRC, 2000; Tsuchiya et al., 2002)

There were historical roots for the failure of the internal oversight. The **reorganization** in 1992 weakened the internal oversight and a result, safety control manager served as quality control manager whose interest was more on customer satisfaction, and the safety committee lost jurisdiction over accident investigation. (Tsuchiya et al., 2001) Furthermore, also **deviations from the approved operating procedure** began to occur several years before the company developed the revised operating procedure for use. (NRC, 2000)

Furthermore, the fourth level of oversight (external oversight) failed because there was **no oversight by the Japanese nuclear industry**, which was mainly concerned with nuclear power generation and paid almost no attention to nuclear fuel conversion. The Japanese government had licensed this facility under the assumption that a nuclear criticality accident was impossible at the facility. There were no ongoing or periodic government inspections to ensure that there was no deviation from the approved procedure. (Tsuchiya et al., 2002)

The regulatory oversight program for the Tokaimura fuel processing facility failed to establish and maintain an **adequate safety margin**. The licensing review incorrectly concluded that there was "no possibility of criticality accident occurrence due to malfunction and other failures." Consequently, no criticality accident alarm was required or installed, and the facility was not included in the National Plan for the Prevention of Nuclear Disasters. This conclusion relied heavily on the use of administrative controls that were subject to human error. In addition, the lack of an independent inspection program resulted in the regulator not having an early indication of developing adverse performance trends and emerging problems at the facility. (NRC, 2000)

3.6 Key lessons learned for INSO

3.6.1 The importance of identifying and managing external pressures

Schedule pressures and financial constraints were a common denominator in all accident cases presented in this chapter.

In NASA's case, failure to meet externally induced deadlines threatened their funding, which was in any case declining after the Apollo mission years. The **external pressures faced by NASA did not change after the accidents, thus their culture did not really change**. This included continuing budget constraints of the Space Shuttle Program, efficiency pressures

related to International Space Station, treating the shuttles as "operational" (instead of R&D project) and management approach that emphasized production (Farjoun, 2005).

NASA's culture affected the possibility of the safety department to influence the decisions at NASA, but it did not give the safety department a possibility to influence the culture. Oversight must not be constrained only to overseeing the organization(s) directly involved in the work, but it must also take an active role in **making parties behind external pressures aware of their influence and prompt them to change their problematic behaviours appropriately**. For example, the NASA case describes well how difficult and ultimately doomed to fail were NASA's attempts to reach the very ambitious goals with a chronically insufficient funding and pressure to near-perpetual cost cutting. It is obvious that NASA and the people representing it were in no position to put a foot down when the White House made unreasonable demands. In other words, it is ineffective to blame NASA for its failure in communicating to the White House that it was being pressured to do things that were impossible. Such approach only adds stress to an already overstressed organization and its leadership.

Organizations that successfully operate complex, high-hazard systems must shield themselves from various forms of environmental competition to ensure reliable and safe operation; in NASA's case, achieving such a goal would have required redesigns of space vehicles and accepting higher costs, and consequently significant value shifts in its political and societal environment (Boin & Schulman, 2008). This means that **it is not only up to the organization alone to successfully operate the complex, high-hazard systems**. An analysis that focuses solely on the organization while ignoring its operating environment and the external pressures it must survive, misses a key component of safety.

In Boeing's case, the **competition with Airbus and pressure from the airlines** affected many key decisions, including the decision to redesign an old plane (Boeing 737) instead of going for a completely new design. Boeing also had a strong focus on shareholder value and stock prices, to the extent that they used more money for stock buybacks than R&D (Robison, 2021).

In the Tokaimura criticality accident in Japan, the economic pressures leading to the accident were clear. The company, JCO, faced a **significant drop in profits due to competition**, resulting in a one-third reduction in its workforce in the year before the incident. Subsequently, after the layoffs, the company received an order for 18.8 percent enriched specialty fuel, a product which is produced infrequently. Schedule pressures to meet the order contributed to continuing the nuclear fuel process in an unauthorized manner. (NRC, 2000)

Financial pressures also influence **independent safety auditors that are external to the organization of interest**, such as Arthur Andersen, Enron's auditor. Andersen's auditing branch was facing external financial pressures both from outside the organization in the form of increased competition between accounting firms, but also within the organization from the consulting branch of the company. Moreover, the same deregulation wave in the USA that was adding to the pressures was also contributing to Enron's ever-increasing risk taking in its operations. In other words, Andersen's auditing function was facing pressures from both its own operating environment and its client, and its responses to these pressures were the distribution of power to independent local partners and the shift of its culture to a sales culture. Both responses ultimately contributed to its failure in properly audit Enron. As a result, regulatory control of auditing was strengthened in the accounting industry in USA.

3.6.2 The importance of understanding the organizational core task and the life cycle of the system

NASA and Boeing 737 MAX accident examples show the importance of **understanding the sociotechnical system** that is managed. This includes the life cycle of the system, whether it is still in planning or development phase (e.g., construction and commissioning phases), an operational system, an aging system, or a system that is being decommissioned or phased out.

For example, NASA's Space Shuttle was characterized as "operational" even though it was basically an ongoing R&D project. Furthermore, the Space Shuttle fleet was aging, and this brought new challenges for maintenance that were not considered in safety analyses or budgeting.

In case of 737 MAX, Boeing did not sufficiently consider it as a development project, because they considered the previous versions of the aircraft already safe.

3.6.3 Balance between independence and influence

Failure to build a **centralized, independent yet sufficiently influential safety function** has been seen as a contributing factor in both Challenger and Columbia accidents (CAIB, 2003; Leveson et al., 2005). At Boeing, the independence of Authorized Representatives was also in question. The Authorized Representatives were aware and worried about many of the issues facing the Boeing 737 MAX development, but they did not share these concerns with the FAA, but rather kept them in the family, in Boeing.

Different **types of independence** can be identified: functional, financial, and cultural. **Functional independence** means that oversight is targeted at tasks the oversight function has not done, or contributed to, itself. This "functional oversight" can also be performed by senior managers or different types of technical and/or safety forums (see WANO & IAEA, 2018). However, functionally independent does not mean that the person or function is independent of the organization's other shared functions, such as rules, procedures, leadership, and culture. This means that functional independence needs to be supported by other types of independence. It can, and should be, a starting point for oversight, but not sufficient for a truly independent oversight.

Financial independence means that the financial survival or salary is not dependent on the function or organization that is being overseen. This type of independence is probably rare, and it was not realized in NASA, Boeing, or Enron. Rewarding systems can make financial independence even worse, if key performance indicators bring monetary rewards for oversight based on production related performance of the line organization.

Cultural independence means that the oversight targets a group or an organization that does not share the same assumptions, beliefs and values as the oversight group does. This is probably very rare form of independence and taken to the extreme would compromise the ability of the oversight function to make sense of their object of oversight. An example of problems associated with excessive cultural independence can be seen in the Nimrod accident. Members of Nimrod Integrated Project Team, a military organization, seemed to harbor suspicious attitudes towards QinetiQ, a commercial business, which led the former to maintain a distant relationship with the latter. This lack of trust and distance in the relationship was perceived by QinetiQ as a threat to future business, and it would facilitate QinetiQ's client pleasing efforts and lenience in auditing the Nimrod safety case, even though the company did understand the

topic of oversight and had successfully conducted Safety cases of other military platforms before.

Outsourcing the independent safety oversight to an external company is not a guarantee to ensure sufficient cultural independence. For example, it is probable that the culture of Enron's auditor Arthur Andersen became mixed with Enron's, because they had their own floor in the Enron headquarters and there was a regular transfer of employees especially from Andersen to Enron. Moreover, both companies had developed strong sales cultures.

A complete **lack of cultural independence** means that the oversight shares the same blind spots and potentially dysfunctional assumptions, beliefs, and routines as the function being overseen. The bigger and more value-cohesive the oversight function, the better its chances of building a strong identity (and cultural independence). The more the oversight function recruits externally (outside the company, but also outside nuclear), the more cultural independence it can build.

3.6.4 Taking organizational phenomena and time into account in organizing oversight

Oversight is subject to the **same "forces" that shape the line organization**, such as drift, normalization, and development of norms and assumptions. The forces may manifest differently depending on the degree of independence, but independence does not eliminate these naturally occurring organizational phenomena, it only changes their manifestation. In NASA's case, the institutional problems that were in effect at the time of the Challenger accident, and that had initially been addressed to some extent, had returned by the time of the Columbia accident (CAIB, 2003; Evans, 2021), showing a "gradual slide into disaster" (Vaughan, 2005, p. 42).

Organizational phenomena typically affect safety gradually. Thus, it is important to consider **temporal aspects** in organizational analysis. Oversight as it is planned and designed in the beginning of a life cycle of a sociotechnical system (or after a major transition) will be a different oversight to the one that develops as the system matures.

Rewarding can be considered an organizational phenomenon that both affects oversight, and one that internal oversight should monitor for its safety effects. At Boeing, senior management's rewards were dependent on short-term profits and stock prices, discouraging investments that took a long time to manifest as revenue (e.g., R&D, design of a new airplane). At the regulator (FAA), in turn, for some of its senior management, bonuses were dependent on Boeing meeting its schedules (Robison, 2021, p. 126).

3.6.5 The role of oversight in decision-making and issue identification

There are also several well-known mechanisms that affect **decision-making and communication** in organizations, such as confirmation bias, groupthink, structural secrecy (cf. Lee, 1993), or the influence of power on raising concerns. These issues affect oversight as well, but oversight should at the same time monitor how these issues manifest in the line organization.

The term "**structural secrecy**" refers to the way that organizational structure and information dependence obscures the seriousness of problems from people responsible for oversight (Vaughan, 1996, 2005). For example, in NASA, internal safety organization was dependent upon their parent organization for authority and funding, which resulted in personnel cuts in the safety organization, the inability of the safety department to conduct independent tests, and

safety-related information being withheld by NASA engineers if they did not consider it significant (Vaughan, 2005).

Similarly, the Authorized Representatives at Boeing could communicate directly with FAA only to "better understand a documented FAA method of compliance", which prevented the free communication of issues or concerns to the FAA. Boeing management served as a buffer for Authorized Representative's inquiries to FAA engineers to help "funnel information regarding certification issues to the FAA in a more effective and efficient manner" (Defazio & Larsen, 2020, pp. 67–68).

Another issue concerns the **type of problems** that the oversight focuses on. "Out-of-family" events as a focus for oversight at NASA led to familiar (or "in-family") issues being neglected. Both the O-ring corrosion (Challenger) and foam strikes (Columbia) were known phenomena, and as such they were not subject to increased attention by the safety organization. For example, the Columbia Accident Investigation Board (2003) noted that over time, foam strikes came to be considered an "in-family" event – or, "a reportable problem that was previously experienced, analyzed, and understood" rather than an "out-of-family" event, which was an "operation or performance outside the expected performance range for a given parameter or which has not previously been experienced" (CAIB, 2003, p. 122).

In addition, oversight function's ability to influence decision-making and issue identification in practice can be undermined by **leadership failures in the oversight function**. In Nimrod case, for QinetiQ (the provider of an independent assessment of the Nimrod Safety Case), a crucial mistake happened during the Customer Acceptance Conference. QinetiQ leader was unavailable at the last minute and sent an employee who was completely uninvolved with the project, who then went on to sign off the deliverables without having read the safety reports prepared by BAE Systems. Moreover, QinetiQ leadership had failed to officialize the auditing contract with Nimrod Integrated Project Team in the beginning of the project, which freed them from many laborious obligations but also weakened their ability to influence critical decisions in the project.

In the Enron scandal, the managing local partner responsible for overseeing the auditing of Enron failed to object to Enron's increasingly aggressive accounting practices and to protect his staff from intimidation tactics used by Enron executives on the Andersen employees. In other words, **strong commitment to integrity and willingness to face possible objections and conflicts from the overseen organization are crucial competencies** required from the leadership of the oversight function.

3.6.6 The challenge of being and staying relevant

Independence from the line activities and the mere number of technical details meant at both NASA and the FAA a challenge for the safety personnel to maintain the competence and to stay relevant. After the Boeing 737 MAX accidents it was noted that the regulators tended to focus on administrative issues and minor details instead of technical issues.

Oversight can **never have deep competence in everything**, which means that the line organization typically has more technical expertise (in most areas) than the oversight. The challenge for oversight is how to **add value and select the focus** so that all important areas are covered in sufficient detail.

3.6.7 Accident theories and oversight

The identification of lessons learned from the accident cases is **dependent on the source material, and especially on the models and theories utilized** in the source material. For example, the Columbia Accident Investigation Board relied heavily on the High Reliability Organization (HRO) theory. This decision was later criticized by some of the HRO theorists. For example, Boin and Schulman (2008, pp. 1053–1055) noted that HRO's exist in closely regulated environments, which force the organizations take reliability seriously, but this was not the case with NASA, which was driven by external, political and economic pressures.

Vaughan (2005), in turn, criticized the Challenger accident investigation (Presidential Commission on the Space Shuttle Challenger Accident, 1986) for its reliance on an individually focused human factors approach, that missed the cultural and external factors affecting the accident. This bias was reflected in the Commission's recommendations.

In contrast to the Challenger accident investigation report, the Columbia accident investigation report (CAIB, 2003) was a social analysis that explained how the layers of NASA's organizational system combined to cause this second accident. Still, Boin and Fishbacher-Smith (2011) argued that the conclusions of the Columbia accident investigation report would have been different if the investigation board had relied on the Normal Accident Theory instead of the HRO theory. They (Boin & Fishbacher-Smith, 2011, p. 84; see also Feldman, 2004) noted that "NASA had no proper procedures to identify and properly weigh signals of doubts, coming from respected engineers, which were not substantiated by engineering data".

Woods (2006), on the other hand, proposed that Resilience Engineering perspective could help accident investigation to move away from proximal events, human errors and vague root causes.

The cultural assumptions about expertise, knowledge, and safety can also be interpreted as forming an important element of an implicit accident model at NASA. This begs the questions: What are the accident models prevalent at the oversight function or department? What accident models have been utilized, implicitly or explicitly, in organizing oversight?

4 Independent Internal Nuclear Safety Oversight Globally

4.1 Methodology and dataset

Publicly available documentation was used to review how the INSO function has been implemented globally in the nuclear industry. The purpose of the review was not to gain a comprehensive overview of the INSO practices globally, but to find illustrative examples of different approaches to the INSO function. The following themes were sought from the documents: history and reason for introducing the INSO function, and goal, structure, and activities of the INSO function.

Nordic countries were excluded from this analysis because details of their INSO functions will be analysed as part of in-depth case studies in the second phase of NKS-R INSOLE activity.

Two approaches were used for data collection:

- Review of national reports in the framework of Convention on Nuclear Safety (CNS)
- Exploratory literature search from the scholarly databases (Scopus and Google Scholar) and the Internet (Google)

The Convention on Nuclear Safety (CNS) aims to commit contracting parties operating land-based civil nuclear power plants to maintain a high level of safety[4]. The parties submit reports on the implementation of their obligations for peer review meetings that are held periodically. The national reports are published publicly on the IAEA website, and/or on the websites of national nuclear authorities. The national CNS reports follow a defined structure, they include information concerning existing nuclear installations, legislative and regulatory framework, regulatory body, responsibility of the license holder, priority for safety, human factors, quality assurance and assessment and verification of safety, among many other topics. CNS review meetings also involve a Q&A procedure, which is reported in supplementary reports.

Countries with no operating power plants at the time of publishing the CNS meeting report were excluded. Reports from 26 countries[5] were examined. All newest national CNS reports (9th (2023) or 8th (2020) review meeting) were reviewed. The national reports and the Q&A supplements were searched for primary keywords: “independent oversight”, “INSO”, “nuclear safety oversight”, “oversight”, “independent”, and “committee”. The keyword search was also used to identify older documents with relevant content. In many national CNS reports, independent oversight arrangements were described under the article 9 (responsibility of the license holder) or article 10 (priority to safety). However, not all national CNS reports described nuclear power company specific independent oversight practices, and rather focused on regulatory oversight.

The exploratory literature search resulted in a diverse variety of publicly available materials such as OSART reports, conference papers and presentations, websites, reports, and program documents.

[4] https://www.iaea.org/topics/nuclear-safety-conventions/convention-nuclear-safety

[5] Argentina, Armenia, Belgium, Brazil, Bulgaria, Canada, China, Czech Republic, France, Hungary, India, Japan, Korea, Mexico, Netherlands, Pakistan, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Switzerland, Ukraine, United Kingdom, United States of America

The following chapter describes examples of INSO practices globally based on publicly available materials. It is acknowledged that the descriptions may not be up to date because the INSO functions are subject to continuous change and the publicly available information may not always reflect this change comprehensively. It is also acknowledged that some countries that have a large nuclear industry with many power companies are not represented or represented in a limited way (e.g., USA, China, Japan). This is due to a lack of public information about the companies' INSO practices or because the information was not available in a concentrated manner.

4.2 Examples of INSO practices globally

4.2.1 Argentina

Nucleoelectrica Argentina S.A. (NA-SA) is a state-owned company that operates all operational nuclear power plants in Argentina: Atucha (two reactors) and Embalse NPPs (one reactor).

NA-SA implemented an Independent Nuclear Oversight process in 2017 based on WANO and IAEA guidelines (ARN, 2022). Its object is to "promote excellence in the operation of nuclear power plants throughout the company and to provide the CNO [Chief Nuclear Officer], plant managers, corporate managers and the board of directors with a permanent perspective of the performance of nuclear power plants and corporate organization compared to the industry, focusing mainly on nuclear safety, plant reliability and emergency preparedness" (ARN, 2022, p. 17).

The Independent Nuclear Oversight has dedicated organisations at plant and corporate level. Their activities include daily activities at plant level, periodic reviews, escalation of plant issues, and tracking the completion of corrective actions (ARN, 2022).

Since 2021, NA-SA also has a Nuclear Safety Review Board. This function is implemented by senior staff and it provides NA-SA board of directors with a critical and external view on nuclear safety, nuclear safety culture, plant and corporate organizational performance, and independent oversight performance (ARN, 2022).

Argentina, Brazil, and Mexico cooperate in the Latin American peer review process "Lat-INOS" (for details, see subchapter 4.2.14 concerning international practices).

4.2.2 Belgium

ENGIE Electrabel operates Doel (four reactors) and Tihange (three reactors) NPPs.

The Independent Corporate Nuclear Safety Department started at corporate level in 2005. The INSO function is performed at three levels: Local INSO at sites, Corporate INSO, and an Independent Nuclear Safety Committee. (ENGIE Electrabel, 2016; FANC, 2022)

The Local INSO challenges daily operations at the plant, executes technical reviews, and independently analyses and approves safety assessments of modifications (FANC, 2022).

The objective of Corporate INSO is to deliver the operational line with a current perspective of the nuclear safety performance of the fleet. It conducts in-depth process reviews, independently analyses and approves safety assessments of modifications managed at corporate level, performs QA audits, and challenges line organization assessments (FANC, 2022).

The objective of Independent Nuclear Safety Committee (INSC) is to evaluate the nuclear safety performance and safety culture of ENGIE Electrabel. The committee consists of external members and members of the internal INSO. Its activities include the analysis of activities, events, projects, and processes with major impact on nuclear safety. The INSC reports to ENGIE Electrabel management team, the CEO, and Board of Directors. (FANC, 2022)

The INSO function also executes safety culture evaluations independent from the line organization's self-assessment (FANC, 2022).

4.2.3 Brazil

Eletrobras Eletronuclear S.A. operates Angra NPP (two reactors). The third unit is currently in construction phase.

Eletronuclear created Nuclear Safety Oversight Committee (COSIS) to do independent assessments of nuclear safety in 2014. This decision related to results from WANO corporate peer review in 2014, which highlighted that "senior leaders acknowledged that the monitoring and oversight organisation should use independent nuclear safety assessments more effectively" (CNEN, 2019, p. 106).

Eletronuclear has three safety committees: Plant Operation Review Committee at the plant level and Nuclear Operation Review Board reporting to Operations Directorate level. COSIS is the third and independent safety committee at Eletronuclear. It is established at the highest company level, comprising of representatives from all directorates. COSIS reports directly to company board. (CNEN, 2022) Its subject areas include plants safety performance, supply chain management, integrated management and main design modifications (CNEN, 2019). In practice, it conducts reviews of performance indicators and reported events, performance audits, plant safety reviews, and recommendations from the other safety committees, and it may set up working groups for investigations.

In 2021, the independent nuclear safety oversight function was further formally reinforced through organizational update. This involved the creation of Independent Nuclear Oversight Coordination, which performs activities such as observations and inspections in the field, and issuing reports and notifications relevant to nuclear safety (CNEN, 2022).

Argentina, Brazil, and Mexico cooperate in the Latin American peer review process "Lat-INOS" (for details, see subchapter 4.2.14 concerning international practices).

4.2.4 Canada

There are three licensee organizations in Canada with operating NPPs: Bruce Power (private corporation), Ontario Power Generation Inc. (OPG, owned by the province of Ontario), and New Brunswick Power Corporation (NB Power, a Crown corporation owned by the Government of New Brunswick) (Government of Canada, 2022). In total, there are 19 operating nuclear power reactors[6].

NB Power operates one nuclear power reactor: Point Lepreau NPP. It has an Independent Nuclear Oversight group (NOS), which "provides the organization with an ongoing perspective of performance, with a principal focus on nuclear safety, station reliability, and emergency response effectiveness". The NOS group conducts evaluations, investigations, audits, and

[6] https://pris.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=CA

assessments of performance, as well as internal compliance audits, surveillances, and functional area monitoring. Independent Nuclear Oversight is one of the executive processes of the plant's management system process model. The manager of Nuclear Oversight group reports to Chief Nuclear Officer. (NB Power, 2022)

In addition, NB Power has Nuclear Safety Review Board (NSRB) and Corporate Nuclear Oversight Team (CNOT), which provide external nuclear oversight. NSRB activities include providing Chief Nuclear Officer with an external assessment of activities at the plant; observe aspects related to safety, productivity, human performance, material condition, and reliability; report on the effectiveness of the nuclear oversight function; communicate with NB power personnel; provide advice on lessons learned; and provide recommendations to senior management. The CNOT activities include monitoring and oversight of the plant with the goals of ensuring long-term safe and reliable operation, ensuring that there are appropriate procedures developed and fully implemented (incl. nuclear safety, nuclear safety culture, risk identification and management, station reliability), receiving advice from corporate nuclear peers, ensuring consistency between processes and procedures used at the plant with external corporate policies and expectations, and participating in meetings on-site. (NB Power, 2022)

OPG operates NPPs at two sites: Darlington and Pickering. The Nuclear Oversight division conducts independent assessment of the nuclear management system to determine whether the established programs are being effectively implemented by the nuclear line organizations. The activities of the Nuclear Oversight division include implementing a 5-year audit plan, providing feedback to program owners through an onsite independent assessment group, and identifying performance deficiencies and reporting them. The effectiveness of Nuclear Oversight division itself is being assessed through independent assessments (e.g., Nuclear Industry Evaluation Program). (OPG, 2015, 2017)

Bruce Power operates two nuclear power stations (Bruce A and Bruce B) with four reactors each. Both stations are in the same overall site in Tiverton. At Bruce Power, Nuclear Oversight and Regulatory Affairs (NORA) division performs the INSO function. Its goal includes ensuring that "adverse conditions, incidents, and acts/practices/behaviours that represent substandard or non-conformance situations with regard to established quality requirements are identified, investigated, analysed and corrected" (Candesco, 2015, p. 70). The activities of NORA include preparing quarterly NORA oversight reviews covering audits and performance-based assessments, continuously reviewing the effectiveness of oversight against the WANO Performance Objectives and Criteria, and independently reviewing each area to provide independent advice on potential improvements (Candesco, 2015, 2017).

In addition to NORA, Bruce Power has implemented Nuclear Safety Review Board (NSRB), which reports directly to the Board of Directors on safety issues, performance, and culture. Its emphasis is on the long-term effort required to make permanent improvements in safety culture and leadership. NSRB members are independent of Bruce Power and are required to be experienced in matters of operational safety including. The NSRB also includes up to 10 non-voting members, including the President and CEO, and the Chief Nuclear Officer. Its activities include reviewing management safety reports, regulatory inspection reports, and internal audit reports, receiving briefings from staff and management, reviewing significant events, reviewing industry reports, and conducting plant tours, observations, and investigations. (Bruce Power, 2020)

All Canadian licensees with operating nuclear power plants have implemented a Nuclear Safety Review Board (NSRB) function to initiate regular, independent, external nuclear safety

assessments. The NSRB is a team of external industry experts that performs assessments (typically three to five days in duration) of NPP activities that might affect nuclear safety and performance. In OPG and NB Power, the NSRB reports to the Chief Nuclear Officer, while at Bruce Power it reports to the Board of Directors. (Government of Canada, 2022)

4.2.5 Czech Republic

ČEZ operates Dukovany (four reactors) and Temelin (two reactors) NPPs.

ČEZ has a three-level safety oversight: independent corporate level oversight, divisional oversight, and power plant level oversight. ČEZ established Independent Oversight Section in 2007 as part of quality management section. Corporate level independent oversight (IBS) was separated and moved into CEO's division in 2011. (IAEA, 2013)

IBS is a fully independent corporate level unit, which reports to the CEO and Board of Directors. The activities of IBS include oversight and feedback for strategic management with respect to safety, benchmarking, verifying management system functions for safety areas, monitoring events and activities, supporting and acting as secretariat for Corporate Safety Committee, preparing annual safety reports, monitoring and evaluating safety culture, and facilitating experience sharing and exchanging. IBS focuses on performance issues rather than compliance, with nuclear safety being its main focus. (IAEA, 2013)

4.2.6 France

Électricité de France (EDF) is a state-owned company that operates all French NPPs. As of 2023, there are 56 nuclear power reactors in operation and one under construction in France[7].

After Three Mile Island (1979) and St. Laurent A-2 (1980) accidents, and due to request from the government, in 1982 EDF established the General Inspectorate for Nuclear Safety and Security (IGSNR), which is an independent group level nuclear safety oversight function (EDF, 2021).

Overall, the independent safety oversight organization of EDF is called FIS (La Filière Indépendante de Sûreté). FIS operates at three levels: group, corporate, and plant level. (ASN, 2022).

IGSNR is the unit responsible for conducting independent oversight at EDF group level and across the whole group (incl. assets outside France). It consists of five independent members, of which Inspector General is from outside the EDF Group. IGSNR activities include field observations, meetings, interviews, inspections of plant and corporate FIS functions, participation in committees and preparing annual reports. The IGSNR reports directly to the CEO. IGSNR prepares annual reports which are submitted to CEO, EDF Board of Directors, the regulator, and made public. (IAEA, 2014)

Corporate level independent oversight consists of two units: Nuclear Safety Director and Nuclear Inspectorate. Nuclear Safety Director is supported by experts at corporate level. They conduct safety analyses, event cause analyses, and trends of safety indicator to challenge the operating organization. Nuclear Inspectorate performs regular independent assessments at sites

[7] https://pris.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=FR

and in corporate functions in a variety of areas, including operation, maintenance, engineering, chemistry, nuclear safety and site management, and safety culture. (IAEA, 2014)

At plant level the independent assessment is performed by Nuclear Safety Advisor who reports to corporate Nuclear Safety Director and Plant director. The Senior Nuclear Safety Advisor has authority to escalate safety issues to corporate level in case of disagreement with Plant Director. Plant level independent oversight activities include daily safety challenge meetings with shift supervisors, preparation of weekly reports, and participation in Technical Safety Operational Meetings and Operational Safety Committee. (IAEA, 2014)

FIS staff competences are maintained with a mobility program that ensures experience at more than one NPP, qualification requirements, structured training, and career path management between line management and independent assessment lines. (IAEA, 2014)

Finally, EDF also has Nuclear Safety Council (CSN) and Nuclear Safety and Operations Committee (CSNE). CSN is a platform to decide on strategically important safety issues at group level where Inspector General participates and has the authority to raise concerns (IAEA, 2014). CSNE is a platform at corporate level, which allows cross-cutting safety analysis of operating events with the participation of senior management of all the units (ASN, 2022).

4.2.7 Japan

Tokyo Electric Power Company (TEPCO) is the operator of Fukushima Daiichi, Fukushima Daini and Kashiwazaki-Kariwa NPPs. Fukushima Daiichi and Daini NPPs are currently permanently shut down and Kashiwazaki-Kariwa is in suspended operation[8].

In the aftermath of the Fukushima Daiichi disaster, TEPCO compiled a Nuclear Safety Reform Plan, with one of the measures being the establishment of Nuclear Safety Oversight Office (NSOO) (Kawano, 2016). NSOO was established in 2013 and it is responsible for overseeing the decommissioning of Fukushima Daiichi and Daini plants, and restarting of Kashiwazaki-Kariwa plants (WANO, 2021). In 2015, NSOO was reorganized to report directly to TEPCO president. The goal of NSOO is to monitor, offer advice to executives, and assist the Board of Directors in making decisions. It is led by a person outside TEPCO. (Kawano, 2016) For example, in 2017, the NSOO monitored the effectiveness of corrective actions for non-conformities, change management, design management, implementation of lessons learned, maintenance management, emergency preparedness, cooperation between headquarters and sites, human resource management, risk and management in all three sites (TEPCO, 2017, 2018).

4.2.8 Korea

Korea Hydro & Nuclear Power (KHNP) is the operator of all nuclear power plants in South Korea. There are a total of 25 nuclear power reactors in operation, three under construction and two in permanent shutdown in Korea[9].

KHNP implemented Nuclear Oversight (NOS) as a pilot program in 2016 and established it in 2017 as independent oversight function (NSSC, 2019). NOS "encourages improvement by observing major tests and jobs performed by plant employees including contractors, checking the compliance with safety related regulations and procedures, identifying areas for

[8] https://pris.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=JP

[9] https://pris.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=KR

improvement and providing feedback to the plant" (NSSC, 2019, p. 58). Organizationally it is located under the Head Office of KHNP (NSSC, 2019).

4.2.9 Romania

Societatea Nationala Nuclearelectrica, S.A. (SNN) is the operator of Cernavoda NPP (two reactors).

SNN formed an Independent Nuclear Safety Oversight group in 2016 according to a regulation on independent nuclear safety assessment[10]. At first, the group reported to Cernavoda NPP general manager, but after 2018, the group reported to the CEO of SNN. In 2022, the INSO function was extended to corporate level with a new group which has the oversight responsibility of the INSO activity. The main purpose of these groups is to ensure that nuclear safety is the overriding priority for the plant and for the corporation. (CNCAN, 2022a)

The procedures are the same for corporate and site level INSO function. The activities include of observations of meetings, field observations, and day-to-day assessments of plant performance. The oversight group prepares periodical reports to management of SNN and Cernavoda NPP, and conducts special proactive (e.g., decision-making, analysis of operational focus) and reactive reviews (e.g., analysis of unplanned shutdown events, root cause analyses).

4.2.10 Russian Federation

Rosenergoatom is the operator of all Russian NPPs. In Russian Federation, there are currently 37 nuclear power reactors in operation, three in construction and ten permanently shut down[11].

Rosenergoatom established an independent nuclear safety oversight service in 1997 after the enactment of Federal Law "On the use of atomic energy". Since 2000, the oversight service has been subordinate to the CEO and it is led by Inspector General. In 2006, plant-level inspection service was introduced with Plant Chief Inspector position, who reports to Plant Manager and Inspector General. After WANO Corporate Peer Review in 2011 and other international cooperation, the nuclear safety oversight service was changed to a process-based management model, more systematic plans and provisions were implemented, and assessment methodologies were improved. The nuclear safety oversight service conducts inspections of corporate-level departments and NPPs to assess the effectiveness of the implementation of Corporate Technical Policy and performance of the centralized safety functions. The service prepares corporate-level Inspector General's report and Plant Chief Inspector's reports for senior management. (Zonov, 2015)

4.2.11 Slovakia

Slovenské Elektrárne (SE) operates Bohunice and Mochovce NPPs. Two Bohunice units are in operation; three Mochovce units are in operation, and one is in construction[12].

SE established Independent Nuclear Oversight (NOS) function in 2007 (Slovenské Elektrárne, 2015). The mission of NOS is to "provide the Company's management with an independent evaluation of the performance in the operation of nuclear installations in order to identify areas for improvement in safety and reliability of nuclear installations, compared to the Company

[10] NSN-20, originally issued in 2015, revised in 2022 (CNCAN, 2022b)

[11] https://pris.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=RU

[12] https://pris.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=SK

management's goals and expectations and the best world practices in the nuclear sector" (Slovenské Elektrárne, 2023, p. 131). Its focus is nuclear safety, reliability, and efficiency of emergency response, but it also performs independent oversight of OHS and fire protection. NOS carries out independent analyses of selected operational events, monitors trends, conducts independent assessments of organizational changes, conducts inspections and prepares quarterly and annual reports. (Slovak Republic, 2022; Slovenské Elektrárne, 2023)

SE also has an external oversight body, Nuclear Safety Advisory Committee (NSAC), which assesses safety level and proposes solutions for complex safety-related issues. (Slovak Republic, 2022)

4.2.12 South Africa

Eskom is the operator of Koeberg NPP (two reactors).

Eskom has a corporate Nuclear Safety Assurance group (NSA) (previously Generation Nuclear Safety and Assurance group) operational since the 1990s (NNR, 2022). It provides independent safety assurance to the Chief Nuclear Officer. For example, the NSA group carries out independent safety assessments of design and operation and performs a comprehensive safety review jointly with Nuclear Licencing Group and QA every six months. The NSA group reports the results of its evaluations to oversight safety committees and directly to the Eskom Group Executive. The reporting encompasses all matters relevant to nuclear safety, including human factors aspects. (NNR, 2022)

4.2.13 United Kingdom

EDF Energy is the French state-owned operator of NPPs located in United Kingdom. It has nine operating nuclear power reactors and two in construction[13].

EDF Energy has implemented corporate and plant level Independent Nuclear Assurance (INA) teams. Plant level INA teams report directly to the corporate organization instead of the site management. The INA function reports to the Board of Directors and it has an independent reporting route to the EDF Group Inspector General for Nuclear Safety. (EDF, 2023; ONR, 2022)

INA has three evaluators based at each power station and the corporate team providing independent assessment of significant changes to plant safety case and support for fleet-wide corporate audits and inspections. Both teams prepare semi-annual report on nuclear safety, industrial safety, radiation protection and the environment for each site or the EDF Nuclear Generation executive team. Activities of the INA teams include regular meetings with the management, conducting assessments, analyses of non-conformities, and observations and discussions during outages. They are also invited to technical decision-making meetings to give an independent opinion. There are also independent oversight functions for all engineering and project divisions and functions, such as the Independent Nuclear Regulator (INR) at Hinkley Point C construction site. (EDF, 2023; ONR, 2022)

EDF Energy has also implemented Nuclear Safety Review Boards, which provide independent external advice and counsel to each station director and chief nuclear officer on issues related

[13] https://pris.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=GB

to nuclear safety. The board includes independent expert members with backgrounds from operating companies, regulator, or suppliers. (ONR, 2022)

4.2.14 International practices

WANO and IAEA provide peer support for implementing independent oversight. WANO and IAEA have published the guideline GL 2018-01 to support nuclear operators in developing and implementing their own independent oversight function (WANO & IAEA, 2018). WANO periodically arranges Independent Oversight Working Group meetings to help facilitate information exchange between licensees. IAEA examines independent oversight practices as part of their corporate OSART missions (IAEA, 2022a). In addition, the WANO and IAEA missions serve as an external, independent source of information which is used as part of the overall independent oversight framework in licensee power companies.

Latin American countries (Argentina, Brazil, and Mexico) have implemented a cooperation agreement since 2017 for the development of independent oversight called Lat-INOS (ARN, 2022). The objective of Lat-INOS is to "establish an external and independent control mechanism focused on safety, reliability, and emergency preparedness, and in non-exclusive way, in the functional, trans-functional, organizational, and corporate areas of the company" (ARN, 2022, p. 179). In practice, the group conducts peer review missions, which are reciprocal visits between the parties.

4.3 Summary

Nuclear power companies have introduced an INSO function in their organizations in **different times** and (seemingly) due to **different reasons**. Peer pressure from WANO or from the industry in general, regulatory requirements, or adverse events seem to have been the main drivers contributing to the implementation of INSO function.

The INSO functions are performed under **different labels**. One challenge in integrating the lessons learned from the INSO functions globally is recognizing when an organizational function is indeed an "INSO" function. There are also indications that existing organizational functions with similar task profile may be relabelled as "INSO" or their scope may be revised to meet industry expectations.

Typical **goals** of the INSO functions included ensuring nuclear safety and excellence, independently challenging the line organization, and providing information to senior management and board of directors. The INSO functions achieve this through assessments and observations, investigations, reviews and approvals, and providing advice. The INSO functions typically **report** to board of directors, CEO, and/or the Chief Nuclear Officer.

Implementing a **multi-level INSO structure** was common. It seems that the more complex the organization, the more levels of INSO were implemented. An example of a more complex INSO structure was the FIS of Électricité de France with three levels of INSO (group, corporate, and plant). Smaller companies usually implemented corporate INSO and plant level INSO.

In addition to the internal INSO function, many power companies have also implemented "**external INSO**", which is a safety commission or council with external experts. In some cases, power companies have agreed to cooperate to create a peer-type external INSO function between the companies (e.g., Lat-INOS is Latin America).

5 Formulation of Nordic Case Studies

5.1 Nordic cultural context

5.1.1 Introduction

The INSOLE study aims at developing a framework for independent nuclear oversight in the Nordic Countries, more specifically in Finland and Sweden. **Commonalities, but also differences between the national cultures** in these countries are of interest when it comes to nuclear safety and how to perform an effective oversight.

Geert Hofstede, who has made extensive studies of national culture, has described them in the six dimensions (see comparison between Finland and Sweden in Figure 2). The Hofstede national culture dimensions have a varying degree of effect on safety performance (Keiser, 2017; Mearns & Yule, 2009). The dimensions that have often been discussed in safety-critical contexts include power distance, individualism, motivation towards achievement and success, and uncertainty avoidance (e.g., Meshkati, 1998; Noort et al., 2016; Yorio et al., 2019).

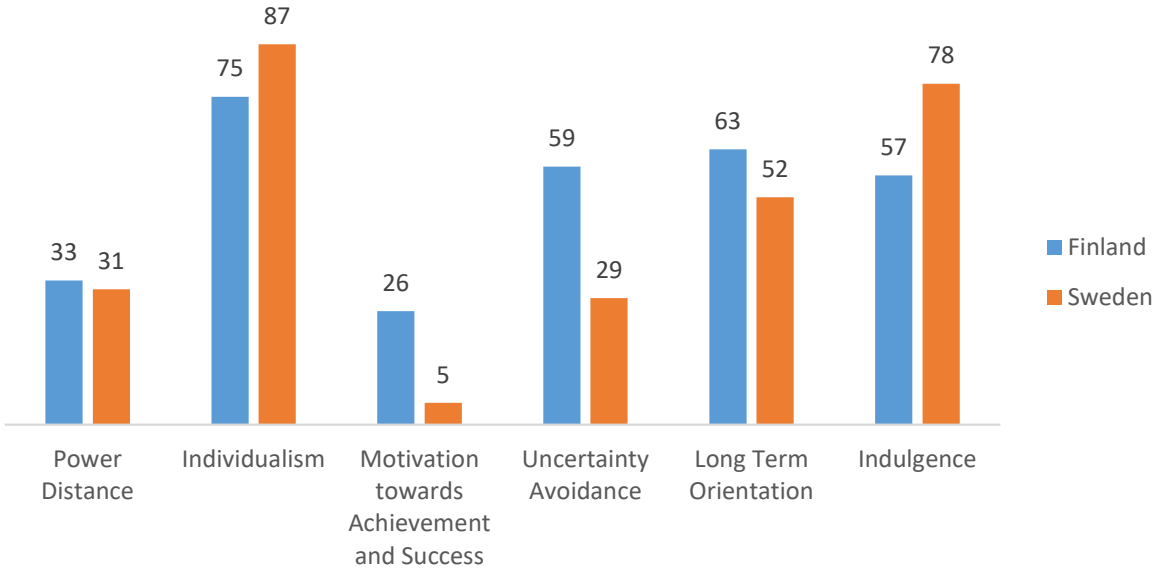

Figure 2. Comparison of Finland and Sweden based on Hofstede cultural dimensions (data source: https://www.hofstede-insights.com/country-comparison-tool)

The **Country Specific Safety Culture Forum** (CSSCF) was developed by the Nuclear Energy Agency (NEA) and the World Association of Nuclear Operators (WANO) to provide countries with a forum for dialogue and reflection on how the national culture attributes can influence nuclear safety culture. Information on national culture attributes were gathered and discussed in cooperation with participants from the nuclear regulators and from the licence holders in Sweden in 2018 (OECD NEA & WANO, 2018) and Finland in 2019 (OECD NEA & WANO, 2019).

The below subchapters describe the national culture dimensions that are most relevant from safety perspective and summarize the findings from the two CSSCF reports.

5.1.2 Power distance and Individualism

Finland and Sweden are both countries where **power is decentralised**, and **trust is a very strong value**. They are both **individualistic** countries where being independent is highly valued and **personal responsibility** is evident no matter the position or level in the organisational hierarchy. Relations between employees and managers are **informal**. The employees expect to be consulted and the managers trust that employees will perform according to the expectations.

The results from CSSCF studies reinforced the general characteristics that Hofstede describes. In both the Swedish and Finnish studies, freedom and trust were highlighted as important characteristics, even to the extent that control of work or performance can be perceived as mistrust by employees. In the Finnish study, trust was highlighted as a particularly strong value. It was mentioned that this could pose a risk if misused, for example, in association with people from other cultures.

5.1.3 Motivation towards achievement and success

This dimension deals with people's motivation. A high score (decisive) indicates competition, wanting to be the best, and a low score (consensus oriented) means liking what you do and caring for everyone.

Both Finland and Sweden score low in this dimension and belong to the so-called "**consensus societies**", where people strive for consensus and value equality and solidarity. It is not perceived as favourable to stand out from the crowd. Conflicts in these societies are resolved by **compromise and negotiation**.

In this dimension, Sweden stands out as the country that scores the lowest of all the countries in the world, resulting in traits that were specifically pointed out in the CSSCF report for Sweden. Swedish CSSCF report introduced the concepts of "Samskap" (Togetherness), a focus on conformity and getting along, and "Allskap" (Commonality), which means that everyone should be allowed to participate, and that no one should be left out. In the Swedish CSSCF report, the combination of these traits was highlighted as something that can complicate and delay decision-making.

5.1.4 Uncertainty avoidance

This dimension describes how a culture deals with the anxiety that comes from not knowing what the future brings and to what extent people feel threatened by ambiguous or unknown situations.

Finland scores high on the cultural dimension Uncertainty Avoidance. This implies an **emotional need for rules**. People have an inner urge to be busy and work hard. Precision and punctuality are the norm. Security is an important element in individual motivation. The Finnish CSSCF report highlighted that the need to be **efficient and solution-oriented** is a Finnish cultural characteristic. Finnish communication style was described as effective, i.e., straightforward and fact-based, without elements of personal expression. According to the Finnish CSSCF report, Finns are as keen as the Swedes to avoid conflicts, but Finns avoid conflicts mainly because it is not considered effective.

Sweden on the other hand has a very low preference for avoiding uncertainty. People show a **relaxed attitude where practice counts more than principles**. Swedes generally believe that there should be no more rules than necessary. Deviances from the norm is more easily tolerated, schedules are flexible, precision and punctuality do not come naturally. In Sweden hard work

is undertaken, when necessary, but not for its own sake. Participants in the focus groups of the Swedish CSSCF agreed that it is not a successful strategy to just give orders since people will not follow them blindly. **Sensemaking and shared understanding** were described as more successful ways to ensure that people will take the right action and get the work done.

5.2 Nordic regulatory frameworks

Statutory and regulatory requirements concerning the INSO function vary globally. WENRA Safety Reference Levels (WENRA, 2021) refer to qualified independent review function[14] and to independent assessments[15]. The implementation and resourcing of independent safety oversight and utilizing its insights are also stated as a recommendations in IAEA guidelines concerning the operating organizations for nuclear power plants (IAEA, 2022b)[16].

Current **Finnish regulatory framework** does not explicitly require the implementation of an INSO function. There are, however, requirements for independent group of experts to support the responsible manager (STUK, 2018)[17], safety unit independent of operational activities

[14] WENRA B2.2 The licensee shall ensure that decisions on safety matters are timely and preceded by appropriate investigation and consultation so that all relevant safety aspects are considered. Safety issues shall be subjected to appropriate safety review, by a suitably qualified independent review function.

[15] WENRA C5.1 The senior management shall ensure that:

- The adequacy and effectiveness of the management system is monitored and measured;
- Self-assessments and independent assessments are conducted regularly regarding:
    - the performance of work for which they are responsible,
    - leadership for safety, and
    - safety culture, including the underlying attitudes and behaviours.

WENRA C5.2 An organisational unit shall be established with the responsibility for conducting independent internal assessments. This unit shall have sufficient authority to discharge its responsibilities. Individuals conducting independent assessments shall not assess their own work.

[16] IAEA SSG-72 5.24. The operating organization should develop and effectively utilize independent oversight. The purpose of the independent oversight is to verify that the utility has the full capability to perform in a manner that achieves the safety goals through appropriate staffing, processes, activities, actions and monitoring. The independent oversight personnel should be sufficiently independent from the line organization to be capable of providing objective oversight not hindered by line reporting relationships. The independent safety oversight should pay specific attention to verifying that the plant management has taken measures with regard to changes in national regulations and international safety standards, operating experience, and new operating practices and technologies, and has implemented plant modifications as necessary. The independent safety oversight should have a direct reporting line to the senior management of the operating organization.

IAEA SSG-72 5.25. Senior management should provide the necessary resources to support the independent safety oversight function, and roles, responsibilities and expectations should be clearly established and documented. The effectiveness of independent safety oversight should be periodically evaluated.

IAEA SSG-72 5.26. Expertise from both inside and outside the operating organization should be used to support independent safety oversight activities, and individuals should have the necessary experience, training, skills and credibility to perform oversight activities.

IAEA SSG-72 5.30. The plant management should conduct regular performance reviews. Such reviews should involve the review and analysis of a wide variety of information and data, including the following: […] (f) Reports from independent safety oversight;

[17] STUK Y/1/2018 Chapter 6 Section 25 9. The licensee shall, as support for the responsible manager, have a group of experts, independent of the other parts of the organisation, convening on a regular basis to handle safety-related issues and giving recommendations thereon if necessary.

(STUK, 2019b)[18], and general requirements for independent assessments (STUK, 2019a)[19] and (independent) internal audits (STUK, 2019a)[20].

In **Sweden**, the nuclear power plants have implemented an organizational function whose task it is to perform independent oversight, as per SSMFS 2021:6 chapter 2, 3§[21] (SSM, 2021). Their purpose is to oversee that internal and external requirements regarding nuclear safety are fulfilled, but also to act as a driving force in the development of nuclear safety. This includes tasks such as independent safety review and performance-based oversight of targeted areas within reactor safety, radiation protection, physical protection, information- and IT-security, non-proliferation, emergency readiness preparation and daily operation. The function shall also have the necessary resources that the tasks require.

Oversight and safety assessment are also implemented as per SSMFS 2021:6 chapter 2, 21§ (SSM, 2021) in which the independent function could perform some parts, e.g., investigations regarding deviations and shortcomings.

According to SSMFS 2018:1 chapter 3, 7-9§[22] (SSM, 2018), the organization shall also have a function performing independent audits. These audits aim to systematically assess the organization with regards to implementation of the management system and its adequacy and effectiveness.

5.3 Areas of interest for the Nordic INSO

[18] YVL A.6 414. A safety unit independent of direct operational activities shall oversee the safety of the operational activities.

[19] YVL A.3 712. The management system shall include the requirements and procedures for regular, independent assessment of the system's conformity, performance, and effectiveness. Areas to be assessed in particular shall include the effectiveness of processes as regards the achievement of objectives and the realisation of the strategies and plans, the results of work performances and leadership, the organisation's safety culture, and the quality of products.

[20] YVL A.3 713. Internal audits may be conducted by a unit within the organisation with sufficient authority and independence for discharging its responsibilities. Individuals participating in independent assessments shall not assess work for which they are responsible and they shall have expertise related to the object of assessment. Procedures of standard ISO 19011 can be followed in auditing the management system.

[21] SSMFS 2021:6 2 kap. 3§ Fristående funktion för frågor om strålsäkerhet 3 § Det ska finnas en funktion som är direkt underställd högsta ledningen och som fristående från övrig verksamhet 1. har högsta ledningens stöd i att agera pådrivande för att strålsäkerheten ska utvecklas vid drift av kärnkraftsreaktorn, 2. bevakar att krav gällande strålsäkerhet efterlevs, 3. bevakar att nödvändig samordning sker mellan den egna organisationen och externa aktörer med uppgifter som vid krishantering har betydelse för strålsäkerheten, och 4. granskar kärnkraftsreaktorns konstruktion och drift med avseende på strålsäkerhet. Funktionen ska 1. ha de resurser som behövs för uppgiften, och 2. utgöra kontaktpunkt för Strålsäkerhetsmyndigheten. De som ingår i funktionen ska ha nödvändig kompetens och får inte samtidigt ha andra arbetsuppgifter av sådan art eller omfattning att det kan ifrågasättas om funktionen är fristående.

[22] SSMFS 2018:1 kap. 3, 7–9§ Intern revision 7 § Ledningssystemets tillämpning och ändamålsenlighet ska systematiskt och regelbundet granskas av en revisionsfunktion. Revisioner ska utgå ifrån ett revisionsprogram enligt 8 §, dokumenteras samt så långt som det är möjligt och rimligt genomföras på ett objektivt och opartiskt sätt. Revisionsfunktionen ska ha befogenhet att rapportera direkt till verksamhetens högsta ledning. 8 § Det ska finnas ett revisionsprogram där revisionsområden anges utifrån den betydelse som verksamhetens aktiviteter och eventuella processer har för strålsäkerheten. Revisionsområdena ska granskas minst vart tredje år eller med de kortare intervall som motiveras av deras betydelse för strålsäkerheten eller när särskilda behov av revision föreligger. 9 § Avvikelser som identifieras vid revision av ledningssystemet, ska värderas och hanteras så snart som det är möjligt. För åtgärder som beslutas med anledning av identifierade avvikelser ska ansvariga personer utses. Åtgärder som har vidtagits ska följas upp med avseende på uppnådd effekt.

5.3.1 *Introduction*

An important success factor for the NKS-R INSOLE implementation and to facilitate the development of the INSO functions in Nordic NPPs was to **create participation** from the licensees and to align the INSOLE activity with the activities and challenges of the Nordic licensees. Learning and development for the Nordic licensees will be optimized if the case studies are designed with their input. To achieve these goals, the Nordic case studies were designed to be **comparable and complementary**, which will enhance learning between the licensees in Finland and Sweden, and the case studies have **harmonized overall themes** (see below subchapters).

The main **data collection method** in the Nordic case studies is interviews with a diverse range of respondents, including INSO experts (managers and non-managers), functions being overseen (managers and non-managers), and functions that the INSO function reports to. Other data collection activities include document reviews (e.g., longitudinal study on historical developments of the INSO function), workshops with INSO experts, and focus groups on specific topics.

As shown in Figure 1 (the overall structure of NKS-R INSOLE project), the draft framework (chapter 6) and the lessons learned in organizational failure case studies (chapter 3) will be used as an input to the Nordic case studies. For example, we will use results from the accident case studies (e.g., lessons learned chapter 3.6) and theory integration as a basis for designing the case studies. The results from the Nordic case studies (lessons learned) will generate input to the final normative framework developed in the second phase of NKS-R INSOLE.

The research group had ongoing **discussions and preparatory meetings with the Nordic nuclear power companies** throughout the first year of the activity. At these meetings, we went through the project, its purpose, and goals. We described our plan for setting up the project. Further, we presented parts of our draft of the INSO framework. Based on this review, we asked the power companies what areas and topics that they would find interesting to study further in case studies next year. The licensees involved showed common interest in the **four themes** outlined in the next sections. Under each theme the research project has formulated examples of issues to explore. These themes were presented to and validated with the Nordic power companies.

5.3.2 *Theme 1: The role of INSO*

The first theme covers a variety of topics concerning the **role** of the INSO function. These topics related to how the INSO function is integrated into the activities of the organization.

A fundamental topic was the **understanding of and expectations** for the INSO function. This included how different bodies, such as the INSO members themselves, but also the line organization, the CEO, board, the regulator, etc., view the INSO function. An area of interest was that the different bodies might have different expectations and a different understanding of the INSO function, which might influence how the function is (or can be) implemented. This understanding and the expectations can also change over time and create threats or opportunities for the INSO function, especially amid organizational and strategy changes.

Independence from the line organization is one of the main defining characteristics of the INSO function and it also sparked interest among the licensee organization. Emerging topics of interest related to independence and dependence/involvement, that is, how to navigate between helping and supporting, and being an outsider. The effect of different types of independence

was also noted (functional, financial, and cultural), as well as how other organizational members perceive the independent role of INSO, and how this impacts the possibilities for the INSO function to operate.

5.3.3 Theme 2: Effectiveness of the INSO function

The second theme covers topics that relate to **defining and evaluating the effectiveness of the INSO function**.

What constitutes an effective INSO function may vary depending on the **perspective**. This is influenced by things such as the goals and expectations set for the INSO function, how they are used in evaluations, and what self- or external evaluation activities are used to assess them. The use of external parties (e.g., WANO, IAEA, and regulatory authorities) and their assessments to assess the effectiveness of the INSO function was also noted as an area of interest.

The **topics of assessment, and methods and review practices** used by the INSO function were also raised as an area of interest. For example, how to ensure that the INSO function is looking at the right things, and what things it should (and should not) be looking? In addition, an area of interest was the guidelines and instructions that are used as the basis for activities of the INSO function.

Level of detail in the oversight was another emerging topic when it comes to evaluating performance. This involves examining how detailed topics relate to overarching topics and to the overall picture, and when to look at topics at what level. An example of detailed topic might be task completion or requirement fulfillment. However, for effective INSO function, it is not sufficient to just verify that a task has been done or that requirements are fulfilled, as this might not provide an understanding of more overarching topics such as the organization's capacity for sustained safe operations. Indeed, it was highlighted that the line organization has better detailed view of issues, but INSO should have a wider perspective on the organization. It is also important to make the distinction between performance based and compliance-based oversight.

5.3.4 Theme 3: Long-term and recurring issues

The third theme covers topics relating to how the INSO function handles **long-term and recurring issues** in the organization. The challenge with long-term and recurring issues is that they may be difficult to identify because they are embedded in the organization's culture, and once they become known, they may be interpreted as inherent to the organization and thus become accepted and normalized. The INSO function may need a strategy to deal with these types of issues. For example, areas of interest included: What special procedures concerning communication, reporting or escalation should the INSO function adhere to when it identifies repeating issues? If identified problems are not solved, what procedure should the INSO function apply, and what escalation channels should it use? Another potential issue is that the recurrence of issues identified by the INSO function may have over time erode the strategy and activities of the INSO function itself and affect its strategy in terms of what the INSO considers valuable or useful to assess.

5.3.5 Theme 4: Cross-functional and organizational issues

The fourth theme covers themes that relate to cross-functional and organizational issues.

Organizational **power relations** between the INSO function and the rest of the organization came up as an area of interest. In particular, the difference between personal power and institutionalized power was highlighted. That is, what is the extent to which the role and power

of the INSO function is dependent on the personal attributes of its managers and personnel (or of the personal attributes of its stakeholders) rather than on the INSO as an organizational function? This may have implications on what are the ways in which the INSO function can have impact on decision-making (e.g., formal vs. informal escalation routes) and how changes can influence its power (e.g., organizational structure/process changes vs. personnel changes). Power relations also define the **mandate** of the INSO function, which affects its possibilities to carry out its tasks (incl. conditions such as competence and resources).

A related topic concerns the **interactions and communication** between the INSO function and the rest of the organization. One example area of interest related to how the views between the INSO function and the line organization are (or should be) handled when they diverge. Another area of interests were what kinds of forums of communication should/could the INSO function use to disseminate their findings, what should the balance between formal and informal communication channels be, and how to communicate in a way that the message is "heard" (i.e., communicating the right way to the right recipient). The relationship and division of responsibilities between different levels of INSO (plant and corporate) was highlighted as a specific type of interaction of interest.

6 Independent Nuclear Safety Oversight Framework (draft)

During the first phase of the project in 2023, a draft framework for independent nuclear safety oversight was developed. At this phase of the project, the framework is in "question-form", and it was used to guide data collection and analysis. In the next year of the activity, the draft framework will be finalized into a normative format ("answer-form") based on findings from case studies and all other research activities. The final normative framework will contain best practices and lessons learned.

The draft framework was iteratively developed in researcher workshops, and it is based on relevant scientific theories, literature review, as well as discussions with representatives from Nordic nuclear power companies. The draft framework contains four overall dimensions and several subcategories for each dimension (Figure 3). Each subcategory is associated with theories or models describing their content.

The following subchapters describe each of the four overall dimensions, the subcategories, as well as the reasoning behind their inclusion and content. The subcategories also contain example questions (in boxes). The example questions can be utilized for several purposes, including self-assessment of the INSO function, guiding the self-improvement of the INSO function, and external evaluation of the INSO function. In NKS-R INSOLE, they are used for designing the case studies and interviews.

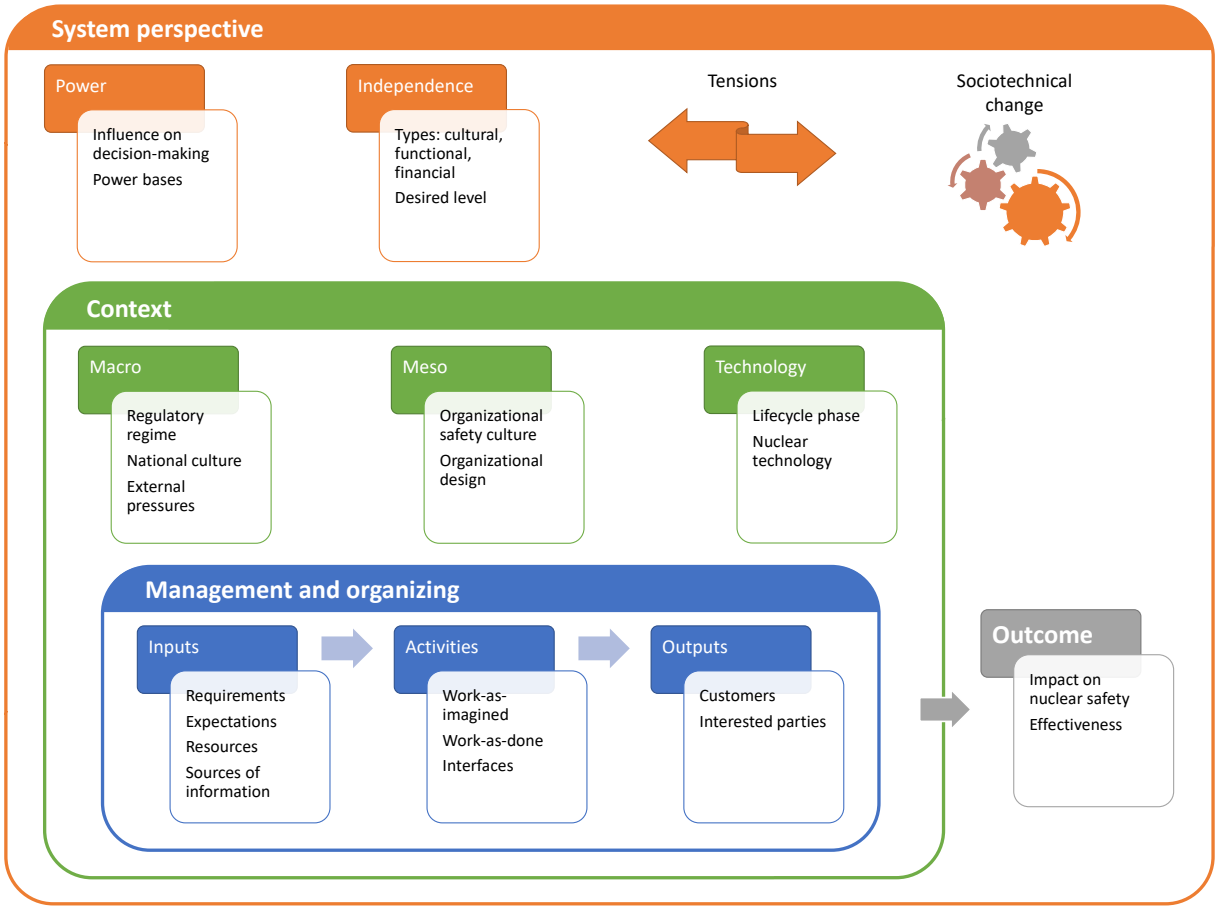

Figure 3. Overview of the draft independent nuclear safety oversight framework

6.1 Management and organizing

Management and organizing dimension is concerned with how the INSO function is organized, what is done within the framework of INSO, and how the INSO function interfaces with other organizational functions. As a guiding principle, we apply a process-based approach, which involves modelling the input, activities, and output of the INSO function (cf. ISO, 2015b).

6.1.1 Inputs

Typical **inputs** for process functions include statutory and regulatory requirements, industry standards, other expectations coming from within or outside the organization, resource provisions for implementing the function, and sources of information relevant to the function. The inputs are both the drivers facilitating the introduction of the INSO function, as well as factors enabling its implementation.

Requirements and standards concerning INSO globally and in the Nordic are reviewed in detail in chapter 5.2.

Example questions

What is the needed resource base for the INSO function and who is responsible for ensuring its availability?

What information sources the INSO function utilizes and how is it ensured that INSO has access to them?

How does the INSO function make sure that it does not only receive the information the line organization wants to deliver to INSO, or the information that the line organization considers relevant?

6.1.2 Activities

To model the INSO function **activities**, we apply the concepts of "work-as-imagined" (WAI) and "work-as-done" (WAD) (Hollnagel, 2015). WAI and WAD are used to distinguish between formal INSO arrangements from performed work and working practices. This distinction helps understand the gap between the prescribed ideals of processes and procedures, and the organizational reality, which is characterized by situational adaptation and tacit knowledge.

Examining the **formal INSO arrangements** includes the following topics:

- Roles, responsibilities, and authorities
- Organizational arrangements
- Formal reporting and escalation channels
- Competence model
- Information model / architecture
- Planned activities
- Tools and methods

Work-as-done approach directs attention towards the working practices, mindsets, values, and assumptions applied by the INSO function and its staff. This approach highlights the contextual, informal, and unwritten aspect of activities. They include:

- Leadership style within the INSO function
- Perception and application of the roles, responsibilities, and authorities of INSO
- Ways of implementing the INSO activities
- Reporting and communication style
- Information flows

Examples of INSO activities globally are described in detail in chapter 4.

Example questions

How is the INSO function organized currently and how has it been implemented in the past? What were the historical triggers or factors that still influence its implementation?

What activities does the INSO function perform and how?

What information does the INSO function collect and how does it analyse the information?

What escalation channels are used and how often?

How does the INSO function bring its observations forward? (E.g., is the communication style aggressive or negotiated, does the INSO function only highlight shortcomings or is there a more balanced review that highlights good practices?)

How does the INSO function monitor chronic issues in the organization?

How does the INSO function balance between monitoring old issues and identifying new issues?

How does the INSO function remain informed about technical issues, omissions, and worries in the organization? How does it assess their significance?

6.1.3 Interactions

Due to its integrative nature, the INSO function needs to be highly connected to other organizational functions and activities, while still retaining sufficient independence. The **interactions** to other organizational functions can be process inputs (provide something to INSO), outputs (get and/or expect something from INSO), or collaborative partners in implementing the INSO activities. Key stakeholders and interested parties related to the INSO function include:

- Board of directors
- Senior management at plant or corporate level

- Safety committees
- Other levels of INSO (corporate and plant level INSO)
- Other independent processes (e.g., QA, and external auditors and assessors)
- Line organization
- Regulator
- Supply chain
- Peers (other power plants)

The interactions with key stakeholders and interested parties can be influenced, for example, by how both parties perceive the roles, responsibilities, authorities, and activities of the INSO function. For example, WANO and IAEA (2018) emphasize that internal independent oversight should coordinate with organizational functions with similar tasks to avoid overlap, specifically QA.

Example descriptions of INSO reporting lines globally are described in chapter 4 and interactions of oversight functions with other stakeholders in accident case studies are described in chapter 3.

Example questions

How does the INSO function interact with its main stakeholders (board of directors and senior management)? How do these stakeholders interact with the INSO function? How does this affect the opportunities of the INSO function to bring up nuclear safety issues?

What demands, constraints or opportunities do interactions with other stakeholders and interested parties provide for the INSO function?

What information is exchanged with each key stakeholder? How does the INSO function utilize this information?

Which stakeholder interactions are effective, and which are not? Why?

How does the INSO function coordinate with non-independent (line) oversight?

How does the INSO function monitor how the organization monitors and cooperates with its supply chain?

6.2 Context

Like any other organizational function, INSO operates within the constraints of its operational environment and needs to be aligned with its **context** to be effective (ISO, 2015b). The context affects, for example, what are goals and activities of the INSO function, and what are the possibilities and limitations for implementing them. We have identified three types of contexts as relevant to the INSO function: macro-sociotechnical, meso-sociotechnical, and technological.

6.2.1 Macro-sociotechnical

The **macro-sociotechnical** context refers to the operational environment outside of the licensee organization. This includes regulatory regime, national culture, and external pressures from stakeholders outside of the operating organization.

Regulatory regimes can be characterized by various dimensions, including their prescriptiveness (detailed rules vs. broad goals), the extent to which the requirements are binding (strict command and control vs. self-regulation with voluntary acceptance), the role of regulator (expert vs. authority vs. public servant), prioritization of regulatory oversight (risk-based vs. rules-based), and regulator's proactiveness (monitoring compliance vs. capacity-building) (Hopkins, 2007; Reiman & Norros, 2002; Skotnes & Engen, 2015). The regulatory regime affects, for example, what is the role and significance of the INSO function in the overall "defence-in-depth" oversight structure – in particular, how the roles and responsibilities between the regulator and INSO are differentiated.

There are multiple frameworks to characterize differences in **national cultures**. A common framework is the Hofstede model, which distinguishes national cultures along the dimensions "power distance", "uncertainty avoidance", "individualism", "motivation towards achievement and success", "long-term vs. short-term orientation", and "indulgence vs. restraint" (Hofstede, 2011). These national culture dimensions have been associated with organizational safety culture and behavioural patterns (e.g., Yorio et al., 2019). For example, in high-power distance countries, hierarchy is strongly established and not questioned. This may mean that hierarchical position is valued over expertise in decision-making. Uncertainty avoidance refers to reliance on rules and procedures. National culture with high uncertainty avoidance may be less likely to adopt new ideas, while those with low uncertainty avoidance may be more likely to rely on individual excellence and situational adaptation rather than generalized rules and procedures.

National culture characteristics in the Nordic countries are further elaborated in chapter 5.1.

External pressures that organizations face include competition, owners' demands, transformations within the industry, etc. Competition was a factor affecting oversight in Boeing 737 MAX case described in chapter 3.1, and owner's demands was a factor in NASA case described in chapter 3.2. Competition was also a salient factor pushing Enron's auditor Arthur Andersen to adopt a sales culture and to value financial incentives and client pleasing above the protection of public interest, as described in chapter 3.4.

Example questions

What constraints and opportunities does the regulatory framework set for the INSO function? How does the INSO function take them into consideration?

How does the INSO function localize the generic, global best practice recommendations to its national and organizational context?

How does the INSO function consider the constraints, opportunities and demands of the local national culture when establishing its role and activities?

How does the INSO function consider (anticipate, monitor, or respond to) the effects of external environment and its pressures on the (licensee) organisation? What role does the INSO function take in mitigating external pressures, or in raising awareness of them?

How do external influences affect INSO? How does the INSO function consider (anticipate, monitor, or respond to) the effects of external pressures on its own activities?

6.2.2 Meso-sociotechnical

Meso-sociotechnical context refers to the operational environment within the licensee organization. The includes, for example, organizational (safety) culture and organizational design.

The impact of **organizational (safety) culture** on activities in nuclear organizations is well-established. The industry widely expects a good safety culture in all lifecycle phases (e.g., IAEA, 1991, 2016a). Organizational culture is a multi-level phenomenon consisting of behavioural, technological, and organizational artifacts, values, norms, beliefs, and assumptions (Guldenmund, 2000; Schein & Schein, 2016). It can be used as an approach to understand how taken-for-granted assumptions, beliefs and values influence safety-related behaviour and structures, and how they iteratively create and change each other (Reiman & Rollenhagen, 2018). Organizational culture is created over a period of time and its development may follow certain steps of maturity, which may range from pathological, bureaucratic to generative, or from emerging, managing, involving, cooperating to continuously improving (Goncalves Filho & Waterson, 2018; IAEA, 1998; Westrum, 2004). The implementation of INSO function is also affected by the organizational (safety) culture. INSO may face different possibilities or challenges depending on the maturity of the organizational culture, or how the organization and its leadership conceptualizes safety, values safety in relation to other goals, or appreciates independent viewpoint. Conversely, INSO may also have a role in facilitating the development of a good safety culture.

Organizational design refers to the formal aspects that are used to build and describe the organization, including its structure, management system and process structure. Common generic types of structural organizational configurations include simple structure with direct supervision, machine bureaucracy where work processes are standardized, professional bureaucracy where skills are standardized, division form where outputs are standardized and adhocracy, which is characterized by mutual adjustment (Mintzberg, 1979). Nuclear power companies are predominantly machine bureaucracies (Haber et al., 1991) but may also exhibit characteristics of other structural types. For example, companies with large fleets in different sites may be characterized as division forms where a central structure (“headquarters”) oversees multiple power plant sites (“divisions”). Organizations may also decide to include multiple

ways to group its activities and introduce a matrix structure. Management systems in the nuclear industry are expected to be process-based and integrated, and their content is largely guided by nuclear industry standards (e.g., IAEA, 2006, 2009, 2016a) as well as general quality management standards such as ISO 9001. Implementing the INSO function thus involves (at least) the consideration of existing (or planned) organizational configuration, reporting lines, and process structure.

Some examples of structuring of INSO functions are included in chapter 4.

Example questions

What is the role of INSO function in assessing and developing the (licensee) organization's safety culture? How does it cooperate and coordinate with the line organization's role in developing safety culture?

What constraints or opportunities does the (licensee) organization's (safety) culture set for the effective implementation of the INSO function? How does the INSO function consider these effects?

How does the INSO function monitor its own leadership and culture?

What is the position and structure of the INSO function in the (licensee) organization? If applicable, how do group, corporate, and plant level INSO functions interact and coordinate? What is their respective added value and role? How does the INSO structure enable or inhibit the monitoring and escalation of nuclear safety issues?

What is the division of labour between the INSO and other independent functions performing similar tasks such as Quality Assurance, Internal Audit, etc.? How and how well do these functions coordinate on nuclear safety issues?

6.2.3 Technological

Technological context refers to the nuclear technology applied by the licensee.

Nuclear power companies have this far applied only a handful of different **nuclear technologies** in their power plants. The most common reactor types used for commercial electricity production are PWR, PHWR, BWR, and LWGR[23]. They are implemented as single large power plant units, or as sites with multiple single large units. However, new nuclear technologies such as SMRs are in the process of being introduced. They may involve different organizational arrangements and new challenges for the INSO function compared to traditional large units.

Different approaches to INSO may also be necessary in nuclear facilities that are not nuclear power plants, such as research reactors, spent fuel storage facilities, uranium enrichment facilities, spent fuel reprocessing facilities, and waste management facilities.

[23] https://pris.iaea.org/PRIS/WorldStatistics/OperationalReactorsByType.aspx

Example questions

How does the INSO function consider the special characteristics of the nuclear technology applied by the nuclear facility it oversees?

How does the INSO function apply graded approach intelligently to ensure the right kind and extensiveness of oversight?

6.3 System perspective

We apply **sociotechnical systems theories** to gain a more profound and holistic understanding of the various phenomena affecting the implementation of the INSO function within the organizational reality. Interactions and interfaces between stakeholders and interested parties have already been discussed under the "Management and organizing" dimension. Here we focus on tensions, paradoxes and trade-offs, types of independence, power, and dynamics as factors that influence the implementation of the INSO function.

6.3.1 Tensions, paradoxes, and trade-offs

Tensions, paradoxes, and trade-offs are inherent characteristics in complex systems that successful organizations must balance. They have been described in many models. The competing values framework identifies two general tensions: internal focus and integration vs. external focus and differentiation, and flexibility and discretion vs. stability and control (Cameron & Quinn, 2006). Cameron and Quinn (2006) describe the resulting quadrants as follows: hierarchy culture (clear authorities, standardized rules and procedures, high control and accountability), market culture (customer-orientation, focus on competition and results), clan culture (shared values and goals, cohesion, participativeness, focus on teamwork) and adhocracy culture (temporary, specialized, dynamic, focus on innovation and reconfiguration). Competing values framework suggests that successful organizations integrate elements from all four quadrants into their culture in a balanced manner.

Further elaboration has identified four categories of organizational tensions or paradoxes: belonging (tensions between individual and collective and between competing values), organizing (collaboration and competition between designs and processes to achieve organizational goals), performing (tensions caused by plurality of stakeholders with differing demands), and learning (caused when the organization changes, renews and innovates) (Smith & Lewis, 2011). Responses to the paradoxes range between acceptance and resolution strategies (Smith & Lewis, 2011). Acceptance strategies are passive or proactive approaches that embrace the paradoxes as inherent and unsolvable traits and either avoid confronting them or use them as a source of performance improvement. Resolution strategies try to find ways to meet the competing demands, for example, through separation (allowing poles of the tension to exist in different organizational units or in different points of time), synthesis (seeking a common view), or metacommunication about the tensions.

In safety science, complexity theory has been applied to identify tensions related to safety management in complex systems (Reiman et al., 2015). They include responding to contingencies (systematic response to expected contingencies vs. capacity to flexibly respond to any contingency), disposition toward variability (command and control vs. self-organization), connections in the system (central prioritization vs. facilitation of interactions), and goals at different system levels (system goals vs. local goals). Reiman et al. (2015) summarize that in complex systems, safety management should have the capacity to apply all

of the seemingly contradictory safety management principles, instead of only focusing on a limited selection of them. This also applies to the implementation of the INSO function, with the special consideration that the INSO function must retain its independence.

Example questions

How does the INSO function identify different types of tensions, paradoxes, and trade-off existing in the organization and monitor their safety significance?

How does the INSO function ensure that its goals, activities, and organizational arrangements are defined and implemented in a balanced manner – so that one pole of a tension or trade-off is not overemphasized?

6.3.2 Type and level of independence

Independence is commonly conceptualized in **functional** terms. That is, it is defined as freedom from responsibility for the activity being audited (ISO, 2015a), or not participating in the work being assessed (IAEA, 2018). Due to independence being one of the primary distinguishing factors of the INSO function, it is relevant to examine the dimensions and prerequisites of independence in detail.

The factors affecting independence have been studied widely in the context of auditing and accounting. Common topics include the impact of auditors providing non-audit services, the level of auditor's ethical cognition, client importance and affiliation, auditor rotation, and audit firm's culture (Beattie & Fearnley, 2002; Masyitah, 2023; Tepalagul & Lin, 2015). A common issue has been the economic interests of auditing companies to provide additional services to auditees. This may create a **financial dependence** and may affect adversely the objectivity of the auditors (Masyitah, 2023). An example of the consequences can be seen in the case of Arthur Andersen and their client Enron, described more in detail in chapter 3.4. The INSO function in nuclear licensee organizations is also financially tied to its "customers" – the board of directors and/or the senior management. Their strategy concerning INSO affects the resource base (budget and people) available to the INSO function as well as the access to the organization's other resources such as information or cooperation.

Dependence can also be **cultural**. The INSO function – despite being functionally independent – is part of the same organization, has a common overall core task as other organizational functions, may have staff who worked previously in operational functions, and operates under the same management system and leadership. This means that there may be cultural values, beliefs or assumptions that are shared by INSO and the operating organization, including blind-spots and weaknesses which the INSO function might not be able to recognize due to being the member of the same organizational culture.

In addition to the type of independence, it is also worth examining the **desired level of independence** of the INSO function. A trade-off is made between involvement and independence (Woods, 2006). Too much emphasis on independence may cause the INSO function to be distant from the operation and lose an understanding of the realities of the operational organization, i.e., the object of oversight. It can also influence the extent to which the INSO can positively influence the organization. For example, positioning safety culture experts in the independent oversight function has been found to decrease possibilities for development and negatively affect trust and cooperation with the line organization (Viitanen et al., 2022).

Examples of losing independence in various accident cases are described in chapter 3.

Example questions

How does the INSO function remain sufficiently independent of the activities to avoid bias in judgment?

What type of independence do different INSO activities require?

How does the INSO function balance independence and involvement in its daily activities to remain aware of the challenges in the field?

How does the INSO function balance between being an outsider versus an insider?

6.3.3 Power

To have a positive impact on nuclear safety, the INSO function should have sufficient influence on decision-making. We examine this capacity to influence through the concept of social power. **Social power** is the ability of one social unit (individual, group, organization, or group of organizations) to influence the behaviour of another social unit (Rosenfeld & Wilson, 1999). Different types of power can be distinguished in organizational context. A widely-applied model identifies six bases of power (French & Raven, 1959; Raven, 1993): reward power (perceived ability to mediate rewards), coercive power (perceived ability to mediate punishments), legitimate power (perceived right to prescribe behaviour), referent power (identification with the other), expert power (perceived special knowledge or expertise), and informational power (controlling or possessing knowledge). All these power bases may be available to managers in the line organization, but due to the independent and expert-oriented nature of the INSO function, most power bases might not be available (or may not even be desirable) for the INSO function.

A more fine-grained examination of the **influence of safety professionals towards managers** reveals that the safety professionals utilize a variety of different tactics (Madigan et al., 2021). They include (in the order of most often used to least often used) rational persuasion (logical arguments, factual evidence), coalition (involving others to influence the manager), legitimating (calling on higher authority, legislation, rules), inspirational appeals (emotional appeals linking to manager's values), consultation (asking for input or suggestions), coaching (prompting the manager to think differently), collaboration (offering assistance), pressure (using threats or assertive behaviour), social proof (evidence that others are doing the same), and storytelling (narratives based on workplace experiences). These influence tactics are likely to be used also by the members of the INSO function.

It is also worth noting what is the **direction of the social power**. As discussed in previous subchapter regarding interfaces, the INSO function should be closely connected to other organizational functions, getting inputs, providing outputs, or collaborating with them. This means that in many cases, the INSO function is the object of social power. It is thus relevant to examine the complex power relations between the INSO function and other stakeholders or interested parties the INSO function interacts with.

Example questions

What is the power of the INSO function (e.g., its effect on decision-making)?

Where does the power of the INSO function come from? Does the power come from individual persons or from within the INSO function itself (e.g., organizational arrangements)?

Does the INSO function have an influence on the strategic choices of the company?

What power do other organizational functions have over the INSO function? How do they use it?

6.3.4 Sociotechnical change

Despite the nuclear industry being relatively stable, in practice it is also affected by many **sociotechnical changes**, some of which may permeate the whole sociotechnical system. Examples of sociotechnical changes include modifications to plant configuration, modernizations, lifecycle transitions, introduction of new nuclear technologies, organizational changes, sociotechnical aging (aging of technology, people, and organizations), and changes in regulatory requirements or regimes. All these examples are currently topical in the Nordic nuclear industry.

Nuclear power plant **lifecycle phases** include design/licensing, construction, commissioning, operating, and decommissioning. Each involve different organizational and cultural challenges. For example, pre-operational phases are characterized by uncertainty, large supply networks and complex interactions between parties with different mindsets, and long and abstract interrelation with nuclear safety; operational phase is characterized by routinization and sociotechnical aging; and decommissioning is characterized by changes in hazard profile, working practices and business model, and feelings of job insecurity and demotivation (Gotcheva & Oedewald, 2015a, 2015b; IAEA, 2012). While the generic goal of INSO as an independent oversight function may be the same in each lifecycle phase, the special characteristics of the lifecycle phases may need to be reflected in how the INSO function is implemented or what its focus areas are.

The INSO function has a **dual role during sociotechnical change**: first, the INSO function and the management needs to have the capacity to adapt the goal, activities, and interactions of the INSO function to the future state of the system, and secondly the INSO function has a role in overseeing that the change occurs in a way that nuclear safety is maintained. For both roles, the ability to proactively understand the organizational demands of sociotechnical changes is essential.

Examples of sociotechnical changes affecting the oversight function are described in chapter 3 (e.g., Boeing 737 MAX and NASA case studies).

Example questions

How does the INSO function consider the current and future lifecycle phase of the nuclear facility in its activities and organizational arrangements?

Does the INSO function change its focus when the organization (or the culture) it oversees changes or matures? How is the INSO function prepared to identify the need for this change in focus and implement it when needed?

How does the INSO function know which issues are really important, and how to maintain that awareness as time goes by?

What precautions does the INSO function take to avoid the drift and normalization phenomena that happens in the line organization over time?

6.4 Outcome

The ultimate goal and desired outcome of the INSO function is to help the licensee organization **maintain and improve its nuclear safety**. Establishing the relationship between the INSO function and a complex phenomenon such as nuclear safety is challenging and isolating its specific effects may not be a feasible target. Instead, we focus here on examining what nuclear safety is and what are the implications of different ways of characterizing nuclear safety for the implementation of INSO function. We then move forward to characterizing how the effectiveness of similar organizational functions is generally examined.

6.4.1 Nuclear safety

IAEA defines **nuclear safety** as "the achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation risks" (IAEA, 2018, p. 155). The main (technological) nuclear safety functions are control of reactivity, removal of decay heat and confinement of radioactivity and releases (IAEA, 2016b). Defence-in-depth is a guiding principle in the design of nuclear power plants and the concepts of diversity, redundance, physical separation and functional independence are applied on technical systems to ensure nuclear safety (IAEA, 2016b). Non-technical safety assurance approaches widely applied by the nuclear industry include HFE, human performance improvement, integrated management system, and leadership and safety culture.

Throughout the history of safety science, conceptualizing "safety" has been a challenging topic. Numerous competing yet complementary **safety or accident causation theories** have emerged and established themselves in safety-critical domains. They can be categorized to three groups based on their underlying assumptions of how accidents occur: simple linear models, complex linear models, and complex nonlinear or systemic models (Hollnagel & Goteman, 2004; Underwood & Waterson, 2013). Each have their advantages and disadvantages.

Simple linear models include event trees or networks that describe sequences of events that result in an accident. They are best suited for simple and technological systems. **Complex linear models** such as Swiss Cheese Model (Reason, 1997) introduce the idea of active failures and latent conditions which directs attention towards the more proximal human and organizational factors. Defence-in-depth principle is a variation of the linear categories.

Examples of **systemic models** include the sociotechnical model (Rasmussen, 1997), which sees safety as emerging from the interactions between actors from different levels of the sociotechnical system, Normal Accident Theory (Perrow, 1984), which sees accidents as resulting from a combination of tight coupling and high systemic complexity, High Reliability Organizations (Weick & Sutcliffe, 2015), which highlights the role of mindful organizations in ensuring safety performance, cultural theories, which describe the slow drift of practices, mindsets and assumptions as contributing to accidents (e.g., Turner, 1976; Vaughan, 1996), and Resilience Engineering (Dekker, 2003, 2011; Hollnagel, 2014; Hollnagel et al., 2006; Reiman et al., 2015), which directs attention to adaptations, systemic drift, trade-offs, proactiveness and capacity-building.

Each safety or accident causation theory presents a unique viewpoint to what is the role of the INSO function in ensuring safety, and what are the advantages and disadvantages of different ways of implementing the INSO function. For example, from the perspective of linear models INSO can be considered an additional barrier that prevents accident propagation. On the other hand, nonlinear models suggest that nothing is truly independent in sociotechnical systems and that the effectiveness of INSO can be adversely affected by increased complexity, dysfunctional organizational or cultural interactions, bias caused by knowledge of independent verification, etc. It is important for those who are implementing the INSO function to be aware of their assumptions about the nature of safety.

Examples of how the perspectives of different accident models were related to accidents and oversight are described in chapter 3.6.7.

Example questions

How does the INSO function define “nuclear safety”?

What phenomena does the INSO function consider as significant to nuclear safety? Does its understanding differ from the management’s or the line organization’s?

What safety or accident causation models are prevalent in the INSO function? Why?

What safety or accident causation models have been utilized (implicitly or explicitly) in organizing the INSO function or in implementing its activities?

How does the INSO function reflect the assumptions, blind spots, advantages and disadvantages of the safety or accident causation models it applies, or which are applied in the organization it oversees?

6.4.2 Effectiveness

Despite the primary goal of INSO being the independent oversight of nuclear safety in the license organization, as a formal organizational function, one of its tasks is the continuous assessment and improvement of its own **effectiveness**. Assessing and improving the effectiveness can be divided in two parts: process effectiveness and product effectiveness.

Process effectiveness may include the use of internal audits, self-assessments, and independent assessments to evaluate whether the INSO function is indeed functioning as planned and producing the output it is planned to produce. Such evaluations are often conducted by the QA department, or by external auditors.

Product effectiveness in this context refers to the ability of the INSO function to help the licensee organization maintain and improve its nuclear safety (cf. customer satisfaction in ISO 9001). This is a complex and nonlinear relationship and specific effects may be difficult to isolate. However, sometimes proxy measures, qualitative examination of change in the level of nuclear safety, comparison with assessments from other parties, or incident investigations may reveal insights concerning the functionality of the INSO function.

Example questions

How is the effectiveness of the INSO function observed or assessed? Who or what assesses it?

How does the INSO function itself view what is effective?

How does the INSO function continuously improve itself?

What other organizational functions or stakeholders are involved continuously improving the effectiveness of the INSO function?

7 Conclusions

The NKS-R INSOLE activity aimed to contribute to the development of independent internal nuclear safety oversight functions at Nordic nuclear power plants. This intermediate report described the findings from the first year of implementing the activity. It focused on studying how oversight has contributed to large-scale accidents and organizational failures, examining the different ways to organize and implement the INSO function in nuclear power companies, preparing for Nordic case studies, and developing a draft framework for internal nuclear safety oversight function in Nordic NPP context.

Five organizational failures in safety-critical industries where deficiencies in oversight were one of the contributing causes were examined to identify lessons learned for Nordic INSO. Key lessons learned from these failures related to identifying and managing external pressures, understanding the organizational core task and the life cycle of the system, balancing between independence and influence, taking (naturally occurring) organizational phenomena and time into account in organizing oversight, the role of oversight in decision-making and issue identification, the challenge of being and staying relevant, and acknowledging how the adopted safety or accident theories influence oversight.

Examples of INSO practices were reviewed in the global nuclear industry, in a total of thirteen non-Nordic countries. The INSO functions have been introduced in different times and due to different reasons, and under different labels. Their goals included ensuring nuclear safety and excellence, independently challenging the line organization, and providing information to senior management and board of directors.

Preparations for Nordic INSO case studies were described. This involved the identification of Finnish and Swedish cultural characteristics (differences and communalities), overview of the respective regulatory frameworks, and areas of interest for the Nordic INSO.

Finally, a draft version of the independent nuclear safety oversight framework was developed and used to guide data collection and analysis. It contains four overall dimensions (system perspective, context, management and organizing, and outcome), several subcategories for each dimension, and example questions for each subcategory. The example questions can be utilized, for example, in self-assessments of the INSO function, guiding the self-improvement of the INSO function, and external evaluation of the INSO function. The draft framework will be finalized into a normative format (contains best practices and lessons learned) in the next phase of the NKS-R INSOLE.

Acknowledgements

NKS conveys its gratitude to all organizations and persons who by means of financial support or contributions in kind have made the work presented in this report possible.

Disclaimer

The views expressed in this document remain the responsibility of the author(s) and do not necessarily reflect those of NKS. In particular, neither NKS nor any other organisation or body supporting NKS activities can be held responsible for the material presented in this report.

8 References

ARN. (2022). Argentinean National Report for the Convention on Nuclear Safety. Ninth Report. Autoridad Regulatoria Nuclear. Retrieved from https://www.argentina.gob.ar/sites/default/files/national_nuclear_safety_report_2022.pdf

ASN. (2022). National Report of France for the Combined 8th and 9th Review Meeting in 2023. Autorité de Sûreté Nucléaire.

Beattie, V., & Fearnley, S. (2002). Auditor Independence and Non-Audit Services: A Literature Review. London, UK: Institute of Chartered Accountants in England & Wales.

Boin, A., & Fishbacher-Smith, D. (2011). The importance of failure theories in assessing crisis management: The Columbia space shuttle disaster revisited. Policy and Society 30: 77–87. http://doi.org/10.1016/j.polsoc.2011.03.003

Boin, A., & Schulman, P. (2008). Assessing NASA's Safety Culture: The Limits and Possibilities of High-Reliability Theory. Public Administration Review 68: 1050–1062. http://doi.org/10.1111/j.1540-6210.2008.00954.x

Bruce Power. (2020). Application for the Amendment of the Power Reactor Operating Licence (No. BP-CORR-00531-00982). Retrieved from https://www.brucepower.com/wp-content/uploads/2021/01/BP-CORR-00531-00982.pdf

CAIB. (2003). Columbia Accident Investigation Board Report. Washington, DC: National Aeronautics and Space Administration.

Callahan, P. (2004, February 29). So why does Harry Stonecipher think he can turn around Boeing? Chicago Tribune. Retrieved from https://www.chicagotribune.com/chi-0402290256feb29-story.html

Cameron, K. S., & Quinn, R. E. (2006). Diagnosing and changing organizational culture: based on the competing values framework. Revised edition. San Francisco: Jossey-Bass.

Candesco. (2015). Safety Factor 10 - Organization and Administration (No. K-421231-00020-R00). Retrieved from https://www.brucepower.com/wp-content/uploads/2022/11/NK21-SFR-09701-00010.pdf

Candesco. (2017). Bruce A and B Global Assessment Report and Integrated Implementation Plan (No. K-421231-00217-R02).

Clearfield, C., & Tilcsik, A. (2018). Meltdown: Why Our Systems Fail and What We Can Do About It. New York, New York: Penguin Press.

CNCAN. (2022a). National Report under the Convention on Nuclear Safety. National Commission for Nuclear Activities Control. Retrieved from https://www.iaea.org/sites/default/files/22/08/romania_nr_9th_cns_.pdf

CNCAN. (2022b). NSN 20 - rev. 1 Normele privind politica de securitate nucleară şi evaluarea independentă a securităţii nucleare, aprobate prin Ordinul preşedintelui CNCAN nr. 212/25.10.2022 şi publicate în Monitorul Oficial, Partea I, nr. 1097 din data de 15 noiembrie

2022. Retrieved from http://www.cncan.ro/assets/NSN/2022/Ordin-nr.-212-din-25.10.2022-NSN-20-rev.-1.pdf

CNEN. (2019). Convention on Nuclear Safety Report by the Government of the Federal Republic of Brazil for the Eighth Review Meeting in March/April 2020. Comissão Nacional de Energia Nuclear.

CNEN. (2022). Convention on Nuclear Safety. Ninth National Report for the Joint Eighth and Ninth Review Meeting in March 2023. Comissão Nacional de Energia Nuclear.

Defazio, P. A., & Larsen, R. (2020). The Design, Development & Certification of the Boeing 737 MAX. Final Committee Report. The House Committee on Transportation & Infrastructure.

Dekker, S. (2003). Failure to adapt or adaptations that fail: contrasting models on procedures and safety. Applied Ergonomics 34: 233–238. http://doi.org/10.1016/S0003-6870(03)00031-0

Dekker, S. (2011). Drift into failure: from hunting broken components to understanding complex systems. Farnham; Burlington, VT: Ashgate.

Dunar, A. J., & Waring, S. P. (1999). Power to Explore. A History of Marshall Space Flight Center 1960-1990. Washington, DC: National Aeronautics and Space Administration NASA History Office Office of Policy and Plans. Retrieved from https://history.nasa.gov/SP-4313.pdf

EDF. (2021). Mémoires d'IGSN 1982 - 2020. Retrieved from https://igsnr.com/wp-content/uploads/2023/03/MEMOIRES-DIGSNR-1982-2020.pdf

EDF. (2023). The Inspector General's report on Nuclear Safety and Radiation Protection. 2022. Retrieved from https://igsnr.com/wp-content/uploads/2023/02/IGSNR-Report-2022.pdf

Edmondson, A. C., Roberto, M. A., Bohmer, R. M. J., Ferlins, E. M., & Feldman, L. R. (2005). The Recovery Window: Organizational Learning Following Ambiguous Threats. In W. H. Starbuck & M. Farjoun (Eds.), Organization at the limit: Lessons from the Columbia disaster. Blackwell.

ENGIE Electrabel. (2016). Use of ISOE for the assessment of the RP practices at ENGIE Electrabel. Presented at the ISOE International Symposium, Brussels, Belgium. Retrieved from https://www.isoe-network.net/publications/pub-proceedings/symposia-thematic/isoe-system/use-of-isoe-database-forum/3451-lance2016-ppt-1/file.html

Evans, B., 1976- author. (2021). The Space Shuttle: An Experiment Flying Machine: Thirty Years of Challenges. Cham: Springer. Retrieved from https://search.library.wisc.edu/catalog/9913300185102121

FANC. (2022). Kingdom of Belgium. Ninth Meeting of the Contracting Parties to the Convention on Nuclear Safety. National Report. Federal Agency for Nuclear Control.

Farjoun, M. (2005). History and Policy at the Space Shuttle Program. In W. H. Starbuck & M. Farjoun (Eds.), Organization at the Limit: Lessons from the Columbia Disaster. Blackwell.

Feldman, S. P. (2004). The Culture of Objectivity: Quantification, Uncertainty, and the Evaluation of Risk at NASA. Human Relations 57: 691–718. http://doi.org/10.1177/0018726704044952

French, J. R. P., & Raven, B. (1959). The Bases of Social Power. In D. Cartwright (Ed.), Studies in social power. pp. 150–167.

Goncalves Filho, A. P., & Waterson, P. (2018). Maturity models and safety culture: A critical review. Safety Science 105: 192–211. http://doi.org/10.1016/j.ssci.2018.02.017

Gotcheva, N., & Oedewald, P. (2015a). SafePhase: Safety culture challenges in design, construction, installation and commissioning phases of large nuclear power projects (Research No. 2015:10). Stockholm: Strålsäkerhetsmyndigheten. Retrieved from https://www.stralsakerhetsmyndigheten.se/contentassets/063308e909f1415498e2f3085488fbe9/201510-safephase-safety-culture-challenges-in-design-construction-installation-and-commissioning-phases-of-large-nuclear-power-projects

Gotcheva, N., & Oedewald, P. (2015b). Safety culture challenges in different lifecycle phases of nuclear power plants. In P. Oedewald, N. Gotcheva, K. Viitanen, & M. Wahlström (Eds.), Safety culture and organisational resilience in the nuclear industry throughout the different lifecycle phases. pp. 91–106. Espoo, Finland: VTT Technical Research Centre of Finland Ltd.

Gotcheva, N., & Ylönen, M. (2021). Regulatory lessons from accidents due to institutional failures: Boeing 737 MAX and Deepwater Horizon. VTT Technical Research Centre of Finland. Retrieved from https://cris.vtt.fi/en/publications/regulatory-lessons-from-accidents-due-to-institutional-failures-b

Government of Canada. (2022). Canadian National Report for the Convention on Nuclear Safety: Ninth Report. Retrieved from https://www.iaea.org/sites/default/files/23/03/canada_nr_9th_cns_and_presentation.pdf

Guldenmund, F. W. (2000). The nature of safety culture: a review of theory and research. Safety Science 34: 215–257. http://doi.org/10.1016/S0925-7535(00)00014-X

Haber, S. B., O'Brien, J. N., Metlay, D. S., & Crouch, D. A. (1991). Influence of Organizational Factors on Performance Reliability (No. NUREG/CR-5538).

Haddon-Cave, C. (2009). The Nimrod Review: an independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006. London: Stationery Office.

Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. Online Readings in Psychology and Culture 2. http://doi.org/10.9707/2307-0919.1014

Hollnagel, E. (2014). Safety-I and Safety–II: The Past and Future of Safety Management. Farnham, Surrey: Ashgate Publishing, Ltd.

Hollnagel, E. (2015). Why is Work-as-Imagined Different from Work-as-Done? In R. L. Wears, E. Hollnagel, & J. Braithwaite (Eds.), Resilient Health Care, Volume 2 The Resilience of Everyday Clinical Work. pp. 249–264. Farnham, Surrey, UK: Ashgate Publishing, Ltd.

Hollnagel, E., & Goteman, O. (2004). The functional resonance accident model. Proceedings of Cognitive System Engineering in Process Plant 2004: 155–161.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). Resilience engineering: Concepts and precepts. Aldershot, UK: Ashgate.

Hopkins, A. (2007). Beyond Compliance Monitoring: New Strategies for Safety Regulators. Law & Policy 29: 210–225. http://doi.org/10.1111/j.1467-9930.2007.00253.x

IAEA. (1991). INSAG-4. Safety Culture (No. 75- INSAG-4). Vienna, Austria: International Atomic Energy Agency.

IAEA. (1996). INSAG-10. Defence in Depth in Nuclear Safety. Vienna, Austria: International Atomic Energy Agency.

IAEA. (1998). Developing safety culture in nuclear activities: practical suggestions to assist progress. Vienna, Austria: International Atomic Energy Agency.

IAEA. (1999). Report on the Preliminary Fact Finding Mission Following the Accident at the Nuclear Fuel Processing Facility in Tokaimura, Japan. Vienna, Austria: International Atomic Energy Agency.

IAEA. (2000). Lessons Learned from the JCO Nuclear Criticality Accident in Japan in 1999. International Atomic Energy Agency. Retrieved from https://www-ns.iaea.org/downloads/iec/tokaimura-report.pdf

IAEA. (2006). Application of the Management System for Facilities and Activities (Safety Guide No. GS-G-3.1). Vienna, Austria: International Atomic Energy Agency.

IAEA. (2009). The Management System for Nuclear Installations (Safety Guide No. GS-G-3.5). Vienna, Austria: International Atomic Energy Agency.

IAEA. (2012). Safety culture in pre-operational phases of nuclear power plant projects. Vienna, Austria: International Atomic Energy Agency.

IAEA. (2013). Report of the Corporate Operational Safety Review Team (co-OSART) Mission to the ČEZ, A.s. Vienna, Austria: International Atomic Energy Agency. Retrieved from https://www.cez.cz/edee/content/file/pro-media-2014/04-duben/finreport-cez-osart-corporate-2013.pdf

IAEA. (2014). Report of the Corporate Operational Safety Review Team (OSART) Mission to EDF France. Vienna, Austria: International Atomic Energy Agency.

IAEA. (2016a). Leadership and Management for Safety (No. GSR Part 2). Vienna, Austria: International Atomic Energy Agency.

IAEA. (2016b). Safety of Nuclear Power Plants: Design. Vienna, Austria: International Atomic Energy Agency. Retrieved from http://public.eblib.com/choice/publicfullrecord.aspx?p=4853330

IAEA. (2018). IAEA Safety Glossary. Terminology Used in Nuclear Safety and Radiation Protection. 2018 Edition. Vienna, Austria: International Atomic Energy Agency.

IAEA. (2022a). Corporate OSART Guidelines (No. Services Series 47). Vienna, Austria: International Atomic Energy Agency. Retrieved from https://www-pub.iaea.org/MTCD/Publications/PDF/SVS-47web.pdf

IAEA. (2022b). The Operating Organization for Nuclear Power Plants (No. No. SSG-72). Vienna, Austria: International Atomic Energy Agency.

ISO. (2015a). ISO 9000: 2015 - Quality Management Systems. Fundamentals and Vocabulary. International Organization for Standardization.

ISO. (2015b). ISO 9001: 2015 - Quality Management Systems - Requirements. International Organization for Standardization.

Kawano, A. (2016). Progress in Tepco's Nuclear Safety Reform. p. 12. Presented at the Human and organizational aspects of assuring nuclear safety — exploring 30 years of safety culture.

Keiser, N. L. (2017, July 27). National Culture and Safety: A Meta-Analysis of the Relationships Between Hofstede's Cultural Value Dimensions and Workplace Safety Constructs (Thesis). Retrieved from https://oaktrust.library.tamu.edu/handle/1969.1/166023

KNKT. (2019). Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP. Final (No. KNKT.18.10.35.04). Komite Nasional Keselamatan Transportasi.

Kraft, C. (1995). Report of the Space Shuttle Management Independent Review Team. Retrieved from https://spp.fas.org/kraft.htm

Le Coze, J.-C. (2015). Reflecting on Jens Rasmussen's legacy. A strong program for a hard problem. Safety Science 71, Part B: 123–141. http://doi.org/10.1016/j.ssci.2014.03.015

Lee, F. (1993). Being Polite and Keeping MUM: How Bad News is Communicated in Organizational Hierarchies1. Journal of Applied Social Psychology 23: 1124–1149. http://doi.org/10.1111/j.1559-1816.1993.tb01025.x

Leveson, N. (2011). Engineering a safer world: systems thinking applied to safety. Cambridge, Mass: MIT Press.

Leveson, N., Cutcher-Gershenfeld, J., Carroll, J. S., Barrett, B., Brown, A., Dulac, N., & Marais, K. (2005). Systems Approaches to Safety: Nasa and the Space Shuttle Disasters. In W. H. Starbuck & M. Farjoun (Eds.), Organization at the Limit: Lessons from the Columbia Disaster. pp. 269–288. Blackwell.

Madigan, C., Johnstone, K., Way, K. A., & Capra, M. (2021). How do safety professionals' influence managers within organizations? – A critical incident approach. Safety Science 144: 105478. http://doi.org/10.1016/j.ssci.2021.105478

Masyitah, E. (2023). Literature Review on Auditor Independence. International Journal of Social Service and Research 3: 704–710. http://doi.org/10.46799/ijssr.v3i3.276

Mearns, K., & Yule, S. (2009). The role of national culture in determining safety performance: Challenges for the global oil and gas industry. Safety Science 47: 777–785. http://doi.org/10.1016/j.ssci.2008.01.009

Meshkati, N. (1998). The cultural context of nuclear safety culture: a conceptual model and field study. In J. Misumi, B. Wilpert, & R. Miller (Eds.), Nuclear Safety: A Human Factors Perspective. p. 8. CRC Press.

Mintzberg, H. (1979). The Structuring of Organizations. Englewood Cliffs, N.J: Pearson.

NASA. (2000). Space Shuttle Independent Assessment Team. Report to Associate Administrator. National Aeronautics and Space Administration. Retrieved from https://ntrs.nasa.gov/api/citations/20000032103/downloads/20000032103.pdf

NB Power. (2022). Application for the renewal of NB Power's licence for the Point Lepreau Nuclear Generating Station (No. CMD 22-H2.1). New Brunswick Power Corporation. Retrieved from https://www.nuclearsafety.gc.ca/eng/the-commission/hearings/cmd/pdf/CMD22/CMD22-H2-1.pdf

NNR. (2022). 9th National Report by South Africa on the Convention on Nuclear Safety. South African National Nuclear Regulator.

Noort, M. C., Reader, T. W., Shorrock, S., & Kirwan, B. (2016). The relationship between national culture and safety culture: Implications for international safety culture assessments. Journal of Occupational and Organizational Psychology 89: 515–538. http://doi.org/10.1111/joop.12139

NRC. (2000). NRC Review of the Tokai-Mura Criticality Accident. U. S. Nuclear Regulatory Commission.

NSSC. (2019). 8th National Report for the Convention on Nuclear Safety. Nuclear Safety and Security Commission. Retrieved from https://www.iaea.org/sites/default/files/national_report_of_the_republic_of_korea_for_the_8th_review_meeting.pdf

OECD NEA & WANO. (2018). Country-Specific Safety Culture Forum: Sweden. Nuclear Energy Agency.

OECD NEA & WANO. (2019). Country-Specific Safety Culture Forum: Finland. Nuclear Energy Agency.

Office of Inspector General. (2015). FAA Lacks an Effective Staffing Model and Risk-Based Oversight Process for Organization Designation Authorization (Audit Report No. AV-2016-001). U.S. Department of Transportation.

ONR. (2022). The United Kingdom's Ninth National Report on Compliance with the Convention on Nuclear Safety. Office for Nuclear Regulation.

OPG. (2015). OPG Written Submission in Support of the Renewal of Darlington's Power Reactor Operation Licence. Ontario Power Generation. Retrieved from https://archive.opg.com/pdf_archive/Nuclear%20Licencing%20Documents/Darlington%20Nuclear%20Operating%20Licence%20Renewal%20(2015)/OPG%20Submissions%20Related

%20to%20Renewal%20of%20Darlington%20Operating%20Licence/I040_WrittenSubmission_DarlingtonLicenceRenewal.pdf

OPG. (2017). Application for Renewal of Pickering Nuclear Generating Station Power Reactor Operating Licence. Ontario Power Generation. Retrieved from https://archive.opg.com/pdf_archive/Nuclear%20Licencing%20Documents/Pickering%20Nuclear%20Operating%20Licence%20Renewal%20(2018)/I017_P-CORR-00531-05055_PickeringNGS_Licence_Renewal.pdf

Perrow, C. (1984). Normal Accidents: Living with High Risk Technologies. United States of America: Princeton University Press.

Presidential Commission on the Space Shuttle Challenger Accident. (1986). Report to the President By the Presidential Commission on the Space Shuttle Challenger Accident (Rogers Commission Report) (No. Book 2).

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. Safety Science 27: 183–213. http://doi.org/10.1016/S0925-7535(97)00052-0

Raven, B. H. (1993). The Bases of Power: Origins and Recent Developments. Journal of Social Issues 49: 227–251. http://doi.org/10.1111/j.1540-4560.1993.tb01191.x

Reason, J. (1997). Managing the Risks of Organizational Accidents. 1 edition. Aldershot, Hants, England; Brookfield, Vt., USA: Ashgate.

Reason, J. (2000). Human error: models and management. British Medical Journal 320: 768–770.

Reiman, T., & Norros, L. (2002). Regulatory culture: balancing the different demands of regulatory practice in the nuclear industry. In B. Kirwan, A. R. Hale, & A. Hopkins (Eds.), Changing Regulation – Controlling Hazards in Society. pp. 175–192. New York: Pergamon.

Reiman, T., & Rollenhagen, C. (2018). Safety culture. In N. Moller, S. O. Hansson, J.-E. Holmberg, & C. Rollenhagen (Eds.), Handbook of Safety Principles. pp. 647–676. Hoboken: John Wiley & Sons.

Reiman, T., Rollenhagen, C., Pietikäinen, E., & Heikkilä, J. (2015). Principles of adaptive management in complex safety–critical organizations. Safety Science 71, Part B: 80–92. http://doi.org/10.1016/j.ssci.2014.07.021

Robison, P. (2021). Flying Blind: The 737 MAX Tragedy and the Fall of Boeing. New York: Doubleday.

Rodgers, E. (1996). Flying High: The Story of Boeing and the Rise of the Jetliner Industry. First Edition. New York, NY: Atlantic Monthly Pr.

Rosenfeld, R. H., & Wilson, D. C. (1999). Managing organizations: text, readings, and cases. 2nd ed. London: McGraw-Hill.

Sarbanes-Oxley Act of 2002, Pub. L. No. 107–204 (2002). Retrieved from https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf

Schein, E. H., & Schein, P. (2016). Organizational Culture and Leadership. 5. Edition. Wiley.

Serling, R. J. (1991). Legend & Legacy: The Story of Boeing and Its People. First Edition. New York: St Martins Pr.

Sgobba, T. (2019). B-737 MAX and the crash of the regulatory system. Journal of Space Safety Engineering 6: 299–303. http://doi.org/10.1016/j.jsse.2019.09.006

Skotnes, R. Ø., & Engen, O. A. (2015). Attitudes toward risk regulation – Prescriptive or functional regulation? Safety Science 77: 10–18. http://doi.org/10.1016/j.ssci.2015.03.008

Slovak Republic. (2022). National Report of the Slovak Republic. Compiled According to the Convention on Nuclear Safety.

Slovenské Elektrárne. (2015). Annual Report 2014. Retrieved from https://www.seas.sk/wp-content/uploads/2021/12/vyrocna-sprava-2014.pdf

Slovenské Elektrárne. (2023). Annual Report 2022. Retrieved from https://www.seas.sk/wp-content/uploads/2023/06/SEAS-2022-Annual-ReportFinancial-StatementsAuditors-Report.pdf

Smith, W., & Lewis, M. (2011). Toward A Theory of Paradox: A Dynamic Equilibrium Model of Organizing. The Academy of Management Review 36. http://doi.org/10.5465/AMR.2011.59330958

Squires, S. E., Smith, C. J., McDougall, L., & Yeack, W. R. (2003). Inside Arthur Andersen: Shifting Values, Unexpected Consequences. 1st edition. Upper Saddle River, N.J.: FT Press.

SSM. (2018). SSMFS 2018:1 Strålsäkerhetsmyndighetens föreskrifter om grundläggande bestämmelser för tillståndspliktig verksamhet med joniserande strålning. Retrieved from https://www.stralsakerhetsmyndigheten.se/contentassets/edd48d6fa0114e9cb3ae07f3956babcc/ssmfs-20181-stralsakerhetsmyndighetens-foreskrifter-om-grundlaggande-bestammelser-for-tillstandspliktig-verksamhet-med-joniserande-stralning-konsoliderad-version.pdf

SSM. (2021). SSMFS 2021:6 Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om drift av kärnkraftsreaktorer.

STUK. (2018). Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant. Helsinki, Finland: Säteilyturvakeskus.

STUK. (2019a). Guide YVL A.3 Leadership and management for safety. Helsinki, Finland: Säteilyturvakeskus.

STUK. (2019b). YVL A.6. Conduct of Operations at a Nuclear Power Plant. Helsinki, Finland.

Swartz, M., & Watkins, S. (2003). Power Failure: The Inside Story of the Collapse of Enron. 1st edition. New York, NY: Doubleday.

Tepalagul, N., & Lin, L. (2015). Auditor Independence and Audit Quality: A Literature Review. Journal of Accounting, Auditing & Finance 30: 101–121. http://doi.org/10.1177/0148558X14544505

TEPCO. (2017). Nuclear Safety Reform Plan FY2017Q2 Progress Report. Tokyo Electric Power Company Holdings, Inc.

TEPCO. (2018). Nuclear Safety Reform Plan FY2017Q4 Progress Report. Tokyo Electric Power Company Holdings, Inc.

Tsuchiya, S., Ito, K., & Sato, M. (2002). High-leverage changes to improve safety culture: A systemic analysis of major organizational accidents. Retrieved from https://proceedings.systemdynamics.org/2002/proceed/papers/Tsuchiy1.pdf

Tsuchiya, S., Tanabe, A., Narushima, T., Ito, K., & Yamazaki, K. (2001). An analysis of Tokaimura nuclear criticality accident: A systems approach. Presented at the The 19th International Conference of the System Dynamics Society, System Dynamics Society, Atlanta, Georgia.

Turner, B. A. (1976). The Organizational and Interorganizational Development of Disasters. Administrative Science Quarterly 21: 378–397. http://doi.org/10.2307/2391850

Underwood, P., & Waterson, P. (2013). Accident Analysis Models and Methods: Guidance for Safety Professionals. Loughborough University.

Vaughan, D. (1996). The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. Chicago: University of Chicago Press.

Vaughan, D. (2005). System Effects: On Slippery Slopes, Repeating Negative Patterns, and Learning from Mistake? In W. H. Starbuck & M. Farjoun (Eds.), Organization at the Limit: Lessons from the Columbia Disaster. pp. 41–59. Blackwell.

Viitanen, K., Airola, M., & Gotcheva, N. (2022). Effective Improvement of Leadership and Safety Culture – Intermediate Report. Espoo, Finland: VTT Technical Research Centre of Finland. Retrieved from https://cris.vtt.fi/en/publications/effective-improvement-of-leadership-and-safety-culture-intermedia

WANO. (2021). TEPCO strengthens its independent nuclear safety oversight. Retrieved 16 November 2023, from https://www.wano.info/news-events/inside-wano/member-story/tepco-s-strengthens-its-independent-nuclear-safety

WANO & IAEA. (2018). Independent Oversight (No. GL 2018-01). World Association of Nuclear Operators.

Weick, K. E., & Sutcliffe, K. M. (2015). Managing the Unexpected: Resilient Performance in an Age of Uncertainty. Third Edition. Hoboken, New Jersey: John Wiley & Sons.

WENRA. (2021). Safety Reference Levels for Existing Reactors 2020. Western European Nuclear Regulators Association.

Westrum, R. (2004). A typology of organisational cultures. Quality and Safety in Health Care 13: ii22–ii27. http://doi.org/10.1136/qshc.2003.009522

Woods, D. D. (2006). How to Design a Safety Organization: Test Case for Resilience Engineering. In D. D. Woods, E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), Resilience

Engineering: Concepts and Precepts. 1st ed., pp. 315–325. CRC Press. http://doi.org/10.1201/9781315605685-26

Yorio, P. L., Edwards, J., & Hoeneveld, D. (2019). Safety culture across cultures. Safety Science 120: 402–410. http://doi.org/10.1016/j.ssci.2019.07.021

Zonov, I. (2015). Experience with Functioning and Development of the Nuclear Safety Oversight Serivce in Rosenergoatom. p. 3. Presented at the International Conference on Operational Safety, Vienna, Austria.

Bibliographic Data Sheet **NKS-482**

Title	Internal nuclear safety oversight as part of organizational defence-in-depth – Lessons learned for the Nordic nuclear industry Intermediate report from the NKS-R INSOLE activity
Author(s)	Kaupo Viitanen[1] Teemu Reiman[2] Sami Karadeniz[1], Merja Airola[1] Fredrik Jakobsson[3], Carin Sylvander[3], Sara Lind[3]
Affiliation(s)	[1]VTT Technical Research Centre of Finland Ltd [2]Lilikoi [3]Risk Pilot AB
ISBN	978-87-7893-578-6
Date	January 2024
Project	NKS-R / INSOLE
No. of pages	74
No. of tables	0
No. of illustrations	3
No. of references	130
Abstract max. 2000 characters	The NKS-R INSOLE activity aimed to contribute to the development of independent internal nuclear safety oversight functions at Nordic nuclear power plants. This intermediate report describes the findings from the first year of implementing the activity. Five organizational failures in safety-critical industries where deficiencies in oversight were one of the contributing causes were examined to identify lessons learned for Nordic INSO. Examples of INSO practices were reviewed in the global nuclear industry. The INSO functions have been introduced in different times and due to different reasons, and under different labels. Their goals included ensuring nuclear safety and excellence, independently challenging the line organization, and providing information to senior management and board of directors. Preparations for Nordic INSO case studies were described. This involved the identification of Finnish and Swedish cultural characteristics, overview of the respective regulatory frameworks, and areas of interest for the Nordic INSO. Finally, a draft version of the independent nuclear safety oversight framework was developed and used to guide data collection and analysis. It contains four overall dimensions (system perspective, context, management and organizing, and outcome), several subcategories for each dimension, and example questions for each subcategory, which can be utilized, for example, in self-assessments of the INSO function, guiding the self-improvement of the INSO function, and external evaluation of the INSO function.
Key words	independent oversight, internal oversight, nuclear safety, INSO