The 15th International Congress of the International Radiation Protection Association

A framework to understand and model the dynamics of safety management in the operation of a nuclear reactor.

Gregorio Acuña[1*], Marcelo Oscar Giménez[1,2], Marcelo Caputo[1,2], Marisa Sánchez[3]

[1] *National Atomic Energy Commission, Bariloche, 8400, Argentina*
[2] *Balseiro Institute, National University of Cuyo, Bariloche 8400, Argentina.*
[3] *National University of the South, Bahía Blanca 8000, Argentina.*
*Corresponding author's e-mail: gregorioacuna@cab.cnea.gov.ar

Abstract. This work aims to present the basis of a framework to understand and then be able to model the management of safety in the operation of a nuclear reactor from a systems perspective. Method: Bibliographic review, use of the inductive and deductive method, and analytical reduction to the root causes of the main nuclear accidents. A safety definition is presented, based on the MTOI framework modifications proposed to it. It is proposed to rename it as MTOE and detail its elements. The problem of security management is analysed and described systematically and dynamically. Some appropriate methodologies are presented to be used in the representation of the proposed subsystems. Conclusions: The bases are presented to model with dynamic modelling methodologies the safety management of an organization operating a nuclear reactor.

KEYWORDS: nuclear, radiological, safety, management.

1 INTRODUCTION

One of the nuclear industry lessons collected from the Fukushima Daiichi nuclear accident was the impact of the different contributions that risk receives from technological, organizational, managerial, and operational factors of technology and human factors [1–3]. In that accident, the environment's influence and pressures were also recognizable as a conditioner of safety.

Although identifying these contributors to risk and safety is not new in nuclear reactors operation [4]. Since the last ten years, academics and practitioners have made new and diverse contributions to understand and address nuclear safety management (SM). These studies [5] show that the level of conceptual and practical atomization is considerable. It was also observed that it lacks integrating theories and frameworks that allow modeling this problem to understand it and then manage it from its understanding. The industry has made many efforts to implement huge and bureaucratic SM systems that lack robust theoretical, conceptual, and causal support.

In [6] cited in [5] mention, "that it is necessary to propose a framework that allows integrating all the models, meta-models, and concepts that were presented." In that way, the most relevant works come from Wahlström [7], the International Nuclear Safety Advisory Group (INSAG) [8], and the International Atomic Energy Agency [9]. In this work, the control theory and the systems view are the more relevant contributions and considerations. The MTOI framework [7,10] seems to be the most appropriate to consider model the SM in a systemic way. Also, state of the art for the nuclear industry still lacks more specific frameworks that: integrate the cited factors, that have a systemic and complete vision of their domains [5], and that allow modeling their causal relationships considering the aspect of time [11] in the incubation of future errors and the capacity of the systems for their correction.

Starting from the identification of this theoretical gap [5] and taking as a basis the lessons learned from nuclear accidents and his main root causes, the theories of accidents causations, the systemic thinking about safety, the contributions to the MTOI framework made in [7,10], this work proposes modifications to this framework and an approach to modeling nuclear SM in an integrative, comprehensive and dynamic way.

2 METHOD

The applied methodology is:

- Apply the deductive-inductive method [12].
  The deductive method is used to develop a definition of safety.
  The inductive method is applied based on the premises of the MTOI [7,10] and the factors that contribute to the risk and causation of modern nuclear accidents. On this basis, a new frame of reference is concluded and proposed that aims to integrate these contributions.
- Apply analytical reduction to the main root causes of the principal nuclear accidents [4].
  It starts from the main roots causes identified in the bibliography, decomposing these into smaller units until finding irreducible causal elements. The auxiliary questions used in the analytical reduction are what? who? and how?
- Analysis of bibliography and study of the gaps identified in state of the art [5].

3 BRIEF DESCRIPTION OF THE MTOI FRAMEWORK

The MTOI framework [7,10] is based on the SM of nuclear power plants' systems view approach. It considers valid dimensions for its logical and systematic understanding. In this sense, the approach considers four systems or dimensions that determine its safety: Man, Technology, Organization, and Information. These subsystems are detailed in the following description:

• "The Man subsystem comprises people who work in and with the plant (designers, operators, maintenance personnel, managers, regulators), all of whom contribute to safety.

• The Technology subsystem is composed of the physical system, including its instrumentation and technological control. Its successful operation depends on the success of the applied design processes (physical system, instrumentation, control system, power supplies) and successful operation and maintenance.

• The Organization subsystem defines the division of labor into roles, authorities, and responsibilities. It is governed by a management system consisting of policies, management system descriptions, instructions, and plans. In contrast, the practices defined in that management system should reflect reasonably well in current practices.

• The Information subsystem is integrated into the system description, data collection and storage, and communication routines. The operation of the management system and the instrumentation and control depends on the information generated, encoded, stored, accessed, and stored appropriately".

Limitations found to the MTOI framework.

Using the MTOI framework, it is possible to describe some SM system components at the micro-level (the plant's operational reality). However, it is not to describe other supra-levels that have external influence the safety. Regarding another limitation of this approach, the externals factors that contribute to safety or influence the risk are not taken into account. This trait omits a fundamental influence in safety that made one of the mains stakeholders in this industry: the nuclear regulatory bodies. That is, the nuclear industry has great relevance and power and (e.g., in the nuclear power plants, the regulatory bodies have resident inspectors)

Regarding the framework's ability to describe the system's risk, this framework does not distinguish the risk contribution made by its constituent elements. Nor does it incorporate the decision-making process as an element that can fail or have deviations.

Another issue about its subsystems (M, T, O, and I) is the questionable isolation of subsystem I. This subsystem seems to compose a subsystem representing an emergent and natural characteristic of the other subsystems' interaction (M, T, and O). Therefore, isolating it seems to be a redundancy of their

interaction. That is, a subsystem is proposed that considers the flow of information between subsystems when in reality the means of transferring data or information is typical of the subsystems M (personal communications), T (physical signals typically of the instrumentation and control of the plant) and O (SM system).
While seeking to propose a comprehensive nuclear SM model, the MTOI framework is useful for characterizing and identifying some of its elements. It seems not to be practical and complete enough to understand the dynamics of the problem and identify which functional unit intervenes in his behavior.

4 RESULTS

4.1.1 What is safety?

In this section, to lay the foundations of the framework, a definition of safety is proposed. This work understands safety as a construct representing the state of an element (according to an observer). This element's state is the result of its interaction with its environment and its interaction with itself. There are no interactions without potential changes from the initial state.

The status of an element will be bound by safety. This state is safe if, for an observer, the result of the interactions that this element has (with itself and with its environment) does not present irreversible and unwanted changes. In the case of the nuclear industry, irreversible and unwanted changes are produced by ionizing radiation.

Interactions are understood to be exchanges, transfer or incorporation of energy, matter (actions included), or information (decisions included). An element is understood as both the fundamental unit of a system or component and a system itself (workers and public included).In this sense, the nuclear system's scope must include the reactor's whole operating organization [9] and its context, including external inputs as regulation and financial strains [11].

4.1.2 Safety lessons learned from main nuclear accidents.

This section presents the results of applying the analytical reduction technique to the root causes of the main nuclear accidents considering in [4] and looking for the triggers of the loss of physical variables of the reactor. The results achieved were to reduce the causes to technological actions, human actions, and human decisions. See Table 1.

Thus, it is inferred that the loss of control over the variables and physical processes of the reactor that end in an accident or incident are due to:

- The technological action (TA) is directly related to the control or monitoring of the reactor's physical variables and processes and its safety functions.
- Human action (HA) is directly related to the control of technological variables and systems.
- Human decision (HD) has direct or indirect control of the human, organizational, and therefore technological actions of the reactor.

Table 1: Summary of the main nuclear accidents adapted from [4] and applying the analytical reduction to root causes.

Year - Accident	Accident Type	Main Root Causes	Results of apply analytical reduction to the main root causes.
1979 - Three Mile Island - USA	Core Meltdown with consequences to operators but not to the environment.	Technical design deficiencies, system malfunctions and Human-related errors, breach of maintenance procedures [13].	*Technological action, human action, and human decision failures.*

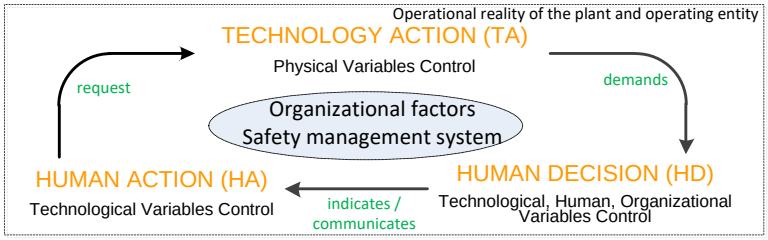
1983 - RA2 - Argentina	Critically Accident with consequences to operators but not to the environment.	Human-related errors, breach of operating procedures. Absence of a radiation protection officer during the operation [14].	*Human action and human decision failures.*
1989 - Chernobyl - Ukraine (ex USSR)	Core Meltdown, Breakage of the containment, and release of radionuclides into the environment.	Regulatory and Technical design deficiencies, system malfunctions, and Human-related [15].	*Technological failure, human action, and human decision failures.*
2011 - Fukushima - Daiichi - Japan	Three reactors (F1-1, F1-2, F1-3) with Core Meltdown and three reactors (F1-1, F1-3, F1-4) with Breakage of the containment and release of radionuclides to the environment.	Regulatory, Institutional-Organizational, and Technical design deficiencies and system malfunctions [1–3].	*Technological failure, human action, and human decision failures.*

The HD-HA-TA constitutes a loop of interactions (not necessarily linear) that can constitute an initiating event of an accident or incident in the event of failure of one or more of them. This loop's dynamics are conditioned by the organizational factors [16,17] and by the availability and instantaneous accessibility to relevant information for human decision.

Considering the perspective of metaphor control [7], it can be inferred that the HD has a domain or incidence on the technological, human, and organizational variables of the operating organization of the reactor. HA has a domain or incidence on technological variables. While the TA domain or incidence on the physical variables. In other words, from this point of view, HD has an interface of action until it intervenes or influences the physical variables.

This loop may have a failure in one or more of these elements (HD, HA, TA). Although this loop is not linear and behaves like a network, the network will usually have some sequence of this type: HD, HA, TA fails, HA, TA, HD fails or TA, HD, HA fails, which can cause an initiating event of an accident/incident. See Figure 2.

Figure 2: Fundamental causal loop unit of accidents/incidents.



4.1.3 Identification of Accidental/incidental sequence

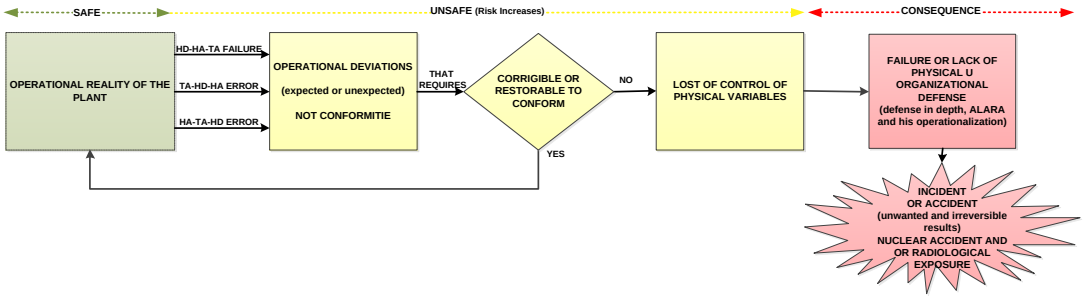
A typical accidental/incidental sequence applicable to nuclear reactors is postulated in this subsection while considering what was previously presented.

Applying the control theory view [7] and considering that the unwanted and irreversible radiological consequences briefly described in the previous subsection, it can be inferred that the primary mission of the technological and organizational systems to operate a nuclear reactor is the control of the physical variables sources of danger and risk.

Then taking into account the accidents causation theories with an emphasis on human and organizational errors [18] and the modern approach of resilience engineering [19], some plant events lead to operational deviations (expected or unexpected) that, when detected by the technological or organizational systems, require or demand to be corrected to a conforming level. When man, technology, and/or organization fail to recover the event to a level of compliance, it can lead (immediately or after an incubation time - latent error) to the loss of control of the physical variables with the potential to have the intended radiological consequences (due to the occurrence of an incident or accident).

Figure 1 shows a case the sequence described and contemplated the concepts of nuclear design of defense in depth and radiological protection of doses "as low as reasonably achievable," where an event demands the physical or organizational defenses that, if they fail or do not exist, will lead to the unintended consequence: the incident or accident.

Figure 1: Simplified accidental/incidental sequence.



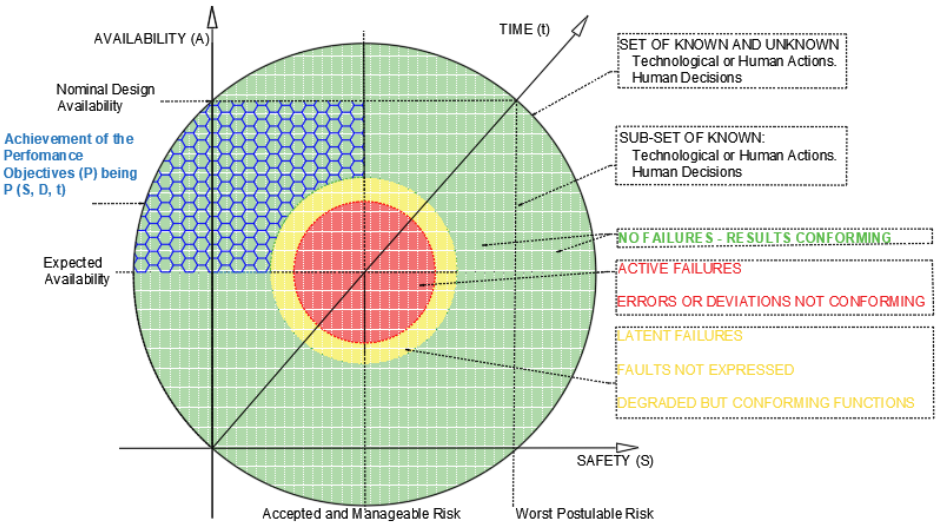
4.1.4 Safety is a dynamic problem.

This work proposes to think the safety as a state (safe, unsafe). It will be determined by the causal interaction of the elements that make up its subsystems (and its states). The value of this state is a risk function. Then, and considering the operating organization as the system under study, the understanding and management of the radiological risk that conditions its status and will intervene in the performance includes achieving the business continuity and sustainability goals.

The previous statement is relevant because another issue that converges with the importance of safety is the plant's availability. Either generate electrical energy (nuclear power plants) or irradiation time (research reactors) that allow them to generate incomes to operate and re-invested in SM programs.

Plant availability shares some conditioning elements with safety, such as the components' reliability and failures. That is why, and laying the foundations for integrated modeling of the plant reality, it seems appropriate to study these integrated domains. These relationships are proposed because it is assumed that the plant operations' sustainable. It implies the achievement of the state of safety and availability for its expected operation. Additionally, both availability and safety can be addressed through failure prevention. Limiting its control capacity, the operating organization will know a certain number of events, actions, or results (at all its organizational levels). Although they are still unknown, they can have an impact on safety or availability.

Figure 4: Integrated domains of safety and availability.



Other considerations in this approach are:

- Such events, actions, and/or their results may present failures, deviations, or degraded functions that may increase the risk and affect the safety or affect the plant (making it unavailable for operation).

- There are events, actions, and results of tasks that do not express their impact on safety or availability instantaneously (they remain latent) at t = 0. These can be combined with other latent failures and affect the plant's safety or availability at t <> 0.

- The plant's availability is defined by its design (for example, the number of hours per year that it can operate or the amount of energy to produce per year).

From the above, it is possible to identify areas where safety and availability objectives are achieved. Adding the dimension of time, it is possible to measure a joint performance between safety and availability. Incorporating the time axis in Figure 4 would allow tracking trajectories of events, actions, and results of tasks that allow diagnosing and/or forecasting unwanted trajectories. The more relevant aspect of this is that it is based on the elements of the causal loop unit (CLU), Human Decision (HD), Human Action (HA), and Technological Action (TA), and their dependence on time.

4.1.5 Proposed modifications to the MTOI framework, the MTOE framework

Based on the MTOI framework, and considering what is presented in the previous sections to argue its limitation to address the problem dynamically and completely, this work proposes to discard its subsystem I for redundant and include a new one. A subsystem that considers the effect of the environment. Then this work refers to this framework with this acronym: MTOE (man, technology, organization, and environment).

The subsystems, dimensions, or layers that compose it are:

- Subsystem M (man or human): includes the HD and HA of the people who work IN the plant (mainly operators, radiation protectionist, maintenance personnel). This subsystem has a direct interface with the equipment for operation, control, and physical variables and reactor processes.

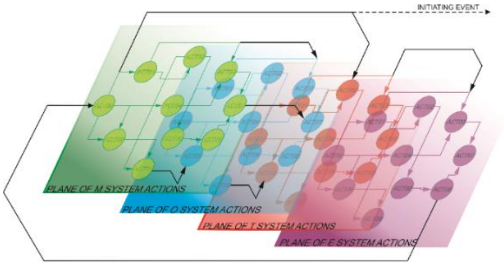
- Subsystem T (technology): includes the TA of the system. It is represented by all of the reactor physical systems subsystems and components (SSC). The SSC failure determines the transition from safe to unsafe state and the availability state of the reactor.

- Subsystem (organization): includes the HD of the internal people who work WITH the plant (mainly internal analysts and internal decision-makers). In this subsystem mainly predominates the elements of the safety management systems. For scale and element consistency (macro-meso-micro), special attention should be paid when considering the constituent elements of the system if it is based on process management.

- Subsystem E (environment): includes the HD of the external persons or entities that work WITH the plant or with its internal people (mainly regulators, inspectors, stakeholders and shareholders, unions and other external decision-makers, political decision-makers and peers who directly inspect the operating organization).

It should be noted that a subsystem's actions can be predecessors or inherited from another action of another subsystem. In Figure 5, each subsystem is represented as a spatial plane with its specific scope. The relevant HD, HA, or TA are represented in a network scheme in each of them. This network represents its interrelated nature.

Figure 5: Conceptual MTOE Taxonomy.



This taxonomy allows to identify and visualize links and interdependencies between different actions and decisions of different subsystems. Also, how they participate in the genesis or development of an initiating event. Other qualities reside in that they allow to see the distribution of decision authority, specialization, degree of automation and unionization, dependencies of the supply chain, and subcontracting impacts.

4.1.6 Methodologies to achieve the representation previous the modeling considering MTOE.

This section presents the most appropriate methodologies to represent the MTOE and its causal relationships, considering the dynamic aspect of the problem as a previous step to the simulation stage. Table 2 summary of the principal methodologies founded in the bibliographic review to cover the requirements of each subsystem of MTOE (described above). This work considers more appropriate methodologies that have been recognized in works with an application to the nuclear industry or to safety engineering, graphical standardization that allows visualizing the dynamics of the system's resilience.

Table 2: Summary of the principal methodologies to represent the MTOE subsystems.

Method or Tool	Typology	Focus-Paradigm	Representation			
			M	T	O	E
Dynamic fault tree (DFT) [20]	Dynamic-Discreet	Components-Functional	√	√	√	X
Goal tree-success tree Dynamic Master Logic Diagram (GTST-DMLD) [21]	Dynamic-Continuous	Components-Hierarchical-Functional	√	√	√	X
System Dynamics (SD) Forrester Diagram [22]	Dynamic-Continuous	Components- Systems-Causal	√	√	√	√
Agent-based modeling (ABM) [23]	Dynamic - Discreet	Components/Individuals-Causal	√	√	√	√
Process-centric discrete event (PC) [24]	Dynamic - Discreet	Processes-Causal	√	X	√	X

From Table 2, this work found more appropriate to integrate the representations of all subsystems with the SD and ABM methodologies/tools. However, for the T subsystem is also appropriate, and next in SD, the GTST-DMLD method.

5 CONCLUSIONS

A framework basis for developing a systemic and dynamic model of the SM of nuclear reactors' operating organizations is developed based on a bibliographical review. A proposal to understand the causal relations of the elements of this system was presented. The MTOE framework was introduced, and the tools to represent its subsystems have initial considerations.

6 ACKNOWLEDGEMENTS

This paper's authors are very grateful for Dr. Björn Wahlström and Ms. Mariela Grinberg's helpful expert comments.

7 REFERENCES

[1] International Atomic Energy Agency, The Fukushima Daiichi Accident Report by the Director-General, Dir. Gen. (2018) 1–222. https://doi.org/10.1037/a0018137.

[2] J.E. Yang, Fukushima dai-ichi accident: Lessons learned and future actions from the risk perspectives, Nucl. Eng. Technol. 46 (2014) 27–38. https://doi.org/10.5516/NET.03.2014.702.

[3] N. Engineering, E. Hollnagel, R.S. Plus, The Fukushima Disaster – Systemic Failures As The Lack Of Resilience, (2014). https://doi.org/10.5516/NET.03.2011.078.

[4] G. Acuña, M. Giménez, M. Sánchez, Evolution of safety management before the Fukushima Daiichi accident . A bibliographical revision in the context of major modern industrial accidents, II International Virtual Congress of Industrial Engineering, Iberoamerican International University, 7-11 September 2020 (2020).

[5] G. Acuña, M. Giménez, M. Sánchez, Nuclear Safety Management after Fukushima accident. A systematic and critical review of the state of the art, International Conference Of Production Research. Americas 2020. December 2020 Bahía Blanca (2020).

[6] B. Wahlström, C. Rollenhagen, Models , methods and tools for safety management Experience from Vattenfall, (2010) 21–25.

[7] B. Wahlström, C. Rollenhagen, Safety management - A multi-level control problem, Safety Science 69 (2014) 3–17. https://doi.org/10.1016/j.ssci.2013.06.002.

[8] International Nuclear Safety Group, Ensuring Robust National Nuclear Safety Systems-Institutional Strength in Depth INSAG-27, (2017) 40. http://www-ns.iaea.org/standards/.

[9] I. International Atomic Energy Agency, Hierarchical Structure of Safety Goals for Nuclear Installations, IAEA-TECDOC-1874, (2017).

[10] B. Wahlström, Systemic thinking in support of safety management in nuclear power plants, Saf. Sci. 109 (2018) 201–218. https://doi.org/10.1016/j.ssci.2018.06.001.

[11] Y. Dien, N. Dechy, E. Guillaume, Accident investigation : From searching direct causes to finding in-depth causes – Problem of analysis or/and of analyst ?, Saf. Sci. 50 (2012) 1398–1407.

[12] A.O. Rodríguez, A., Pérez, Métodos científicos de indagación y de construcción del conocimiento, EAN. (2017) 175–195.

[13] G.B.E. Siddall, An Analysis of the Three Mile Island Accident, AECL-7065, At. Energy Canada Ltd. (1980).

[14] J. Pahissa-Campa, D. Beninson, RA-2 criticality accident, Trans. Am. Nucl. Soc. 47 (1983) 266.

[15] International Nuclear Safety Advisory Group, I. Atomic, E. Agency, The Chernobyl Accident: Updating of INSAG-1, 1993..

[16] G. Rolina, Human and Organizational Factors in Nuclear Safety, Hum. Organ. Factors Nucl. Saf. (2013).

[17] C. Rollenhagen, A framework for assessment of organisational characteristics and their influences on safety, (2018).

[18] J. Reason, A systems approach to organizational error, Ergonomics. 38 (1995) 1708–1721.

[19] E. Hollnagel, Safety-II in practice: Developing the resilience potentials, Safety-II Pract. Dev. Resil. Potentials. (2017) 1–130. https://doi.org/10.4324/9781315201023.

[20] F. Chiacchio, A. Iacono, L. Compagno, D.D. Urso, A general framework for dependability modelling coupling discrete-event and time-driven simulation, Reliab. Eng. Syst. Saf. 199 (2020).

[21] E. Ferrario, E. Zio, Goal Tree Success Tree – Dynamic Master Logic Diagram and Monte Carlo simulation for the safety and resilience assessment of a multistate system of systems, Eng. Struct. 59 (2014) 411–433. https://doi.org/10.1016/j.engstruct.2013.11.001.

[22] M.I. Shire, The application of system dynamics modelling to system safety improvement : Present use and future potential The application of system dynamics modelling to system safety improvement : Present use and future potential, (2020).

[23] K. Furuta, T. Kanno, How the Fukushima Daiichi Accident Changed (or not) the Nuclear Safety Fundamentals ?, (n.d.). https://doi.org/10.1007/978-3-319-58768-4.

[24] Borschev, Anylogic, How to Build a Combined Agent-Based / System Dynamics Model in Any Logic, Syst. Dyn. Conf. (2008).