Acuña, Gregorio; Giménez, Marcelo; Sánchez Marisa

EVOLUTION OF SAFETY MANAGEMENT BEFORE THE FUKUSHIMA DAIICHI ACCIDENT: A BIBLIOGRAPHICAL REVISION IN THE CONTEXT OF MAJOR MODERN INDUSTRIAL ACCIDENTS. RELIABILITY

Segundo Congreso Internacional Virtual de Ingeniería Industrial (CIVII 2020)

7, 8, 9, 10 y 11 de septiembre 2020

Acuña, G., Giménez, M. Sánchez, M.A. (2020). Evolution of safety management before the Fukushima Daiichi accident: A bibliographical revision in the context of major modern industrial accidents. Reliability. *Segundo Congreso Internacional Virtual de Ingeniería Industrial (CIVII 2020). En RIDCA. Disponible en:*
http://repositoriodigital.uns.edu.ar/handle/123456789/5209

Evolution of safety management before the Fukushima Daiichi accident. A bibliographical revision in the context of major modern industrial accidents.

RELIABILITY.

Gregorio Acuña[1,2], Marcelo Giménez[2,3], Marisa Sánchez[4].

1) Research Reactors Department, Comisión Nacional de Energía Atómica, 8400, Bariloche, Argentina.

2) Balseiro Institute, Universidad Nacional de Cuyo, 8400, Bariloche, Argentina.

3) Nuclear Safety Department, Comisión Nacional de Energía Atómica, Bariloche 8400, Argentina.

4) Management Sciences Department, Universidad Nacional del Sur, 8000, Bahía Blanca 8000, Argentina.

*gregorioacuna@cab.cnea.gov.ar

ABSTRACT

This study, through a bibliographic review, describes the evolution of the Safety Management theory and practice from the industrial field and particularized in the nuclear industry. (1) Background: Safety Management is a relatively novel field of safety theory. The last nuclear accident (Fukushima Daiichi) is a point of interest to analyze and capitalize on the theory and the experience developed up to there; (2) Methods: a review and summary of state-of-the-art safety management until 2012. This review is contextualizing the major industrial accidents in modern history. Nuclear accidents are the focus. (3) Results: Theoretical summaries are presented, and a timeline is built on the evolution of safety management. Major and modern industrial accidents are described and analyzed with a focus on nuclear accidents; (4) Conclusions: The evolution of thinking in safety management received numerous theoretical contributions that arose from the lessons learned from the major industrial accidents. The thought in safety management has had a cumulative but evolutionary behavior.

KEYWORDS: safety, management, nuclear, reactors

1. INTRODUCTION

Safety Management thinking is a relatively novel field (Pillay, 2015) of the safety theory. This discipline made numerous theoretical contributions based on the lessons learned from the main conventional and nuclear accidents.

This theoretical approach comprises the company's and society's assets (tangible and intangible assets). Consequently, mention may be made of the facilities, their equipment, and the human capital employed directly or indirectly in their operation. Intangible assets reach the company's brand, the specialized knowledge used and developed by the organization, and its performance in productivity or safety. Concerning the assets of the company that the organization has for the industrial activity and that are reached by it, they are the environment and the people, residents of the region liable to be affected by this activity.

Therefore, the care and preservation of these assets imply avoiding actions that have irreversible consequences (incidents and/or accidents). This is available from the design stages of the installation and the systems that operate and manage it.

This work will begin contextualizing the theme at the beginning of the decade of '70s because the term safety management (object of this paper) was introduced in the scientific safety literature in the '70s (Swuste et al., 2016). This decade is also relevant because this occurs with the first nuclear accident (Three Mile Island, 1979). Meanwhile, this paper contextualizes 1970-2012 theories and practices of safety or accident causation and major industrial accidents. Likewise, these contributions are presented considering the so-called safety ages or ages (Hollnagel, 2014; Pillay, 2015). These eras or ages have been established according to the causes identified to explain the accidents' nature. These eras are Technology Focus (1970-present), Human Factors Focus (1989-present), and Safety Management Focus (1995-present) (Hollnagel, 2014).

2. OBJETIVE

Identify, describe, and synthesize the evolution of theoretical thinking about safety management in the context of major industrial accidents in modern history.

3. METHODOLOGY

A conceptual bibliographic review is carried out. The main industrial accidents that occurred between the decade of 1970 and 2012 are identified. Their root causes are analyzed and described. The main theories of Safety Management developed between the mentioned decades are identified. The inputs received are analyzed. Their main contributions are described. They are classified in their contributions in thematic ages.

4. RESULTS

This section briefly reviews the academic theories or models that have been put forward to explain the causes of major industrial accidents before the Fukushima Daichii accident. The results are presented in the form of summaries of accidents and their root causes. Also, they are particularized in nuclear accidents with radiological consequences for workers, the population, and/or the environment (see Table 1). It was considered accidents in nuclear power reactors and nuclear research reactors. Then two subsections are developed. The first presents the accidents that occurred and theories developed between the 1970s and 1990s. The second presents the accidents that occurred and theories developed between the 1990s and early 2010s.

Table 1 Resume of the main nuclear accidents, including research reactors.

Year – Accident	Technology and Accident Type	Main Root Causes	Lessons Learned
1979 - Three Mile Island – USA	Pressurized Water Reactor- NPP, Core Meltdown with consequences to operators but not to the environment.	Technical design deficiencies, system malfunctions and Human-related errors, breach of maintenance procedures	The need for Incorporation of Probabilistic Safety Analyses, Human reliability analysis. Change the focus in the training of operators from diagnosis to action.
1983 - RA2 – Argentina	Material Test Reactor – RR, 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	Need for strict compliance with procedures and protocols with external supervision of the operator.

1989 - Chernobyl – Ukraine (ex URSS)	High Power Condenser Reactor - RMBK- NPP, Core Meltdown, Breakage of the containment, and release of radionuclides into the environment.	Regulatory and Technical design deficiencies, system malfunctions, and Human-related. (INSAG, 1992)	Need to develop a safety-oriented organizational culture.
2011 - Fukushima – Daiichi – Japan	Boiling Water reactor- NPP, 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 into the environment.	Regulatory, Institutional-Organizational, and Technical design deficiencies and system malfunctions.	Need of Stakeholders and decision-makers involved in safety.

4.1. From the '70s to the '90s. Technology focus and the start of human factor focus.

At the beginning of the '70s in 1972, Cohen, March & Olsen published their article "A garbage can model of organizational choice," where he characterizes the decision-making process and its impacts in complex organizational contexts. This description of the process is relevant in decision-making for organizational, technical problems that may have main implications for worker or asset safety in the industrial context.

Turner (1978) formulates his work Man-Made Disasters (MMD), "general rules and principles on the occurrence of disasters, derived from the examination of the available evidence of past disasters and major accidents". This work is the precursor of the identification of the socio-technical causes of accidents.

It is in 1979 when the first nuclear accident occurs in a nuclear power plant: Accident in Unit 2 of Three Mile Island (TMI), in the USA, where deficiencies in the design and failure to apply maintenance procedures and failures in the operators' decision-making process in the face of the emergency were its leading causes (Brooks & Siddall, 1980).

As early as the 1980s in 1982, the RA-2 research reactor criticality nuclear accident occurred, with causes focused on the non-compliance with operating procedures (human failure). In 1984, the Bhopal accident in India occurred in the chemical industry. A pesticide plant exploded with causes in Human-related, information, and hardware related errors and corporate-level failure of safety management systems and procedures (Bowonder, 1988). Likewise, that same year in Mexico, a PEMEX petrochemical plant had a major accident with the causes of technical malfunctions in the facility after modifications were made (Arturson, 1987).

While the academy, also in that year, made one of the main contributions to the theory of modern safety, since it was Perrow (1984) inspired by the causes of the Three Mile Island accident, he was the one who postulated the theory of the Normal Accidents (NAT), which concludes that accidents involving unanticipated interaction of multiple failures in systems with high-risk technologies (Hopkins, 1999). It also states that complex technology is the cause of accidents (technological determinism) and organizations and people who naturally incubate and escalate design problems or operational errors, which ultimately trigger their consequences. Its innovation is recognizing complex interactions and the different levels of coupling of the systems and components as a determining factor.

Then in 1986, the aerospace industry had its first major accident, that of the Space Shuttle Challenger whose main causes were technical (failure in one component) and the organization (failure to detect the technical cause) (Boin, 2007).

INSAG in 1988, proposed in its Professional Report "Basic Safety Principles for Nuclear Power Plants" several concepts that would take down in depth in the following years. These concepts are Culture Safety and Defense in Depth. Both ideas are explained later in this paper.

It is in 1989 when the second major nuclear accident in history occurs in Chernobyl (Ukraine, former USSR). Their causes are multiple, including a unique design with Regulatory and Technical deficiencies, system malfunctions, and Human-related errors context of a poor safety-oriented organizational culture (INSAG, 1992).

High-Reliability Organizations (HRO) or High-Reliability Theory (HRT) is an approach proposed by Roberts (1989) that arises from the observation of NAT-type organizations, which,

according to this technological determinism should suffer-normal accidents. However, in practice, there are some of those high-risk organizations with technological complexity that do not suffer from them. These types of organizations are called HROs, and this theory characterizes them. As a counterpoint to NAT, it is stated that technological determinism can be moderated by organizational tools and management (Hopkins, 1999).

Having analyzed the TMI, Chernobyl, and Challenger accidents, Reason (1990) explains the nature of Human Error. Their work suggests that recurrent error forms have their origins in fundamentally useful psychological processes and that errors can be modeled by an extension of accepted human performance models. (Gray et al., 1993). To this, and based on the study of the accidents mentioned above, the Human Reliability Analysis model, used in the nuclear industry until today, is proposed. Another model developed by Reason is the so-called Swiss Cheese Model (SCM) that explains how accidents can be seen as the interrelation of a series of unsafe acts at different levels and underlying conditions of the organization.

Already in 1991, from the study of the Chernobyl accident and its causes, the International Nuclear Safety Advisory Group (INSAG) of the IAEA (International Atomic Energy Agency), postulates the concept of Safety Culture, as a type of organizational culture oriented mainly to the safety of the facilities as a conditioning factor of the operational performance in safety.

Finally, in 1992 PEMEX (Petrochemical) again had an accident due to a technical failure that caused fuel leaks to the sewer lines system (Andersson & Morales, 1992).

Below, Figure 1 summarizes in a timeline focused on the succession of nuclear accidents, their context with common industrial accidents, and the evolution of safety thinking. As detailed above, it is inferred that during these decades, the theories concentrated on explaining the causes of accidents with a focus on technology and towards the end of the '90s after the Chernobyl accident, the theoretical bases for analysis and focus on human factors.

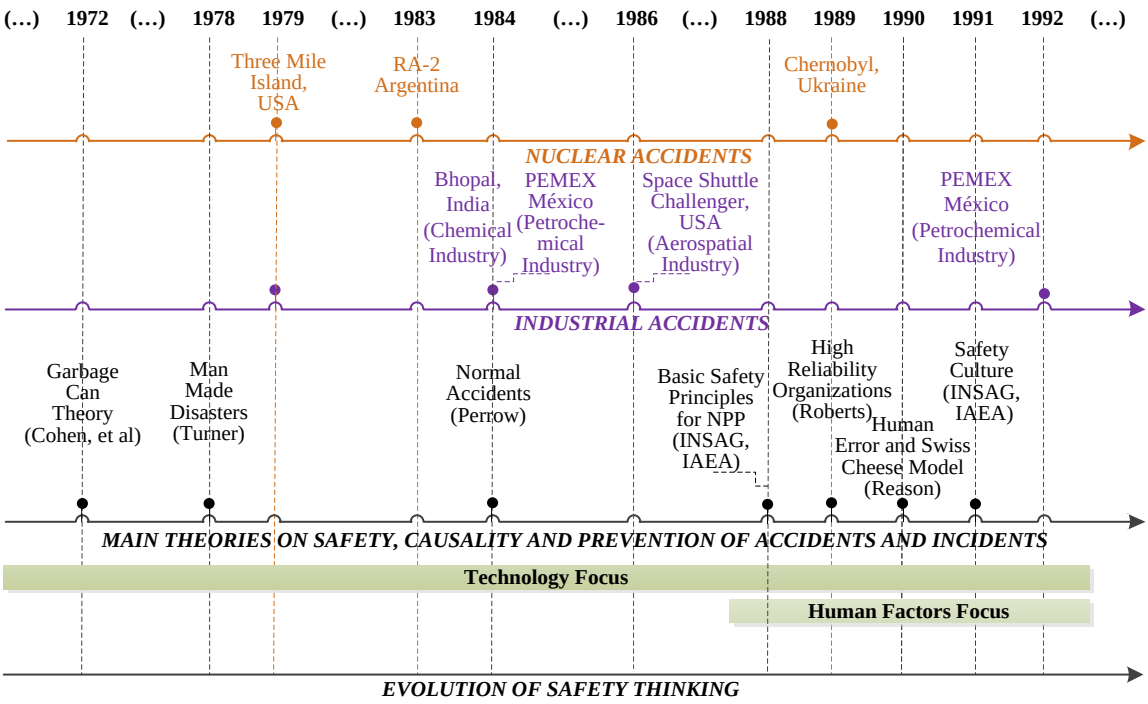

Figure 1 Major industrial accidents and the evolution of safety thinking (1970-1990).

4.2. From the early '90s to the 2012. Technology focus and the start of management factor focus.

In 1996, the lessons learned about the analysis of the causes of the TMI and Chernobyl accidents, INSAG formulated the conceptual model of Defense in Depth. This approach "consists in a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant (INSAG, 1996). The concept established a universal framework for all reactors' design and operation with a high degree of implementation.

Already in 1997, Rasmussen's developments on the Risk Management Framework (RMF) took place, which made another great contribution that had and still has a significant theoretical and practical impact on many high-risk activities. There it lays the foundations for risk modeling as a control problem in multi-level socio-technical decision-making systems and accident

causality analysis. In the same year, Reason, based on his SCM model, develops his work "Managing the Risks of Organizational Accidents" where he raises the distinction between individual accidents (active failure) and organizational ones (latent failure) where the second are multiple causes and capable of developing or incubating for a long time before manifesting, it follows that some accidents have not only technological and human but also organizational causes. These approaches highlight the relevance of probabilistic risk/safety assessments (PRA / PSA).

In 2003, technological problems, management, decision-making, and communication were the causes of an accident in this case in the aerospace industry with the explosion of the space shuttle Columbia (Levenson, 2008).

Returning to the academy and based on Rasmussen model in 2004, Levenson developed the Systems-Theoretic Accident Model and Processes (STAMP). This is an Accident Model Based on Systems Theory. With this proposal being the forerunner in systematizing the application of the theory of systems. This approach considers factors of complexity and closer coupling observed in the continuous evolution of organizations with high technological risk, such as human-software-machine interfaces. Then in 2006, what is supposed to be the last radical contribution to safety thinking is postulated: the Resilience Engineering that proposes that 'failure' is the result of the adaptations necessary to cope with the complexity of the real world, rather than a breakdown or malfunction" (Hollnagel. et al. 2006). In this approach, a model is proposed to strengthen an organization's resilience in the face of changes that may disturb its normal operation, including errors.

Finally, the most recent accidents during this period were in 2010: British Petroleum, Mexico Petrochemical. Whose causes were determined by the BP Incident Investigation Team as design failures, failures in technical operation, failures in maintenance, failures in emergency management, it is said both technical and organizational and management failures. The following year, in 2011, the last nuclear accident occurred in Fukushima - Japan, in the context of an extreme natural catastrophe not contemplated in its entirety in the design baseline of the all infrastructure, industry, and reactors of Japan. Likewise, at the plant operation and

emergency management level, the accident's causes were design failures, technical failures in operation, institutional, organizational and regulatory failures (IAEA, 2014; Yang 2015; IAEA, 2015).

Below, Figure 2 summarizes in another timeline the last nuclear accident, and his context with common industrial accidents, and the evolution of safety thinking.

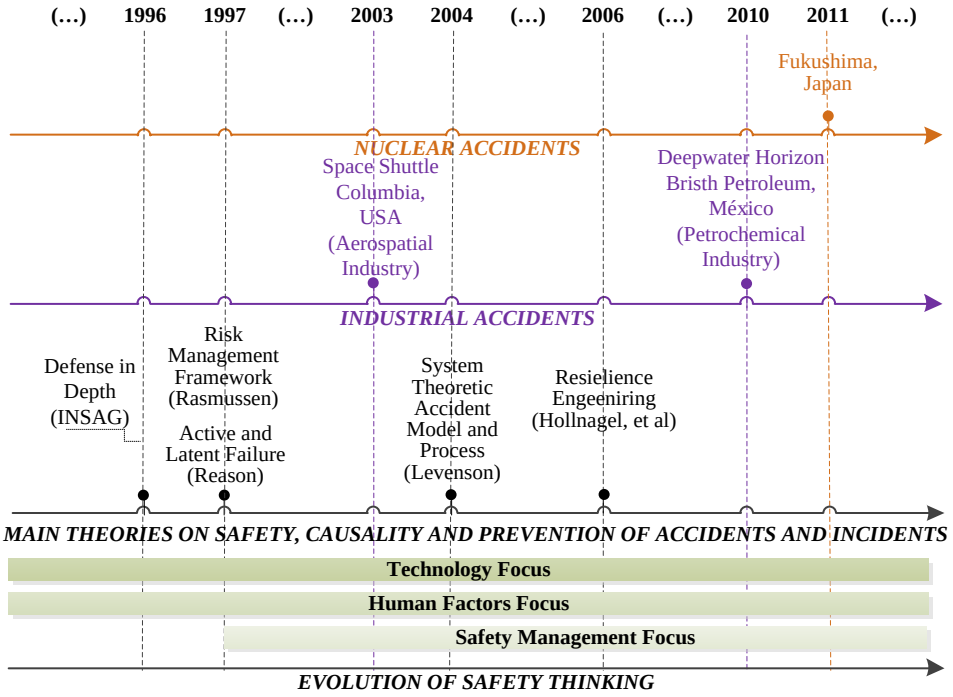

Figure 2 Major industrial accidents and the evolution of safety thinking (1990-2011)

As detailed above, it is inferred that the theories expanded their approaches to other factors during these decades. These approaches were the emphasis on the analysis of the causes of accidents related to human factors and safety management. This occurs based on the theoretical developments of the RMF and the causes that evidenced the best described industrial accidents. This supports the premise presented above. Safety management is an area of knowledge of recent academic development and adoption by practitioners.

5. CONCLUSIONS

The main theoretical contributions to the safety management field until 2012 (Fukushima Daiichi accident) were summarized. The major and modern industrial accidents and his root causes were presented and analyzed. Nuclear accidents were presented and analyzed. It was

observed that it is only towards the end of the 1990s when safety management takes center stage in theory and practice, and that integrative and holistic views have not yet been addressed.

Conflicts of interest

The authors declare there are no conflicts of interest regarding the publication of this paper.

Acknowledgements

This work was partially financially supported by the Universidad Nacional de Cuyo nº 80020180100498UN.

We thank Dr. Carlos Gho and Mr. Fabricio Brollo for his support and Mr. Nicolas Dechy of IRSN, France, for their expert comments.

REFERENCES

- Amalberti R. (2001), The paradoxes of almost safe transportation systems, Safety Science, Vol. 37, Issues 2–3, pp. 109-126
- International Atomic Energy Agency (2014), IAEA Report on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, IAEA, Vienna.
- Yang J. (2014), Fukushima Dai-ichi accident: lessons learned and Future actions from the risk perspectives, Nuclear Engineering and Technology, Vol.46 No.1, pp. 27 – 38.
- International Atomic Energy Agency (2015), The Fukushima Daiichi Accident, Report by the Director General, STI/PUB/1710 Technical Volume 1, IAEA, Vienna.
- Pillay, M. (2015). Accident causation, prevention and safety management: a review of the state-of-the-art. Procedia Manufacturing, 3 (Ahfe), pp. 1838–1845. https://DOI.org/10.1016/j.promfg.2015.07.224
- Hopkins A. (2014), Issues in safety science, Safety Science 67, pp. 6–14
- Swuste P., Gulijk C., Zwaard W., Lemkowitz S., Oostendorp Y., Groeneweg J. (2016), Developments in the safety science domain, in the fields of general and safety management between 1970 and 1979, the year of the near disaster on Three Mile Island, a literature review, Safety Science 86, pp. 10–26.
- Cohen M., March J., Olsen J. (1972), A garbage can model of organizational choice, Administrative Science Quarterly Vol. 17, No. 1, pp. 1-25.
- Turner B. (1978), Man Made Disasters, Wykeham Publications, First edition ISBN 0 85109 750 2.

- Brooks G., Siddall E. (1980), An Analysis of the Three Mile Island Accident, AECL-7065, Atomic Energy of Canada Limited.
- Bowonder B. (1987) An analysis of the Bhopal accident, Project Appraisal, 2:3, pp. 157-168, DOI: 10.1080/02688867.1987.9726622
- Pahissa-Campa J., Beninson D. (1983), RA-2 criticality accident, Transactions of the American Nuclear Society; Worldcat; v. 47 pp. 266.
- Perrow, C., (1984), Normal Accidents: Living With High-Risk Technologies. Basic, New York.
- Rodrigues De Oliveira A. (1984), Criticality Accident in Argentina, INIS-BR-141, Radiation Medicine Section, Nuclebras.
- Roberts, K.H. (1989). "New challenges in organizational research: High reliability organizations". Organization & Environment. 3 (2): pp. 111–125. https://DOI.org/10.1177/108602668900300202
- Reason J. (1990), Human Error, Cambridge, Cambridge University Press.
- Reason, J. (1990), The contribution of latent human failures to the breakdown of complex systems. Philosophical Transactions of the Royal Society (London), series B. 327: 475-484.
- International Nuclear Safety Advisory Group (1991), INSAG-4, Safety Culture, INSAG-4 a report by the International Nuclear Safety Advisory Group, IAEA, Vienna.
- Andersson N., Morales A. (1992), Mexico: Disaster in Guadalajara, The Lancet, Volume 339, Issue 8801, pp. 1103. https://doi.org/10.1016/0140-6736(92)90680-2
- International Nuclear Safety Advisory Group (1992), INSAG-7, The Chernobyl Accident: Updating of INSAG-1, a report by the International Nuclear Safety Advisory Group, IAEA, Vienna.
- International Nuclear Safety Advisory Group (1996), INSAG-10, Defense in Depth in Nuclear Safety, INSAG-10 a report by the International Nuclear Safety Advisory Group, IAEA, Vienna.
- Rasmussen, J. (1997). Risk Management in a Dynamic Society : A Modelling Problem. 27(2), pp. 183–213.
- Reason J. (1997), Managing the Risks of Organizational Accidents. Aldershot, UK: Ashgate.
- Leveson, N. (2004). A New Accident Model for Engineering Safer Systems, 42(4), pp. 1–30.
- Hollnagel, E., Woods, D. D. & Leveson, N. C. (Eds.) (2006). Resilience engineering: Concepts and precepts. Aldershot, UK: Ashgate.
- British Petroleum Incident Investigation Team (2010), Deepwater Horizon Accident Investigation Report, British Petroleum.

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