Journal of Risk Analysis and Crisis Response, 2023, 13(1), 19-34
https://jracr.com/
ISSN Print: 2210-8491
ISSN Online: 2210-8505

Article

The Sociotechnical Construction of Risks, and Principles of the Proactive Approach to Safety

Washington Barbosa [1,2,*], Luiz Ricardo Moreira [2], Gilson Brito [3], Assed N. Haddad [4] and Mario Cesar Vidal [2]

[1] Oswaldo Cruz Foundation, Rio de Janeiro (21040360), Rio de Janeiro, Brasil
[2] Production Engineering Program, Federal University of Rio de Janeiro, Rio de Janeiro (21941914), Rio de Janeiro, Brasil
[3] Production Engineering Program, Federal University Fluminense, Niterói (24210240), Rio de Janeiro, Brasil
[4] Environmental Engineering Program, Federal University of Rio de Janeiro, Rio de Janeiro (21941909), Rio de Janeiro, Brasil
* Correspondence: washington.fiocruz@gmail.com

Received: December 17, 2022; Accepted: February 17, 2023; Published: March 31, 2023

Abstract: This proposal presents the Sociotechnical Construction of Risks, Ergonomics, and the two principles of the Proactive Approach to Safety, Risks, and Emergencies, the Structured Sociotechnical Approach and Dynamics of Proactive Safety intending to complement traditional risk assessments, and prevent and Mitigating Major and Fatal Negative Events, the in organizations such as cases of the explosion of the space shuttle Challenger, the nuclear accident in Fukushima, the Texas City Refinery and the explosion in the Port of Beirut, among others. To propose these two principles, case studies were developed at Fiocruz, and in organizations, sectors, and activities, a bibliographic review on theses, dissertations, reports from regulatory bodies, books, scientific articles, and media articles, on major and fatal negative events, and ergonomics, socio-technical approach, and resilience engineering. A tragedy prevention course was created, with four free online consultation modules, based on cases of major negative events. These principles redirect the focus from human error to Focus on the Structured Sociotechnical System and Focus on the Dynamics of Proactive Safety. It is proposed that these two principles can provide us with bases for analysis, to prevent and minimize Major and Fatal Negative Events, and are a complement to traditional risk assessments.

Keywords: Safety; Risks; Ergonomics; Sociotechnical Construction of Risks; Proactive Approach to Safety

1. Introduction

We live in a dynamic and complex environment, safety management is an important tool to manage this environment. It is recommended that organizations that seek to achieve their goals incorporate security management throughout their life and activities, including strategies, decisions, operations, processes, functions, projects, products, services, and assets (Dekker, 2006 [1]; Figueiredo, 2018 [2]; Filho, 2021 [3]; Furuta, 2015 [4]; Hollnagel, 2019 [5]; Hopkins, 2005 [6], 2008 [7]; Levenson, 2020 [8]; Llory, 2014 [9]; Pidgeon, 2000 [10]; Perrow, 1999 [11]; Rasmussen, 2000 [12]; Reason, 2016 [13]; Turner, 1997 [14]; Vaughan, 1996 [15]).

Safety management can be divided into two auxiliary functions: risks and emergencies. The first aims to control latent factors and the second is the manifestations of risks in real facts. Therefore,

there are two complementary forms of action: preventive and corrective, and the Proactive Security proposal seeks to prevent the organization from acting only in a reactive way.

The use of risk management, risk assessment, and risk analysis emerged more or less independently in several areas: Nuclear Industry, Insurance, Oil Industry, Safety at Work, Corporate Security, Financial systems, Information Security, and Security of Products and Processes.

The word risk is used in many areas and with different meanings, such as in mathematics, economics, engineering, and the field of public health.

Safety is a state of low probability of occurrence of events that cause damage or loss.

The term safety culture was conceptualized for the first time in the technical report on the accident at the Chernobyl nuclear power plant in Ukraine, in the 1980s, as being:

"Set of characteristics and attitudes of organizations and individuals, which guarantee that the safety of a nuclear plant, due to its importance, will have the highest priority".

Accident is defined as: "an undesirable event that results in death, health problems, injuries, damages and other losses".

Near-miss is defined as: "an unforeseen event that had the potential to cause accidents". This definition is intended to include all occurrences that do not result in death, ill health, injury, harm and other benefits.

The term "incident" cited is defined as: "an unsafe occurrence arising from or in the course of work, in which no personal injury is generated". This term was added to include all occurrences that generated only material damage and near-accidents in the organizations' focus of action.

Despite the efforts made by companies, organizations, private sectors, and the government, a series of major and fatal negative events have happened, such as the explosion of the space shuttle Challenger, the nuclear accident in Fukushima, and the explosion in Port of Beirut, among others (Barbosa, 2022) [16].

Turner (1994) [17] analyzed serious technical accidents over a long period and concluded that approximately 20 to 30% of the causes of accidents were technical, with 70 to 80% involving social, administrative, or managerial factors.

A series of studies on air and maritime accidents in Qureshi (2008) [18] showed human and organizational factors as the main contributors to accidents and incidents. An analysis of major air and maritime accidents in North America during 1996-2006 concluded that the proportion of causal and contributing factors related to organizational issues exceeds those due to human error. For example, the combined causal and contributory factors of aviation accidents in the US showed: 48% related to organizational factors, 37% to human factors, 12% to equipment, and 3% to other causes; and the analysis of maritime accidents classified causal and contributory factors as 53% due to organizational factors, 24-29% as human error, 10-19% for equipment failures and 2-4% as other causes.

Why do negative events happen?

These complex events require both a socio-technical approach and a working conceptualization of these systems.

According to Llory (2014) [9], however diverse the causes of these accidents are, they all have an organizational dimension, that is, their root causes must be sought to verify what caused the accident. They also confirm that the non-occurrence of serious accidents and good performances in everyday life can hide an important issue, as a catastrophe may be about to happen.

In this way, the objective of the research can be presented as follows:

Principles can be developed, with analysis of these accidents and case studies, according to Barbosa (2022) [16], in search of factors and variables, which present proposals for the prevention and minimization of these accidents, which happen repeatedly, and that can be transmitted to the organizations.

Initially, a case study was developed, conducted by the author that originated a monograph of the specialization course in Ergonomics: "Ergonomic Analysis of Risk Management of Residues of Dangerous Products from Fiocruz" and an article by the author on the "Contribution of Ergonomics to the Development of Proactive Safety, Risks and Emergencies of Waste from Fiocruz Dangerous Products", presented in the panel of articles approved at the Abergo 2020 Congress (Barbosa, 2020) [19].

As a continuation of this research, an in-depth literature review was carried out on theses, dissertations, reports from regulatory bodies, books, scientific articles, and media articles, on major and fatal negative events, ergonomics, socio-technical approaches, and resilience engineering. The initial cases presented in Barbosa (2022) [16] were selected, and the research continued in units, sectors, and services at Fiocruz and in organizations. Regarding Fiocruz, as the author is an employee of Fiocruz, he can carry out several visits to these places, and talk to the Management, Department Heads, Researchers, Engineers, Architects, and Technicians in the areas of research, infrastructure, and management, about the other organizations, confidentiality was requested. This work began in 2016, with the evaluation of the management of Fiocruz's hazardous products, and has continued in the research laboratories and Fiocruz units, in other teaching and research institutions, and in other organizations, until the date of presentation of this work because one of the author's main activities is the safety assessment of the facilities and services provided by organizations.

A tragedy prevention course was also created, with four free online consultation modules, in a blog by the author, with a base of cases of major negative events that are hosted in module three (Barbosa, 2022) [16].

2. Literature Review

Traditionally, in the analysis of negative and fatal events, the blame is directed towards workers, who are the most fragile elements of the companies' chains of command, and there is little analysis of the activities performed by workers, and their consequences in procedures and adequate working conditions, supervision and management of activities, investments in the maintenance of facilities, analysis, and adaptation of projects, company policies, remuneration bonuses for Directors and Managers, social and economic requirements, and analysis of the legislation applied to the activity, among other issues. Safety management researchers have focused on this topic in recent decades and have presented their proposals for analyzing the factors that give rise to these negative events.

2.1. Evolution of the Periods of the Analysis of Negative and Fatal Events

According to Dechy (2011) [20], we can present the evolution of these periods:

- Technical period until the 1970s: the source of problems is seen as technology; security was primarily based on technical reliability.

- Period of "human error" in the 1980s: the source of the problem is seen as the person in particular the operators after the Three Mile Island accident in 1979; allowed improvements in the

domains of the human-machine interface, design of operational procedures, training, among other activities.

- Socio-technical period in the nineties: After Bhopal (1984), Challenger and Chornobyl (1986) the source of the problem is seen as the interaction between the social and the technical subsystems; Furthermore, the concept of "Safety Culture" emerged after the Chornobyl accident.

- Interorganizational relationship period from the 2000s: the source of the problem is dysfunctional relationships between organizations, with the controlling role of authorities, subcontractors, competitors, and other departments within an organization.

The results of this evolution are cumulative, not exclusive, and none of these dimensions should be neglected when analyzing an event, as they all provide useful information for the world to understand the dynamics that gave rise to the accident.

2.2. Theories and Research Related to the Analysis of Accidents and Management of Organizations

We highlight theories and research related to the analysis of accidents and management of organizations, which have worked with the history of Safety and also contribute to the work presented in this article.

According to Hollnagel (2006) [21], we need to have the etiology of accidents, a study of possible causes or origins of accidents, we also need to have a safety etiology – more specifically what safety is and how it can be in danger. This is essential for system safety work in general and resilience engineering in particular. However, for reasons that are not entirely clear, development is lacking. The different perceptions of the accident phenomenon are what in current terminology are called accident models. Accident models appear to have started with a relatively single factor from simple models, and developed via simple and complex linear causality models to present-day systemic or functional models.

Greenwood and Woods [22], presented in 1919 the theory that proposed an individual propensity of workers to accidents at work, in 1931, Heinrich [23] proposed another theory in which a sequence of factors can cause the accident, in a linear sequence of falling domino pieces, aligned side by side, in which the fall of one piece triggers the fall of the other pieces on the side, in a linear sequence of events, called the Domino Theory. It is a linear cause-and-effect model. In this theory, it was argued that it would be possible to avoid the accident, even after the first domino piece had fallen if one of the stones in the sequence was removed. Heinrich states that about 88% of accidents are due to unsafe acts, 10% to dangerous conditions, and 2% to fortuitous situations, this perspective remains one of the preponderant theories in the area of safety in organizations.

Turner (1978) [24] analyzed 84 accidents and disasters in all sectors, presenting the idea that social, technical, and administrative interactions systematically produced disasters; and developed the concept of accident incubation, with a six-stage development sequence:

1. Normal state, initially accepted beliefs about the world and dangers. Precautionary norms in laws, codes of practice, or traditional customs.

2. Incubation period, accumulation of a set of unnoticed events at odds with accepted beliefs about hazards and norms for controlling them.

3. Precipitating event, disaster begins, general perception changes, surprise, and disturbances occur.

4. Events escalate, consequences become apparent, and collapse occurs.

5. Rescue and rescue.

6. Complete cultural readjustment. Investigation. Beliefs and norms of precaution are adjusted to suit the newly acquired understanding of the world ("this must never happen again").

Perrow (1984) [25] analyzed large-scale accidents, which are a problem for society. According to Perrow, high-risk organizations with complex technological systems have structural properties that make these large-scale accidents impossible to predict and avoid. For this reason, in these complex systems, accidents are considered "normal" events, and on this basis, he named the theory of normal accidents, where he concludes that these accidents will repeat themselves, and suggested that some of these systems should be eliminated, due to risks of the occurrence of these accidents, the interaction of multiple failures stands out in these normal accidents, whose operational sequence is not direct. The difficulty in anticipating these situations. it is due to the infinite number of possible interactions between failures in the various components of complex systems.

Reason's model (1997) [26], known as "Swiss Cheese" or the theory of multiple causes, does not defend a single cause as the trigger for a sequence of events that would lead to the accident, but linear combinations of latent conditions and active failures that constitute several chains. and, after overcoming safety barriers by aligning their vulnerabilities, they culminate in an accident. In this theory, the influence of the organization in the occurrence of accidents stands out. Thus, investigations must look for latent conditions that may induce situations conducive to active failures. Thus, the most effective prevention should identify hazards or threats and manage the risks.

Rasmussen (1997) [27] developed the Accimap, which focuses on failure analysis at the following six organizational levels: government policy and budget; regulatory bodies and associations; company planning and budgeting; technical and operational management; physical processes and activities; and equipment, it is a proposal with a generic approach and does not use failure taxonomies at different levels of analysis.

Leveson's STAMP model (2004) [28] is based on levels of control of the socio-technical system. According to the theory behind STAMP, accidents occur due to the violation of the conditions in which the system was designed, to support the identification of violations, a taxonomy of control failures is proposed.

FRAM (Hollnagel, 2004 [29], 2012 [30]) is a method that aims to understand how systems work and how variability propagates between their functions, to develop more resilient systems.

Using this model can identify conditions that can lead to accidents in four steps:

- Identify and characterize the essential functions of the system, for example, based on the six connectors described;
- Characterize the variability potential of these connectors;
- Define functional resonance based on identified dependencies between functions;
- Identify barriers to variability (reduction factors) and specify required performance monitoring.

Table 1 is a Theoretical Framework of Contributions.

2.3. Social Construction of Risk

It must be accepted that the risk is derived from the organization, through its decision-making processes at the strategic, tactical, and operational levels, that is, the risk is a technically constructed partner, according to Dechy (2011) [20], Figueiredo (2018) [2], Filho (2021) [3], Hollnagel (2019) [5],

Hopkins (2008) [7], Le Coze (2013) [31], Levenson (2020) [8], Llory (2014) [9], Pidgeon (2000) [10], Perrow (1999) [11], Rasmussen (2000) [12], Reason (2016) [13], Turner (1997) [14], Vaughan (1996) [15]. And to evaluate it, adequate qualitative methods are needed for the socio-technical question. It is necessary to go beyond the analysis of human and technical factors, compliance with legislation, and good practices to improve risk management. These questions are important and basic for understanding risk management and for preventing Major and Fatal Negative Events.

Table 1. Accident Model Theoretical Framework (Self-elaboration).

Author	Year	Contribution to Safety	Spatial, School, Georeferenced	Major Contribution to Proactive Safety
Greenwood & Woods	1919	Theory about the existence of individual workers' propensity, sought to explain the causality of accidents at work.	United States	Historical View.
Heinrich	1931	Theory in which the accident originates in a linear sequence of events, which he called the Domino Theory.	United States	Beginning of a more technical analysis, and based on negative events.
Turner	1978	Accident incubation concept, and a six-stage development sequence.	England	Dynamic risk management concept, and based on a series of case studies of major negative events.
Perrow	1984	Normal Accident Theory.	United States	Social Construction of Risk, and that accidents are inevitable, as alignment of its causes is unique and not repeatable.
Reason	1997	Swiss Cheese Model" or the theory of multiple causes, does not defend a single cause as triggering a sequence of events that would lead to the accident, but linear combinations of latent conditions and active failures that constitute several chains and, after overcoming safety barriers by the alignment of their vulnerabilities, culminate in the accident.	England	Evolution of Domino Theory and concepts of safety barriers.
Rasmussen	1997	Accimap model, which focuses on failure analysis at the six organizational levels.	Denmark	The concept of performance levels in risk management evolves to the proposal of exogenous and endogenous variables.
Leveson	2004	The STAMP theory is that accidents occur due to the violation of the conditions in which the system was designed.	United States	Evolution of the Accimap Model.
Hollnagel	2004	FRAM is a method that aims to understand how systems work and how variability propagates between their functions, aiming to develop more resilient systems.	Denmark	The complexity of systems, but it is important to seek the representation of complexity, so I present the proposal of the 2 models and principles of Proactive Security.

3. Methodology

The principles of Proactive Safety, Risks, and Emergencies are developed through two models.

3.1. Analysis of Modeling

Study on the elements of the general organization of work in the organization, which were based on the study of major and fatal negative events presented in Barbosa, 2020 [19] and 2022 [16], to know and initiate an analysis, through modeling.

3.1.1. Structured Sociotechnical Approach

The socio-technical approach is divided into organizational, human, and technological factors, which I define as endogenous variables.

As a contribution to this proposal for a sociotechnical approach, I present, based on the case studies research for this work, major and fatal negative events, at the international, national, and local levels (Barbosa, 2022) [16] and the Accimap Model Rasmussen (1997) [27], a proposition of the structured sociotechnical approach, where they are included in this analysis are the contributors: social, economic and other requirements; norms and legislation at the World, Country, State, Municipality and Sector levels, which I define as exogenous variables. As a result of the interaction between exogenous and endogenous variables, positive and negative events will occur, which will be shown in Figure 1.

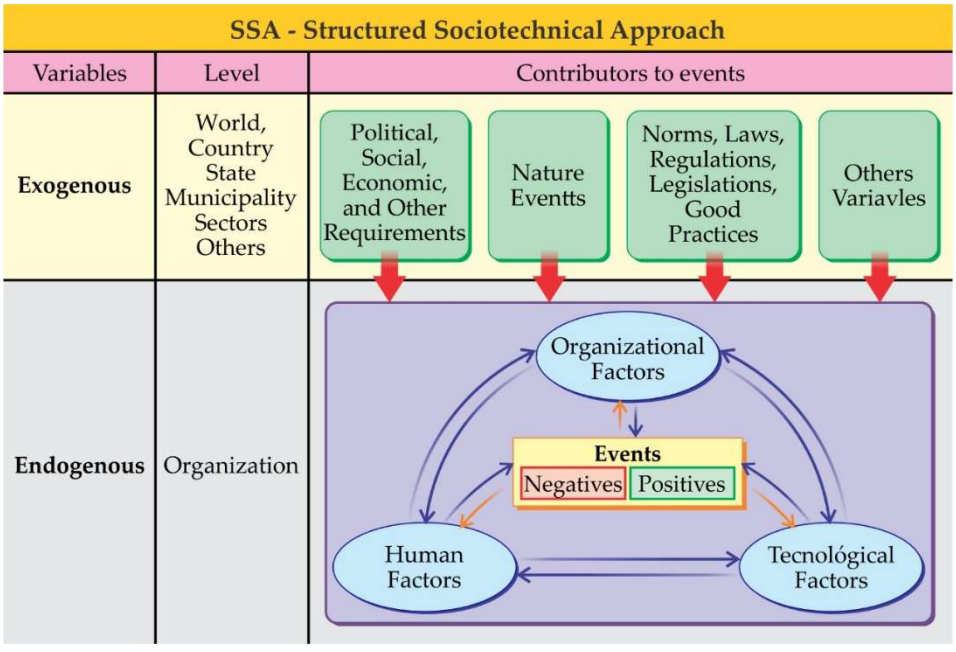

Figure 1. Structural Sociotechnical Approach (Self-elaboration).

The Exogenous Variables are the contributors to the event, external to the organization, a possible classification of level can be at the World, Country, State, Municipality, Sectors, and others, as examples, we can highlight international, national, sectorial, state, municipal standards of security, the economic requirements of recession and economic growth, events of nature, and other variables, which were not verified in the case studies analyzed in Barbosa (2022) [16], such as terrorism, sabotage, theft, and vandalism, among others, present in other unanalyzed negative events.

The Endogenous Variables are the Organizational, Human and Technological Factors.

The Organizational Factors are related to the actions of the Senior Management, Administrative Council, Management, Senior Management, and Advisory/Staff, these functions are in the corporate instance, as an example of actions of this factor are: the definition of investments, corporate procedures, and the decisions that affect the area of operations of the organization, pressures for profitability, continuity, and discontinuity of the business.

Organizational Factors are constitutive elements for Human and Technological Factors issues, an adequate analysis of the organization's risks and emergencies is of vital importance for the prevention of major negative events, and for the success and continuity of the Organization's operations.

The Human Factors are related to the actions of technicians, supervisors, and middle management who work in the operation of the company's activity; as an example of a hierarchical level we can exemplify the case of an oil rig manager, director of a mining company's site and a supervisor of a manufacturing line; cases related to fatigue, stress, and pressure for results are issued to be analyzed in this factor.

The Technological Factors are related to the entire infrastructure for the company's operation, they are the machines, equipment, software, and production and support facilities; equipment failures are related to this factor.

Human Error is the tip of the iceberg, it is what initially appears in major and fatal negative events, it is important to understand the relevance of exogenous and endogenous variables in the systemically structured socio-technical system.

"Focus on the Structured Sociotechnical System and not on Human Error".

First Principle of Proactive Security.

3.1.2. Dynamics of Proactive Safety

To present a dynamic model for Safety Management, the following model is proposed, shown in Figure 2, as an adaptation of the boundaries defined by Rasmussen (1997) [27], separating the activity to be analyzed into three areas:

- Area of Normality - place where the organization must be positioned; occurrence of non-conformities without criticality for a major or fatal negative event;

- Danger Area - occurrence of non-conformities that are critical for a major or fatal negative event, but which have not yet led to the accident. Area of action of the company's management systems, normality must be sought, diagnoses must be developed to seek endogenous and exogenous variables, which may have led to this dangerous area, and through planning, minimize the possibility of recurrence of these issues;

- Accident Area - apply the emergency and mitigation plans, to seek a return to the area of normality, as in the diagnosis of incidents in accidents, the endogenous and exogenous variables that may have led to the incident must be sought, and through planning to minimize the possibility of accidents reoccurring.

The model presents us with an arrow with increased risk, due to social and economic pressures, for profitability, achievement of goals, granting financial bonuses, increased workload, and others, which threaten acceptable limits, for safe and good performance of activities, leading the organization to incidents and accidents.

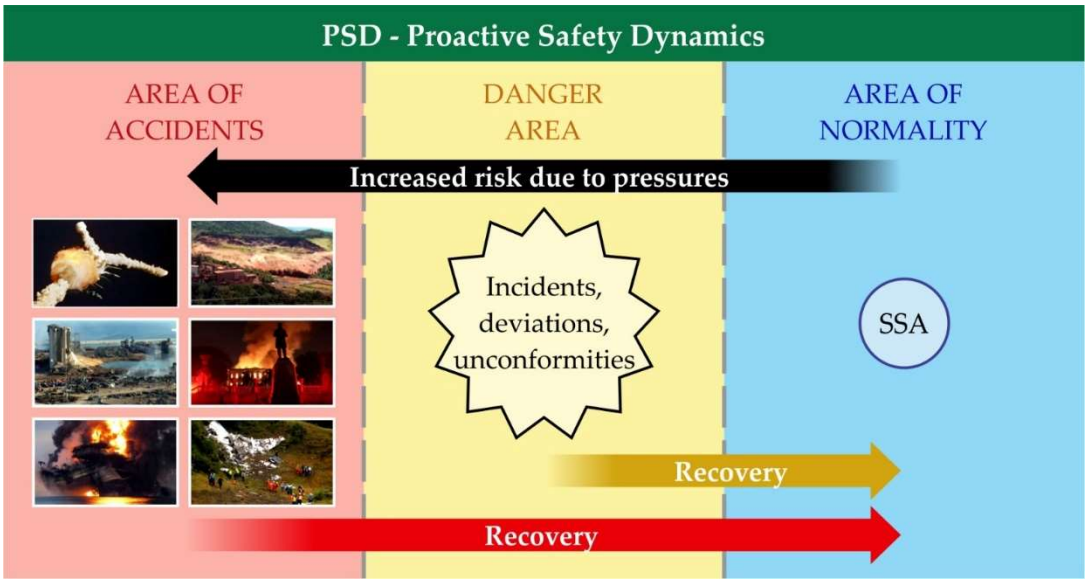

Figure 2. Proactive Safety Dynamics Model (Self-elaboration).

It is important to understand systemically the dynamics of safety management. "Focus on the Dynamics of Proactive Safety and not on Human Error". Second Principle of Proactive Security.

4. Results

Based on the research carried out, the following cases were selected, which represent negative events relevant to the research.

Next, we will present the accidents of Fukushima, Challenger, and Port of Beirut.

4.1. Nuclear Accident in Fukushima

The Fukushima nuclear accident was a nuclear disaster that occurred at the Fukushima Nuclear Power Plant on March 11, 2011, caused by the meltdown of three of the plant's six nuclear reactors (See Figure 3). A 9.0 MW earthquake occurred at 2:46 pm on Friday, March 11, 2011, with the epicenter near Honshu, Japan's largest island.

According to Hollnaghel (2013) [32], immediately after the earthquake, all the nuclear reactors in operation at the Fukushima plant, three of the six, were successfully turned off, but soon after that the external power was lost because the electrical line was shorted, the electrical panel and the transformer went out of order, and a power transmission tower was brought down by the earthquake.

After the loss of external electricity supply, the emergency standby diesel generators were successfully started, but approximately fifty minutes after the earthquake, the tsunami hit the unit, with the wave reaching fourteen to fifteen meters at the perimeter of the plant, the waves broke the ten meters wall of the plant. As the emergency backup generators were located underground, they were flooded with seawater, and electrical equipment, pumps, and fuel tanks were washed away or damaged, as a result, the plant suffered a total loss of electrical power.

The immediate consequence of the loss of electrical energy was the core melting in Reactors one, two, and three, which in turn caused the massive release of radioactive materials into the environment, within a few days, of the reactor buildings of Reactors 1, 3 and 4 exploded because

hydrogen that was produced inside the reactor pressure vessels leaked into the buildings and exploded.

Figure 3. Nuclear Accident in Fukushima (Source: https://brasil.elpais.com/internacional/2021-03-10/10-anos-de-fukushima-golpe-na-reputacao-de-uma-energia-em-retrocesso.html).

The plant began releasing significant amounts of radioactive material on March 12, making it the biggest nuclear disaster since the Chornobyl nuclear accident. The area became contaminated by the presence of radioactive material released over it and such exposure caused the site to be continuously irradiated.

The Fukushima Nuclear Accident Independent Investigation Commission ruled that the nuclear disaster was "artificial" and that its direct causes were all predictable. The report also found that the plant was unable to withstand the earthquake and tsunami. Two employees of Tokyo Electric Power Company died from injuries caused by the earthquake and another six received radiation exposure above the acceptable limit for a lifetime.

An ongoing intensive cleaning program to decontaminate the affected areas and dismantle the plant will take 30 to 40 years. A barrier in the ground, built in an attempt to prevent further contamination of groundwater, decreased the amount of contaminated water collected. In August 2013, however, a huge amount of radioactive water was detected. There were continuous leaks of contaminated water at the plant and some at sea. Factory workers are trying to reduce the leaks through some measures, such as building chemical underground walls, but they still have not significantly improved the situation.

4.2. The Challenger Case

In 1986, 73 seconds after its launch, the space shuttle Challenger exploded (See Figure 4), it was the first accident of the NASA space shuttle program, and all 7 astronauts died (Vaughan, 1996 [15]; Reason, 1997 [26], 2016 [13]).

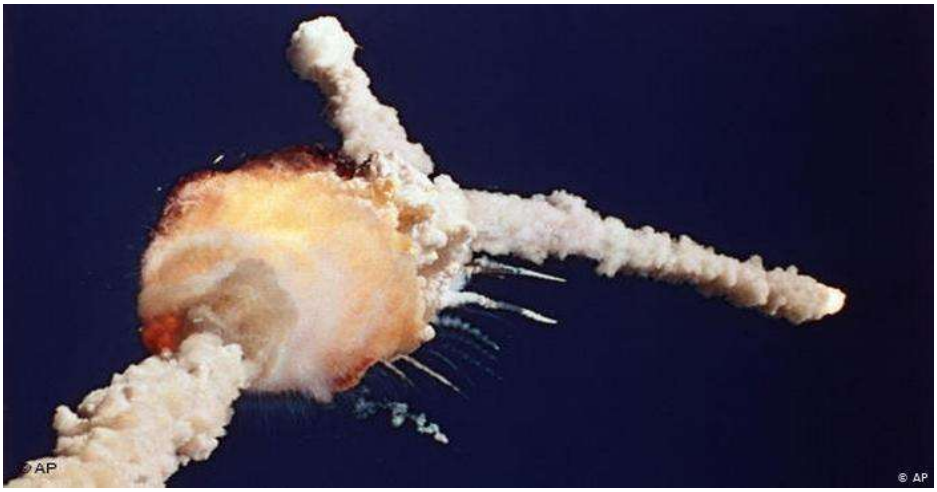

Figure 4. Explosion of the Challenger (Source: https://noticias.r7.com/tecnologia-e-ciencia/acidente-com-onibus-espacial-challenger-ha-30-anos-moldou-nova-geracao-de-espaconaves-29062022).

After 6 delays and with the warning that the temperature was below the ideal for launch, made by mission engineers, and that these low temperatures could cause an accident, NASA decided to launch Challenger.

The O-rings of the Space Shuttle rockets expand and contract as the temperature varies, and on the day of the accident, the temperature at the NASA Space Center was below freezing, causing the rings to contract, and with this contraction, there was a leakage of fuel from the rockets, which, upon finding a source of heat, caused the explosion.

The issue of O-ring safety dates back to 1977 when engineers at the Marshall Space Flight Center repeatedly reported to the Solid Rocket Booster (SRB) Project Manager, George Hardy, that the design of the o-rings provided by Morton Thiokol was unacceptable. Hardy never forwarded these suits to Thiokol, and the o-rings were accepted in 1980.

Still, in the space shuttle design phase, McDonnell Douglas reported that a "burn through" near the fuel tank would result in a failure that would make it impossible to abort the mission. The o-rings were then rated Criticality 1, meaning their failure would result in the spacecraft being destroyed.

Evidence of serious erosion of the o-rings was verified as early as the second space shuttle mission, with the spacecraft Columbia, by the Marshall Center. However, contrary to NASA regulations, the Marshall Center did not report the fact to NASA's Senior Management, keeping the problem limited to its technical area.

In 1985, convinced of the catastrophic potential of the problem, Marshall Center and Thiokol began redesigning the o-rings but did not request a suspension of flights or the use of o-rings. They treated the problem as an acceptable risk.

Thiokol's management initially supported their engineers' recommendation to postpone the Challenger's departure, but in a telephone conversation with a NASA manager, the latter said: "For God's sake Thiokol, when do you want Challenger to be launched? in April?" (NPR, 2016) [33]. NASA's arguments would apparently be that if one o-ring failed, there was a second o-ring. However, NASA's own standards defined that for criticality 1 components, the second element should be redundancy in case of unpredictable failures, and not as a backup of the primary element.

4.3. Explosion in the Port of Beirut

On August 4, 2020, around 6:08 pm, an explosion occurred in the port region in Beirut, the capital of Lebanon, resulting in more than two hundred deaths and more than six thousand injured (See Figure 5). Hours after the event, the news already reported that the catastrophe had occurred in Warehouse 12, where 2,750 tons of pure ammonium nitrate were stored.

Figure 5. Explosion in the Port of Beirut (Self-elaboration).

In the explosion at the Port of Beirut, the Lebanese authorities were informed of the risk of storing the 2.7 tons of Ammonium Nitrate, and the necessary measures were not taken to transfer this material to a suitable storage location that could avoid this tragedy (Human Rights Watch, 2021) [34].

From 2014 to 2020, documents were presented to the authorities of the Port of Beirut, the Prime Minister, and the President of Lebanon, evidence of the organizational factor as a precursor to this great tragedy in which more than 200 people died and 6 thousand were injured in an explosion in the port of Beirut, Lebanon, which completed one year on 08/04/2021.

Storage of ammonium nitrate, without proper port security for years, is what caused the explosion.

No member of the government has yet been penalized for the explosion.

The NGO Human Rights Watch (2021) [34] accuses the Lebanese authorities of criminal negligence. In a 126-page report, the entity documented the numerous violations by politicians and the country's security bodies in the management of this hazardous materials warehouse.

5. Discussion

Parameterization and Highlights, Based on the Proactive Safety Framework, in the Case Studies.

5.1. In the Case of Fukushima

The authorities responsible for the plant were aware of the possibility of larger waves than those designed to contain flooding of the plant by tsunami waves. A historical study revealed that a large tsunami occurred in the middle of the 9th century, estimated at 869 AD and that a researcher had made a strong recommendation to refurbish the plant in 2006, but the recommendation was reportedly declined on the grounds that the tsunami was hypothetical and because the claimed evidence was not accepted by nuclear industry experts.

Recommendations from the IAEA Report (2015) [35] included a few, which specifically address the issue of overconfidence:

- The assessment of natural hazards needs to be sufficiently conservative. The consideration of primarily historical data in establishing the design basis of nuclear power plants is not sufficient to characterize the risks of extreme natural hazards. Even when comprehensive data are available, due to relatively short observation periods, large uncertainties remain in predicting natural disasters.

- The safety of nuclear plants needs to be reassessed periodically to consider advances in knowledge, and necessary corrective actions or compensatory measures need to be implemented promptly.

- Operations experience programs need to include experience from national and international sources. Security improvements identified through operational experience programs need to be implemented promptly. The use of operational experience needs to be evaluated periodically and independently.

Regarding the structured sociotechnical approach, the following stand out:

Economic pressures in relation to the need for high investments to adjust the height of the walls may have been a prominent variable for this and other adjustments.

In relation to dynamic security management, the following stand out:

The recommendation to adjust the height of the wall was made, but there was a lack of planning and execution of actions to address this issue.

5.2. In the Case of the Challenger

The pressure exerted on NASA by society and the government, of 24 launches per year, was not achieved, as they did not even reach 5 per year. In order to ensure that its billionaire budget was maintained, and perhaps increased because despite being reusable, the maintenance of the space shuttle cost millions of dollars with each launch, which were preponderant issues for the erroneous decision to authorize the launch of the space shuttle. Space Shuttle.

After the accident, NASA was prevented from making new missions, while carrying out safety studies and adaptations. It took 3 years for a new launch to be made, and only 22 years later, it sent a civilian into space, not by chance, but another teacher.

Regarding the structured sociotechnical approach, the following stand out:

The social and economic pressures exerted on NASA may have been a prominent variable for the effective decision to launch the rocket.

In relation to dynamic security management, the following stand out:

The warning was given by the rocket engineers, but it was not accepted in a decision by the NASA Directorate and the rocket company.

5.3. In the Case of the Port of Beirut Explosion

In this case, the Lebanese authorities were unable to recognize the risk and transfer the ammonium nitrate to a suitable warehouse.

Around the world, countless numbers including large amounts of the same agricultural fertilizer that detonated in Beirut began to appear: in Dakar, authorities found 3,000 tons of ammonium nitrate in warehouses, in Chennai, port officials admitted they were unsafely storing 800 tons of the chemical, Romanian authorities discovered nearly 9,000 tons, including 5,000 tons in a single warehouse. Disaster prevention is not just about preventing distributors from improperly storing and transporting large amounts of dangerous goods, it is important to check several issues such as supervision, communication, and preventive maintenance.

Regarding the structured sociotechnical approach, the following stand out:

Political and management disorganization may have been a prominent variable, due to the non-effectiveness of adequate storage of Ammonium Nitrate.

In relation to dynamic security management, the following stand out:

The alert was made to the authorities, but the necessary adjustments were not made.

6. Conclusions

From the cases presented of major and fatal negative events, and from the propositions presented in this article, it is suggested that traditional risk assessments need to be reassessed. The assessment of exogenous and endogenous pressures on organizations, the structured socio-technical system, the dynamic management of safety, and the systemic view of safety, provided us with a way to identify contributing factors to these major accidents. In this sense, it is a complement to traditional risk assessments. In risk management, it is important to use the precautionary principle and conservative measures, and when in doubt, re-evaluate and use the opinion of experts, to avoid the major accidents that were described in the cases presented in this article. A decision-making process that prioritizes the production process, achievement of goals, and financial issues, and puts Safety in the background, can lead to bigger and more fatal negative events. These two principles of Proactive Safety, Risks, and Emergencies are proposed: Focus on the Structured Sociotechnical System and not on Human Error and Focus on Proactive Security Dynamics and not on Human Error. Those principles are a complement to traditional risk assessments and can provide us with bases for analysis, to prevent and minimize these Major and Fatal Negative Events.

Contributions: Washington Barbosa: conceptualization, methodology, writing—original draft preparation, visualization, investigation; Luiz Ricardo Moreira: visualization, writing—review and editing; Gilson Brito: conceptualization, writing—review and editing, validation; Assed N. Haddad: conceptualization, supervision, writing—review and editing, validation; Mario Cesar Vidal: conceptualization, supervision, writing—review and editing, validation. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Dekker, S.W. The Field Guide to Understanding Human Error. Ashgate, 2006.

[2] Figueiredo, M.G.; Alvarez, D.; Adams, R.N. O acidente da plataforma de petróleo P-36 revisitado 15 anos depois: da gestão de situações incidentais e acidentais aos fatores organizacionais. Caderno de Saúde Pública 34 (4), 1–12, 2018. DOI: https://doi.org/10.1590/0102-311X00034617.

[3] Filho, A.P.G.; Ferreira, A.M.S.; Ramos, M.F.; Pinto, A.R.A.P. Are we learning from disasters? Examining investigation reports from National government bodies. Safety Science, 2021. DOI: https://doi.org/10.1016/j.ssci.2021.105327.

[4] Furuta, K. "Resilience engineering: A new horizon of systems safety". In: Ahn, J.; Carson, C.; Jensen, M.; et al. (eds.), Reflections on the Fukushima Daiichi Nuclear Accident: Toward Social-Scientific Literacy and Engineering Resilience, Part V, chapter 24, New York, USA, Springer Open, 2015.

[5] Hollnagel, E. The FRAM Model Interpreter FMI: software for FRAM model analysis. Jul. 2019. Available at: https://functionalresonance.com/the-fram-model-interpreter.html. Accessed: Oct. 10, 2021.

[6] Hopkins, A. Safety, Culture and Risk: The organizational causes of disasters, CCH, Sydney, Australia., 2005.

[7] Hopkins, A. Failure to learn: the BP Texas City Refinery Disaster. CCH, Sydney, Australia, 2008.

[8] Leveson, N. "Safety III: A Systems Approach to Safety and Resilience", MIT Engineering Systems Lab, Working paper, Jul. 2020. Available at: http://sunnyday.mit.edu/safety-3.pdf.

[9] Llory, Michel. O acidente e a organização/Michel Llory e René Montmayeul; Tradução de Marlene Machado Zica Vianna Belo Horizonte: Fabrefactum, 2014. 192p.

[10] Pidgeon, N.; O'Leary, M. Man-Made Disasters: Why Technology and Organizations (Sometimes) Fail. Saf. Sci. 34 (1–3), 15–30, 2000.

[11] Perrow, C. Normal accidents: Living with high-risk technologies. Princeton University Press, 1999.

[12] Rasmussen, J.; Svedung, I. Proactive Risk Management in a Dynamic Society. 1. ed. Karlstad, Swedish Rescue Services Agency, 2000.

[13] Reason, J. Organizational Accidents Revisited. CRC Press - Taylor & Francis Group, 2016.

[14] Turner, B.A.; Pidgeon, N.F. Man-made Disasters, 2nd Edition. Butterworth- Heinemann, London, UK, 1997.

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

[16] Barbosa, W.R. MODULE 3 - Case Studies of Major Negative and Fatal Events Internationally and in Brazil. Proactive Management Blog, 2022. Available at: https://gestaoproativawb.blogspot.com/2022/02/modulo-3-estudos-de-casos.html. (In Portuguese)

[17] Turner, B.A. Causes of Disaster: Sloppy Management. British Journal of Management, 5, pp.215-219, 1994. DOI: https://doi.org/10.1111/j.1467-8551.1994.tb00172.x.

[18] Qureshi, Zahid H. A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems, 2008.

[19] Barbosa, W.R. Contribuição da Ergonomia para o Desenvolvimento da Segurança Proativa, Riscos e Emergências dos Resíduos dos Produtos Perigosos da Fiocruz. Congresso da Abergo 2020. Available at: www.even3.com.br/Anais/abergo2020/294483-CONTRIBUICAO-DA-ERGONOMIA-PARA-O-DESENVOLVIMENTO-DA-SEGURANCA-PROATIVA-RISCOS-E-EMERGENCIAS-DOS-RESIDUOS-DOS-PRO. (In Portuguese)

[20] Dechy, N.; et al. Learning lessons from accidents with a human and organizational factors perspective: deficiencies and failures of operating experience feedback systems. EUROSAFE Forum 2011. Available at: https://www.researchgate.net/publication/233997934_Learning_lessons_from_accidents_with_a_human_and_organisational_factors_perspective_deficiencies_and_failures_of_operating_experience_feedback_systems.

[21] Hollnagel, E.; Woods, D.D; Leveson, N. Resilience Engineering: Concepts and Precepts. 1st. ed. Burlington, Ashgate, 2006.

[22] Greenwood, M.; Woods, H.M. The incidence of industrial accidents upon individuals with special reference to multiple accidents. Industrial Fatigue Research Board, AMedical Research Committee, Report No. 4. Her Britannic Majesty's Stationary Office, London, 1919.

[23] Heinrich, H. Industrial Accident Prevention. McGraw-Hill, New York, 1931.

[24] Turner, B.A. Man-Made Disasters, Wykeman, London, 1978.

[25] Perrow, C. Normal accidents: Living with high-risk technologies. New York: Basic Books, 1984.

[26] Reason, J. Managing the Risk of Organisational Accidents. Ashgate, 1997.

[27] Rasmussen, J. "Risk management in a dynamic society: A modelling problem", Safety Science, v. 27, n. 2–3, pp. 183–213, 1 Nov. 1997. DOI: https://doi.org/10.1016/S0925-7535(97)00052-0.

[28] Leveson, N. "A new accident model for engineering safer systems," Saf. Sci., vol. 42, no. 4, pp. 237-270, 2004. DOI: https://doi.org/10.1016/S0925-7535(03)00047-X.
[29] Hollnagel, E. Barriers and accident prevention. 1st. ed. Surrey, Ashgate, 2004.
[30] Hollnagel, E. FRAM - the Functional Resonance Analysis Method: Modeling complex socio-technical systems. Farnham, Ashgate, 2012.
[31] Le Coze, J.C. What Have We Learned about Learning from Accidents? Post-Disasters Reflections. Safety Science 51 (1), 441–543, 2013. DOI: https://doi.org/10.1016/j.ssci.2012.07.007.
[32] Hollnagel, E.; Fujita, Y. "The Fukushima disaster-systemic failures as the lack of resilience", Nuclear Engineering and Technology, v. 45, n. 1, pp. 13–20, Feb. 2013. DOI: https://doi.org/10.5516/NET.03.2011.078.
[33] NPR. Challenger Engineer Who Warned of Shuttle Disaster Dies. 2016. Available at: https://www.npr.org/sections/thetwo-way/2016/03/21/470870426/challenger-engineer-who-warned-of-shuttle-disaster-dies.
[34] Human Rights Watch. "They Killed Us from the Inside". 2021. Available at: https://www.hrw.org/report/2021/08/03/they-killed-us-inside/investigation-august-4-beirut-blast.
[35] IAEA. The Fukushima Daiichi accident, International Atomic Energy Agency, Vienna, Austria, 2015. Available at: https://www.iaea.org/publications/10962/the-fukushima-daiichi-accident.