Integrating Functional Block Diagrams and Systems-Theoretic Process Analysis: A Case Study of a Nuclear Power Station

Article *in* International Journal of Safety and Security Engineering · April 2024

DOI: 10.18280/ijsse.140205

4 authors, including:

Islem Berri
Université 20 août 1955-Skikda
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Zennir Youcef
Université 20 août 1955-Skikda
113 PUBLICATIONS **399** CITATIONS
SEE PROFILE

International Journal of Safety and Security Engineering
Vol. 14, No. 2, April, 2024, pp. 359-372
Journal homepage: http://iieta.org/journals/ijsse

Integrating Functional Block Diagrams and Systems-Theoretic Process Analysis: A Case Study of a Nuclear Power Station

Islem Berri[1*], Youcef Zennir[2], El-Arkam Mechhoud[2], Yiliu Liu[3]

[1] LRPCSI Laboratory Skikda, Université 20 Aout 1955 Skikda, Skikda 21000, Algeria
[2] Automatic Laboratory of Skikda, Université 20 Août 1955 Skikda, Skikda 21000, Algeria
[3] Department of Mechanical and Industrial Engineering Faculty of Engineering, NTNU University, Trondheim NO-7491, Norway

Corresponding Author Email: y.zennir@univ-skikda.dz

https://doi.org/10.18280/ijsse.140205

Received: 25 January 2024
Revised: 30 March 2024
Accepted: 8 April 2024
Available online: 26 April 2024

Keywords:
risk assessment, functional block diagram (FBD), systems-theoretic process analysis (STPA), unsafe control actions, nuclear power station

ABSTRACT

Hazard analysis and risk assessment are critical for ensuring safety and reliability in complex systems. This article presents a combined approach to hazard analysis and risk assessment using Functional Block Diagrams (FBD) and Systems-Theoretic Process Analysis (STPA) methods. The FBD method is a versatile and intuitive diagrammatic technique used to describe the functions and interrelationships of complex systems. It represents the system as a set of interconnected blocks, each depicting a specific function, which collectively defines the system's behaviour. On the other hand, STPA is an advanced safety analysis method focusing on control structures and the interaction between components. It identifies potential unsafe control actions by analysing the information flow and the system's feedback mechanisms. The two methods are complementary and can be integrated to provide a more effective and efficient approach to hazard analysis and risk assessment. A case study of a nuclear power plant is used to demonstrate the benefits of the combined approach. Practical considerations for implementing the approach are discussed and compared with other hazard analysis and risk assessment methods. The article concludes with suggestions for future research and development in this area, highlighting the potential impact of the combined FBD-STPA approach for improving safety and reliability in complex systems.

1. INTRODUCTION

The relentless march of technological progress has ushered in an era defined by intricate and automated complex systems [1], profoundly affecting numerous domains, with none bearing greater significance than the realm of energy management [2]. The relentless pursuit of energy efficiency, sustainability, and unwavering reliability has propelled innovation to unprecedented heights in recent decades [3]. This relentless drive has woven a multifaceted tapestry of sophisticated automated complex systems within energy generation [4]. Among these technological wonders, the nuclear power station stands resolutely as an imposing linchpin in global energy production [5, 6].

The origins of the nuclear power station harken back to the mid-20th century, marked by noteworthy achievements in harnessing nuclear energy [7]. From the seminal triumphs of the Manhattan Project to the erection of the inaugural civilian nuclear power facility in Shipping port, Pennsylvania, in the annus mirabilis of 1958, history bears witness to the tenacious ingenuity that has irrevocably sculpted the landscape of nuclear power [8].

Nonetheless, it is imperative to acknowledge that, despite the prodigious advantages furnished by nuclear power, it carries within its core an accompanying suite of intrinsic perils and hazards that perpetually hover in the collective cognizance [9].

These automated complex systems, characterized by their meticulous engineering and stringent safety protocols, remain in the intricate web of potentiality for cataclysmic misadventures [10, 11].

The Table 1 lists significant nuclear incidents from 1980 to 2020. The Saint-Laurent Nuclear Power Plant Incident in 1980 was a result of an increase in the reactor's thermal energy, leading to the melting of the core [12]. The Chornobyl disaster in 1986 was a nuclear accident that occurred at the No. 4 reactor in the Chernobyl Nuclear Power Plant, near the city of Pripyat in the north of the Ukrainian SSR in the Soviet Union [13]. The Tokaimura nuclear accident in 1999 was a criticality accident that occurred due to improper handling of liquid uranium fuel [12]. The Davis-Besse Nuclear Power Plant Incident in 2002 was a serious nuclear safety incident where a large hole was discovered in the reactor vessel head caused by corrosion [12]. The Kashiwazaki-Kariwa Nuclear Power Plant Earthquake in 2007 resulted from an earthquake that led to the shutdown of the nuclear power plant. The Fukushima Daiichi nuclear disaster in 2011 was a nuclear accident at the Fukushima Daiichi Nuclear Power Plant in Ōkuma,

Fukushima, Japan, which began on March 11, 2011 [14]. The increase in airborne radioactivity in Europe in 2017 was detected in Europe during autumn 2017, starting from the last days of September. The Radiation release during an explosion at the Russian nuclear missile test site in 2019 was a mysterious explosion that occurred at a Russian naval test range in the White Sea in August 2019. These incidents highlight the inherent risks of nuclear power and underscore the importance of stringent safety protocols and continuous improvement in crisis management strategies [15].

Accurate statistics related to the development of technologies in automated systems for energy generation [16].

Table 1. Major nuclear incidents (1980-2020)

Year	Significant Nuclear Incidents	Name of Incident
1980	1	Saint-Laurent Nuclear Power Plant Incident
1986	1	Chernobyl disaster
1999	2	Tokaimura nuclear accident
2002	1	Davis-Besse Nuclear Power Plant Incident
2007	1	Kashiwazaki-Kariwa Nuclear Power Plant Earthquake
2011	1	The Fukushima Daiichi nuclear disaster
2017	1	Airborne radioactivity increase in Europe
2019	1	Radiation release during explosion at Russian nuclear missile test site

Table 2. Development of energy generation technologies (1980-2020)

Year	Solar (GW Installed)	Wind (GW Installed)	Nuclear (GW Capacity)	Hydro (GW Capacity)
1980	0.2	0.1	150	250
1985	0.8	0.5	175	280
1990	2.5	2.0	200	320
1995	6.0	7.5	210	350
2000	15.0	10.0	235	380
2005	35.0	22.0	250	400
2010	55.0	45.0	260	420
2015	140	110	275	450
2020	260	220	280	480

The Table 2 shows the installed capacity (in gigawatts) of four energy generation technologies: solar, wind, nuclear, and hydro. The data are obtained from authoritative sources and span four decades from 1980 to 2020. The table illustrates the rapid growth of renewable energy sources such as solar and wind and the relatively stable contribution of nuclear and hydro power. It also provides a background for the discussion of the advantages and challenges of nuclear power as a sustainable energy option.

The Figure 1 is a graphical representation of the data in Table 1, using vertical bars to compare the installed capacity of each energy generation technology over time. The figure highlights the trends and patterns of the data, such as the exponential increase of solar and wind power, the slight decline of nuclear power after 2010, and the modest growth of hydropower. The figure complements the table by providing a visual overview of the development of energy generation technologies [17]. They consider safety incidents, environmental impacts, and technological challenges. The graphical data depicted in Figure 1, which contrasts the installed capacities of various energy generation technologies over time, is crucial in supporting risk assessment. The sharp rise in solar and wind capacities suggests a transition towards renewable energy sources, generally associated with lower risk profiles. This shift is significant for risk assessment as it involves resource management considerations and the intermittency of renewable energy supplies. The slight decline in nuclear power post-2010 and the steady growth of hydropower may reflect heightened environmental and safety concerns, which are integral to risk assessment. These trends also indicate the impact of technological advancements that can mitigate risk, such as more efficient solar panels or improved wind turbine designs. Additionally, changes in policy and regulations that influence the energy mix can alter risk profiles, emphasizing the need for ongoing risk assessment to navigate the evolving energy landscape. Overall, the visual overview provided by Figure 1 facilitates a quick comprehension of how energy generation has progressed and where potential risks or opportunities might exist, enabling stakeholders to make informed decisions about energy resource allocation and risk mitigation strategies [18].

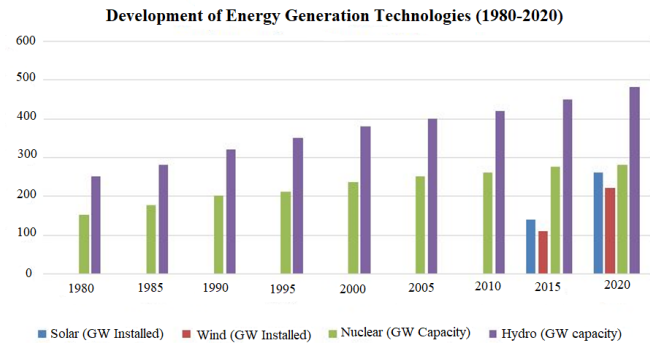

Figure 1. Graphical columns of development of energy generation technologies (1980-2020)

Table 3. Risk index in energy generation systems (1980-2020)

Year	Solar	Wind	Nuclear	Hydro
1980	35	40	55	30
1985	34	33	52	28
1990	30	32	50	25
1995	22	29	48	23
2000	20	27	45	20
2005	16	23	42	18
2010	13	20	40	16
2015	10	10	38	15
2020	8	5	35	14

Table 3 shows the risk accumulation in energy generation systems from 1980 to 2020, based on an index that considers safety incidents, environmental impacts, and technological challenges. The table indicates that nuclear power has the highest risk level among the four energy sources, followed by hydro, solar, and wind power. The table also reveals that the risk levels of all energy sources have decreased over time, suggesting improvements in safety and reliability.

The observed reduction in risk levels for various energy generation systems, as illustrated in Figure 2, can be attributed to advancements in safety technologies, enhanced risk analysis methods, regulatory improvements, lessons learned from past incidents, and increased public and environmental awareness.

Significant progress in safety technologies, particularly in the nuclear sector, has led to improved reactor designs, better containment structures, and advanced monitoring systems that preemptively address potential issues. The evolution of risk analysis methodologies, such as the more nuanced Probabilistic Risk Assessment (PRA), has provided deeper insights into potential risks and their mitigation strategies. Stricter safety standards and more comprehensive regulatory oversight have further driven the adoption of improved safety practices across the energy sector.

The industry has also benefited from the lessons learned from historical incidents like Chernobyl and Fukushima, leading to the implementation of more rigorous safety protocols and emergency response strategies. Moreover, heightened public and environmental consciousness has pressured energy companies to adopt safer and more sustainable practices.

The convergence of risk levels among different energy sources indicates a global trend towards higher safety and reliability standards, reflecting a collective commitment to ensuring that energy generation is efficient and safe for workers, communities, and the environment. This positive trend is expected to continue as the development of safety technologies and risk analysis methods advances, further reducing risk indices in the future [19].

To calculate a risk index for energy generation systems, a formula that incorporates various risk factors is necessary. An example of how you might calculate such an index:

Identify Risk Factors: Determine the factors that contribute to the risk for each energy type [20]. Common factors include:

- Incident Frequency (IF): The number of incidents per year.
- Incident Severity (IS): The average severity of incidents.
- Environmental Impact (EI): The impact of the energy source on the environment.
- Reliability (R): The consistency and uptime of the energy source.

Assign Weights to Each Factor: Each factor is given a weight based on its importance to the overall risk [21].

$(w\_\{IF\})$: Weight for Incident Frequency

$(w\_\{IS\})$: Weight for Incident Severity

$(w\_\{EI\})$: Weight for Environmental Impact

$(w\_\{R\})$: Weight for Reliability

Collect Data: Obtain data for each factor for the assessed energy types.

Normalize the Data: Ensure that all data is on a comparable scale, typically from 0 (best) to 1 (worst).

Calculate the Risk Index: Use the following formula to calculate the risk index for each energy type:

$$Risk\ Index = (IF * wIF) + (IS * wIS) + (EI * wEI) + (R * wR) \quad (1)$$

Aggregate the Scores: Sum the weighted factors to get the overall risk index for each energy type [22]. An example with weights and normalized data:

The weights are as follows:

$$\begin{aligned} (w\_\{IF\}) &= 0.4 \\ (w\_\{IS\}) &= 0.3 \\ (w\_\{EI\}) &= 0.2 \\ (w\_\{R\}) &= 0.1 \end{aligned} \quad (2)$$

The normalized data for a particular year 2000 for solar energy is:

$$\begin{aligned} IF &= 0.1 \\ IS &= 0.2 \\ EI &= 0.05 \\ R &= 0.9 \end{aligned} \quad (3)$$

The risk index for solar energy would be calculated as follows:

$$Risk\ IndexSolar = (0.1*0.4) + (0.2*0.3) + (0.05*0.2) + (0.9*0.1)$$
$$Risk\ IndexSolar = 0.20 \quad (4)$$

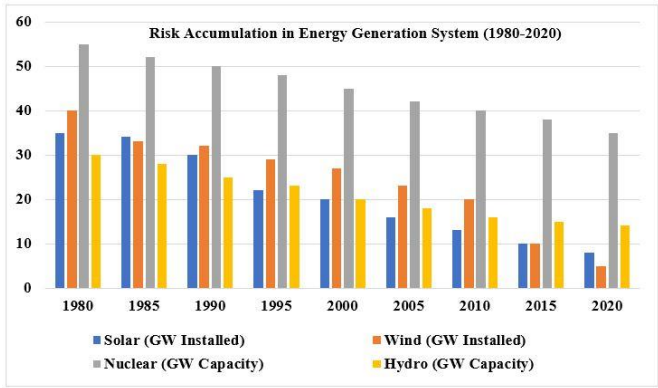

Figure 2. Graphical columns risk accumulation in energy generation systems (1980-2020)

Figure 2 is a graphical representation of the data in Table 2, using columns to display the risk levels of each energy source over time. The figure illustrates the trends and patterns of risk accumulation in energy generation systems more clearly than the table. The figure shows that nuclear power experienced the most significant reduction in risk level, while wind power maintained the lowest risk level throughout the period. The figure also shows that the gap between the risk levels of different energy sources has narrowed over time, indicating a convergence of safety and reliability standards.

2. QUANTITATIVE ANALYSIS METHODS

Exploring the annals of history, we embark on a journey tracing the evolution of these methodologies over the passing decades [23]. The 1970s witnessed the inception of Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) methodologies, while the 1980s marked the advent of Probabilistic Risk Assessment (PRA) techniques [24]. The subsequent years witnessed ongoing refinement [25], culminating in contemporary paradigms such as STPA and FBD methodologies.

Within risk analysis, these methods serve as pivotal instruments, offering distinctive vantage points for scrutinizing and mitigating the inherent hazards endemic to intricate automated systems [26]. By subjecting their applicability to the crucible of nuclear power plants and other energy generation systems, we aspire to illuminate the path forward, ensuring these pivotal technological endeavours' safety, reliability, and sustainability [27].

STPA presents several conspicuous advantages within the

domain of hazard analysis [28]. Foremost, it excels in holistic hazard identification, deftly uncovering complex and often nuanced risks lurking within a system's labyrinthine pathways [29]. Its unwavering focus on control structures and system constraints proffers a panoramic view of potential hazards, ensuring the inclusion of even those perils that might elude other methodologies [30]. STPA espouses a human-centric approach, reckoning with human factors and their interplay with automated systems [31]. This characteristic renders it particularly well-suited for industries wherein the interplay between humans and machines is paramount for safety, such as the precincts of nuclear power plants and aviation [32]. STPA evinces adaptability and flexibility, amenable to application across a spectrum of system types throughout their life cycles. It spans the gamut from design and development to operational deployment and maintenance.

However, the STPA methodology does not emerge unscathed from the crucible of scrutiny. Primarily, its intricate nature can prove arduous to implement, demanding an in-depth comprehension of system behavior and safety precepts. This restricts accessibility for individuals lacking specialized expertise. Moreover, conducting STPA analyses may impose a resource-intensive burden, requisitioning temporal investments and personnel fortified with the requisite knowledge. This resource profligacy can render its practicality wanting for organizations endowed with finite resources. Lastly, STPA invokes subjectivity in the hazard and control structure identification process, thereby introducing an element of variability into the analysis. Diligent oversight becomes imperative to engender outcome consistency.

The fusion of STPA with FBD holds the potential to amplify hazard analysis and risk assessment within intricate systems. This union furnishes a holistic comprehension by harnessing the unique strengths of both STPA and FBD. FBD bequeaths a visual tableau of system functions and dependencies, enriching STPA's hazard analysis. It enhances traceability by leveraging FBD's graphical manifestation to chart the nexus between control structures unearthed by STPA and specific constituents or functions within the system. This augmentation fortifies the tower of safety requisites traceability. In addition, the merger facilitates the formulation of efficacious mitigation strategies. Implementing FBD into STPA's domain empowers organizations to craft targeted and potent control measures. The visual panache emanating from FBD assists in prioritization and the expedited implementation of these mitigation strategies. Nonetheless, amalgamating STPA with FBD ushers in its suite of challenges. This integrated approach can primarily accentuate the complexity inherent in the analysis process, especially when confronting vast and intricate systems. Managing this augmented intricacy may entail a heightened temporal and resource commitment.

Furthermore, expertise remains an indispensable requirement. While FBD complements STPA, more is needed to prevent the necessity for proficiency in both methodologies. Organizations must ensure the presence of personnel endowed with the requisite knowledge and competencies to execute this amalgamated analysis adroitly. The confluence of STPA and FBD bequeaths a robust framework for hazard analysis and risk assessment within intricate systems. Nevertheless, this synergy mandates meticulous stewardship of complexity and resources alongside a workforce dexterous in the intricacies of both methodologies [33]. A comprehensive hazard analysis and risk assessment are imperative to adroitly navigate these perils and safeguard the integrity and dependability of intricate systems. The former involves identifying potential hazards, their etiologies, consequences, and likelihood of manifestation. The latter entails the quantification of the overarching risk quotient affiliated with a specific system or process, predicated upon the identified hazards and their attendant repercussions [34].

FBD and STPA emerge as two symbiotic paradigms for hazard analysis and risk assessment within this landscape [35]. FBD wields a graphical modelling artifice that affords a top-down panorama of a system, delineating how distinct constituents and subsystems coalesce and conspire to fulfil distinct functions [36]. STPA proffers a structured modus operandi for hazard analysis, directing its gaze towards identifying and examining control structures and safety constraints integral for forestalling or ameliorating hazards. By amalgamating FBD and STPA, a more comprehensive and productive framework for hazard analysis and risk assessment in intricate systems is attainable. This harmonious amalgamation bequeaths a more exhaustive, precision-guided insight into intricate systems' latent hazards and risks. This enlightenment, in turn, enables potent risk management strategies to be formulated. Ultimately, this confluence augments the safety and dependability of intricate systems, diminishing the probability and severity of mishaps while safeguarding human well-being, the environment, and property.

This paper presents an integrated approach combining FBD and STPA for risk and hazard analysis of complex systems. We illustrate the application of this approach to a case study of a nuclear power plant and show how it can identify and evaluate the risks and hazards associated with the operation of the plant. We also compare the results of this approach with those of the traditional FTA and PRA methods and discuss each method's advantages and disadvantages. The paper is organized as follows: Section 2 introduces the background and motivation of this research; Section 3 describes the methodology of FBD and STPA and how they can be integrated; Section 4 presents the case study of a nuclear power plant and the results of the risk and hazard analysis using the proposed approach; Section 5 compares and contrasts the proposed approach with the traditional methods of FTA and PRA; Section 6 concludes the paper and suggests some directions for future work.

3. METHODOLOGY OVERVIEW

The Systems-Theoretic Accident Model and Processes / Systems-Theoretic Process Analysis (STAMP/STPA) represent an innovative analytical methodology pioneered by the erudite Professor Nancy G.

Leveson of the esteemed Massachusetts Institute of Technology [37].

Initially conceived for aerospace applications, STAMP/STPA has extended its relevance to many domains, including vital social infrastructure sectors [38].

Conventional analytical approaches such as FTA and Failure Mode and Effect Analysis (FMEA) [39], dating back to the 1960s, primarily concentrate on dissecting singular equipment malfunctions or organizational shortcomings [40, 41]. Nonetheless, when grappling with intricate, continually evolving modern systems, these methodologies exhibit constraints of paramount significance [42].

Within intricate systems, mishaps frequently germinate

from errant individual components and the convoluted web of ensuing miscommunications. STAMP/STPA, crafted by Professor Nancy G. Leveson, adheres to a top-down strategy that endorses a panoramic perspective of interactions amongst intra-system components. Its primary objective? To exert command over the emergence of unintended properties and forestall catastrophic incidents [43, 44]. The STAMP/STPA analysis procedure commences methodically with Step 1, explicitly delineating mishaps and hazards in the system's domain. These encompass adverse consequences resulting in the depletion of stakeholder value and pivotal safety thresholds requisite for hazard management. In Step 2 (Preparation 2), the meticulously constructed control structure scrutinizes system constituents, including subsystems, equipment, and organizations. This dissection takes into account their interrelationships and potential contributions towards the establishment of safety constraints [43].

Step 1 zealously identifies unsafe control actions (UCAs), which are pivotal for safeguarding the system, among the control actions issued by controllers. Four guiding principles facilitate UCA identification, accentuating the indispensability of proffering precise control actions and meticulous attention to timing and sequencing. In Step 2, determining hazard causal factors (HCFs) linked to UCAs transpires, aligned with creating control loop diagrams referencing an abstract cause-and-effect scenario generation model. This methodology yields a systematic framework for scrutinizing intricate systems, laying bare latent hazards, and fortifying safety protocols across various domains.

The STPA method explicates hazards as specific system states or conditions that may precipitate accidents or losses in conjunction with specific environmental factors under worst-case conditions [44]. These hazards can emanate from the actions of sundry controllers ensconced within a system and from interactions amongst an array of system components. The STPA approach pivots on the top-down assessment of dynamic interactions traversing distinct elements of the system via a concatenation of control loops. The culmination? The development of a hierarchical control structure comprising assemblies of control loops serves as an accurate representation of the system model—the paradigmatic configuration of an STPA control loop. Every control loop encompasses indispensable constituents, encompassing a controller endowed with the responsibility of instigating control actions, actuators to execute these actions, the controlled process itself, and sensors instrumental in furnishing feedback to the controller. The governance of control actions succumbs to control algorithms that preside over the decision-making panorama of the controller and the process models encapsulating the controller's inner decision-making mechanics. Significantly, controllers and controlled processes exchange bidirectional information with external components.

In the context of STPA, the term "loss" conveys any emergent system scenario mandated for preclusion. The overarching objective remains the efficacious administration and reduction of hazards entwined with these undesired events.

The STPA methodology unfolds across four pivotal stages:

- Delineating the intent of analysis necessitates identifying system losses, system-level hazards, and concurrent safety prerequisites.
- Erection of a model encapsulating the control structure, encompassing the gestation of a hierarchical control structure interlinking feedback and control loops.
- Discerning UCAs pertain to control actions with the latent capability to engender hazards under worst-case circumstances.
- Identifying loss scenarios encompasses scenarios emerging from the amalgamation of various causal factors (CFs) endowed with the potential to instigate UCAs and prospective losses.

Systemic hazards crystallize by assessing how system control decisions and actions may jeopardize specified security thresholds. UCAs materialize in instances where control actions have the propensity to contravene safety constraints. The elucidation of scenarios leading to UCAs aligns with four pivotal criteria: (a) abstaining from control actions, (b) erroneously issuing control actions, (c) imprecise timing or sequence of control actions, and (d) the application of control actions for an incorrect duration or premature cessation. When pitted against conventional hazard analysis methodologies such as FTA, FMEA, and Hazard and Operability Analysis (HAZOP), several inherent distinctions surface, each shedding luminosity on the unique merits and applications of STPA [45].

Primarily, STPA's superlative attribute lies in its systemic vantage point. It plunges deep into the labyrinthine network of dynamic interactions, weaving through system components, control structures, and external variables. Unlike conventional approaches, STPA excels at excavating complex system-level hazards and vulnerabilities that often lay cloaked in obscurity [46]. Furthermore, STPA champions a top-down analytical modality, allowing analysts to inaugurate their scrutiny with a bird ' s-eye grasp of the system's panorama before descending into the minutiae of its constituents. This hierarchical strategy strikes a critical equilibrium, encapsulating the broad context while assuring the meticulous investigation of nuanced perils.

STPA's forte further distinguishes itself in its adeptness at tackling intricate systems effectively. These intricate systems invariably boast an abundance of interactions and dependencies susceptible to birthing emergent hazards. The comprehensive outlook of STPA renders it particularly adept at identifying these latent risks, distinguishing it from methodologies that falter in their detection. Lastly, STPA epitomizes versatility and is amenable to synergistic confluence with other analytical techniques like FTA and FMEA. This synergy facilitates a comprehensive hazard analysis that fuses the systemic insights of STPA with the meticulous assessments offered by traditional methods on the component level. Nevertheless, selecting the appropriate analytical method must hinge on the unique attributes and objectives underpinning the hazard analysis requisite for a specific system or process. STPA's acumen truly shines when marshalled for unravelling the enigma of complex systems, where comprehension of systemic interactions and emergent hazards assumes paramountcy.

The Table 4 shows comparison between (STPA) and other safety analysis methods reveals distinct differences and advantages. STPA's systems thinking approach, which focuses on control structures and their failures, offers a holistic view of system interactions. This contrasts with the more isolated component-level examination of FMEA, HAZOP's operational focus, and FTA's event-level tracing. STPA's integration of human factors is a significant divergence from the other methods, which typically do not prioritize this aspect [47]. Its ability to handle complex, dynamic systems with emergent behaviours sets it apart from methods suited for

static systems with well-understood components or failure logic. The proactive nature of STPA in identifying unsafe control actions before they lead to hazards is another key advantage, as it allows for early intervention and prevention. Overall, STPA's comprehensive approach to considering technical components, human factors, and organizational aspects makes it particularly beneficial for complex, socio-technical systems where traditional methods might only partially address dynamic interactions. This proactive and inclusive methodology enhances the overall safety and reliability of the system [48].

4. THE FUNCTIONAL BLOCK DIAGRAM

The FBD: A Potent Visual Tool in Systems Engineering and Software Engineering. An FBD emerges as a formidable visual instrument entrenched in systems and software engineering. Its cardinal mission furnishes an all-encompassing depiction of a system's functionalities and intricate interrelationships.

Nestled within the confines of an FBD as shown in Figure 3, one encounters a constellation of pivotal constituents [49]:

- Function Blocks: manifest as geometric blocks, each epitomizing a distinct function within the system's purview. These blocks function as graphical proxies for tasks or processes that orchestrate the broader system's operation [50].
- Input and Output Elements: The labyrinthine interplay of lines orchestrates the ingress and egress elements tethered to each function block. These conduits illuminate the transmission pathways for data or signals as they flow into and out of each function [51].
- Interconnections: FBDs cast light on the web of interconnections knitting diverse functions within the system, unveiling the tapestry of each function's interactions with its counterparts.
- Functional Sequences and Pathways: FBDs diligently chart the trajectories and sequences via which data or signals navigate the system's labyrinth. This graphical portrayal proffers insights into how the system processes information or materials.

Table 4. Comparison table that highlights the features of STPA about other safety analysis methods

Feature	STPA	FMEA (Failure Modes and Effects Analysis)	HAZOP (Hazard and Operability Study)	Fault Tree Analysis (FTA)
Approach	Systems thinking, control-focused	Bottom-up, failure mode-focused	Top-down, deviation-focused	Top-down, event-focused
System View	Holistic, considers entire system interactions	Component-level examines individual failures	Process-level examines operational deviations	Event-level traces paths to specific undesired events
Human Factors	Integrally considers human actions and decisions	Typically, it does not focus on human factors	Can include human factors as potential causes	Rarely includes human factors unless specifically added
Complexity Handling	Handles complex, dynamic systems with emergent behaviours	Suited for simpler systems or well-understood components	It is good for process industries, less for complex interactions	Effective for static systems with known failure logic
Prospective Analysis	Proactively identifies unsafe control actions	Identifies potential component failures	Identifies potential operational issues	Identifies potential paths to failure

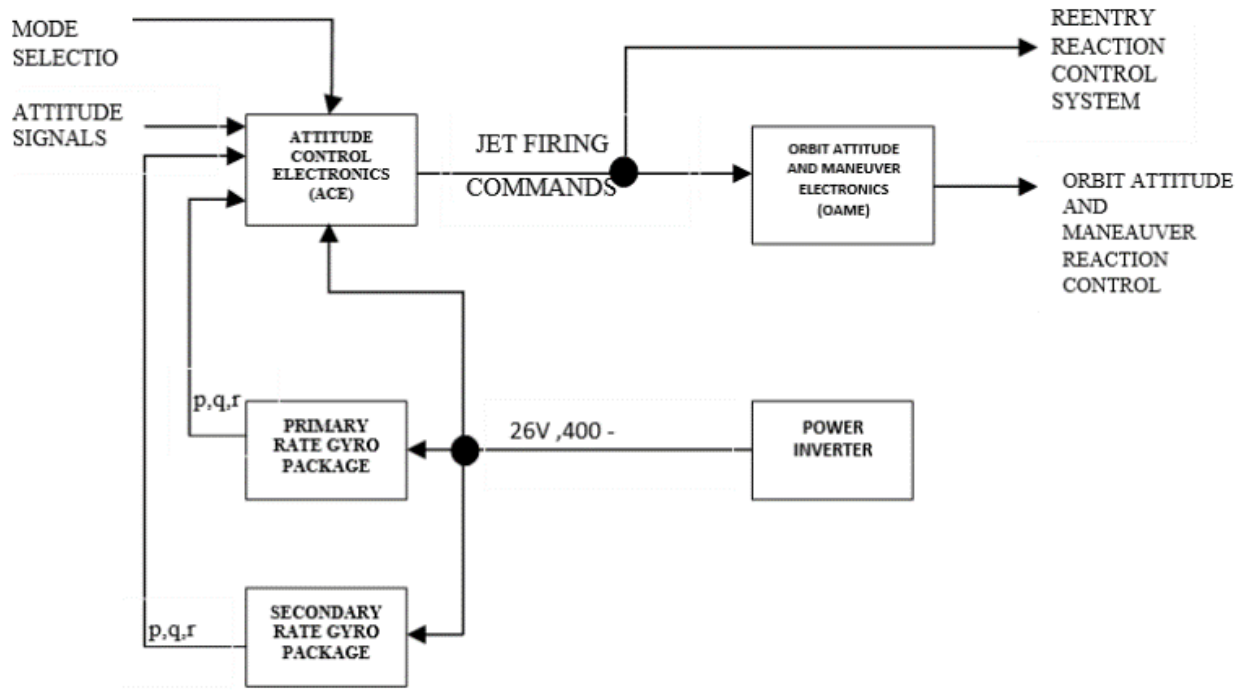

Figure 3. Functional block diagram of the Gemini spacecraft's attitude control and maneuvering electronics system, June 1962 [52]

FBDs can also include specialized schematic symbols that convey specific properties or attributes of the functions. These symbols enhance the expressiveness of the diagram and improve the understanding of the system's operational dynamics [53]. FBDs have a long history from the late 1950s and have been applied to complex system design ever since. They are the essential tools for understanding how a system works, allowing stakeholders to see how the individual components contribute to the system's functionality [54]. A diverse menagerie of specialized FBD variants has surfaced, each meticulously tailored to precise requirements. An exemplary par excellence is the Functional Flow Block Diagram, an amalgamation of elements from functional block diagrams and flowcharts, presenting an all-encompassing visualization instrument. In software development, sundry methodologies exploit bespoke functional block diagram techniques, enriching the design and comprehension of software systems. An illustrious example lies in the FBD, which is ubiquitous in industrial computing. FBDs confer a graphical lexicon for crafting software applications tailored to programmable logic controllers, rendering invaluable assistance in designing and implementing control systems governing industrial processes [55]. FBD ascended to an indispensable pedestal within systems engineering and software development. They function as the vantage point from which stakeholders embark on a profound exploration of system functions, their symbiotic entwinements, and the informational or signal flow, rendering them indispensable in unravelling the intricacies of complex systems.

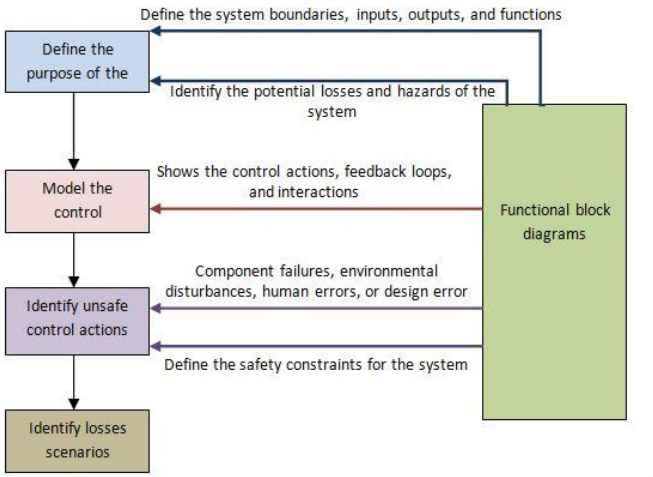

Figure 4. Our diagram shows how FBD helps and assists in STPA analysis

The Figure 4 shows how FBD helps and assists in STPA analysis, in the context of STPA, FBDs serve several purposes.

Define System Boundaries, Inputs, Outputs, and Functions: FBDs help to establish the scope of the system under analysis by defining its boundaries. This includes identifying the inputs to the system (what data or signals it receives), the outputs from the system (what data or signals it produces), and the functions that the system performs (what the system does with the inputs to produce the outputs).

Identify Potential Losses and Hazards of the System: FBDs can be used to identify potential losses (undesirable outcomes) and hazards (conditions that could lead to a loss). This is done by examining the functions and interfaces in the FBD and considering what could go wrong.

Show Control Actions, Feedback Loops, and Interactions: FBDs can illustrate how different parts of the system interact and influence each other. This includes showing control actions (actions taken to influence the behavior of the system), feedback loops (where the output of a function is used as an input to the same or another function), and interactions (where the output of one function affects the input of another).

Component Failures, Environmental Disturbances, Human Errors or Design Error: FBDs can help identify how these factors could lead to unsafe control actions or loss scenarios. For example, a component failure could prevent a necessary control action from being performed, or a design error could result in a control action being performed incorrectly.

4.1 The nuclear power station: A crucible of energy generation through nuclear alchemy

A nuclear power station, known by various nomenclatures, including nuclear power plant or nuclear reactor [56], emerges as a multifaceted edifice architected with the express intent of birthing electricity via the alchemical magic of nuclear reactions [57]. It draws sustenance from the judicious unleashing of energy incarcerated within atomic nuclei. This formidable font metamorphoses into the ethereal essence of heat, subsequently transmuted into the tangible currency of electricity [58]. Here, we embark on a detailed explanation of the orchestration inherent to the nuclear power station's modus operandi presented in Figure 5.

Nuclear Fuel: At the epicentre of a nuclear power station, it pulsates its reactor core, enshrining the sacrosanct nuclear fuel [59]. In commercial nuclear reactors, enriched uranium, notably uranium-235 (U-235), reigns supreme as the predominant fuel. Certain advanced reactors may apply a blend of uranium and plutonium fuels [60]. Fission Reaction: Within the sanctum of the reactor core, the theatre of nuclear fission unfurls. In this dramatic tableau, the nucleus of a weighty atom, such as uranium-235, undergoes cleavage, metamorphosing into two smaller nuclei. This cataclysmic schism bequeaths an abundance of energy, manifesting in the kinetic vigour of the ensuing diminutive nuclei and high-energy neutrons.

Control Rods: Prudent governance of the fission reactions and the aversion of cataclysmic overheating pivot on the utilization of control rods. Composed of materials adept at absorbing neutrons, these control rods ingress into the reactor core. By manipulating the elevation or descent of these rods, operators execute precise choreography to modulate the pace of reactions. This judicious manipulation transmutes the control rods into the veritable conductors of a symphony of control.

Coolant: The copious thermal output forged through nuclear reactions necessitates a medium for its disbursement. Typically, water, akin to an obedient squire, undertakes this role. It circulates through conduits, harmoniously absorbing the heat from the reactor core. In due course, the heating transforms the coolant into steam. Steam Generation: The superheated steam thus generated becomes the impetus propelling a turbine. As it courses over the turbine's blade-laden domain, the steam bestows upon them a mesmerizing gyration. This entrancing pirouette orchestrates the transmutation of thermal energy into mechanical energy.

Electricity Generation: The whirling turbine stands connected to a generator, a device embarking on a subtle dance of electromagnetic induction. As the turbine pirouettes, it

coerces a coil of wire to the pirouette within the magnetic dominion, an act akin to a ballet of electrons. This ballet culminates in the gestation of electricity. Condensation: After passing through the turbine, the erstwhile steam assumes a liquid visage orchestrated by a distinct cooling apparatus such as a cooling tower. This recondensed water embarks on a cyclical odyssey destined to be reheated in the reactor core, embarking on an eternal loop. Safety Measures: Nuclear power stations, cognizant of the potential perils intrinsic to their essence, instate a panoply of safety apparatuses and redundant systems. These encompass emergency shutdown protocols, contingency cooling systems, containment structures fashioned to incarcerate the evil spectre of radioactive effluents, and ardent training regimes for plant personnel. Waste Management: A conundrum dogging nuclear power is the stewardship of radioactive refuse. These establishments yield spent nuclear fuel, which is saturated with radioactivity and necessitates sagacious management. Disposition mandates safeguarding against harm to humans and the environment, a vexing challenge that lingers perpetually.

Regulations: Vigilant scrutiny and governance constitute the bedrock of nuclear power station operations. Rigorous regulations and oversight wielded by governmental entities stand sentinel, ensuring safety and adherence to environmental and operational standards [61]. Nuclear power stations ascend to notoriety for their capacity to generate prodigious electric power with a pall of minimal greenhouse gas emissions [62]. However, these benevolent virtues share the stage with pernicious undercurrents, including concerns about nuclear accidents, the labyrinthine puzzle of radioactive waste disposal, and the arduous capital investment essential for their inception and maintenance [63]. Despite the maelstrom of complexities, nuclear power stations remain ensconced in the tapestry of energy generation, weaving a unique narrative within diverse national energy portfolios [64].

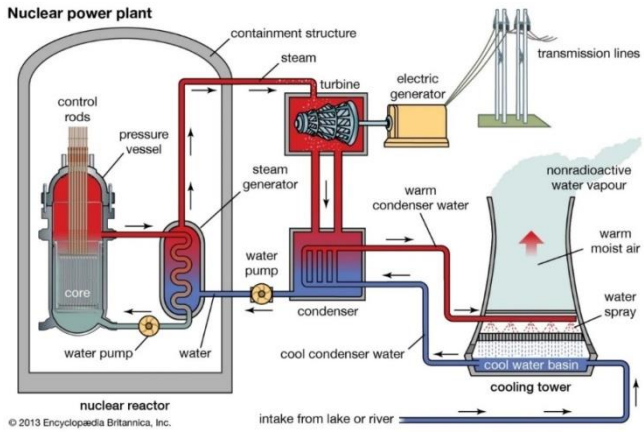

Figure 5. Nuclear power plant diagram [64]

4.2 Application of STPA and FBD in nuclear power plants

In the crucible of analysis, the illumination that unfurls can be the harbinger of transformation. Take, for instance, the potent insights yielded by such an examination. The cooling system may occupy the vanguard of criticality within the power station's operational tapestry. The risk of overheating, a spectral menace, may be mitigated through the infusion of redundancy in cooling mechanisms or the implantation of safety protocols primed for immediate system shutdown in dire straits. Moreover, a tabulation of control actions and their unholy brethren, unsafe control actions, may take form, ensnaring the hazards and perils unveiled through the concerted dance of the FBD and STPA. The nuclear power station case study exemplifies par excellence, illustrating the bounties reaped through the union of FBD and STPA. The confluence of these two methodologies engenders a comprehensive and potent arsenal tailor-made for the dissection of hazards and the assessment of risks amidst the complex systems milieu. The paradigm stands as an ode to how FBD aids in identifying the pivotal functions and constituents and how STPA weaves. The tapestry of hazards and risks enfolding these critical facets. It further serves as a testament to how control measures, akin to guardians at the gates, may be conceived to fend off calamity and smother it in its embryonic stages.

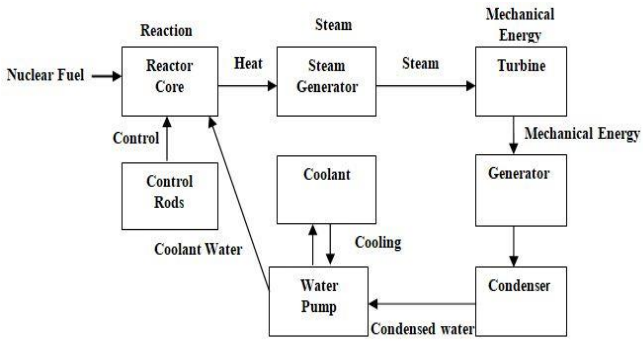

Figure 6. Our functional block diagram of nuclear power station

The Table 5 of UCA using nuclear power plant, meticulously orchestrated, unveils how hazards and risks, akin to errant spirits, may be corralled and kept at bay. To erect this tableau, we embarked on a journey that commenced with the FBD's comprehensive vista of the nuclear power station in Figure 6 and its various constituents. This vista acted as the clarion call, summoning the critical control actions indispensable for the system's safe navigation. These control actions encompassed the act of supplying coolant to the reactor, the vigilant monitoring of reactor temperature and pressure, and the reasonable control of fuel flow into the reactor's maw. In the next phase, STPA stepped onto the stage, wielding its analytical acumen to dissect each control action in exquisite detail. It uncovered the potential hazards lurking beneath the surface, the minefield of unsafe control actions that might trigger the cataclysmic explosion of peril. For instance, the spectre of a coolant loss accident, the harbinger of reactor overheating, and the apocalyptic meltdown emerged from the shadows. STPA further identified the unsavoury control actions that could nourish this growing tempest, such as the failure to detect coolant loss, the neglect to initiate the emergency infusion of coolant or the reckless adjustment of fuel flow. However, it also bestowed the gift of enlightenment, illuminating control actions that could act as bulwarks against the advancing tide of peril. These included redundant coolant flow systems, automated emergency coolant deployment, and a regimen of operator training, honing their fuel flow rate calibration expertise. The control actions were methodically marshalled into a tableau in the final act. This grand mosaic encapsulated the essence of each critical control action, its associated hazards, the malevolent spectre of unsafe control actions in the Table 6, and the safeguards poised to repel the

onslaught of disaster. In sum, the fusion of the FBD and STPA methodologies unveiled the myriad perils lurking in the shadows and provided the blueprint for their containment. It served as a testament to the power of a multi-disciplinary approach, a symphony of analysis woven from disparate threads, to unravel the enigma of complex systems such as the nuclear power station. The loss scenarios its illustrated in the Table 7.

Table 5. Table of UCA using nuclear power plant

Control Actions	Provide	Not Provide	Late	Early	Out of Order	Hazard
Reactor coolant system pumps	X					Loss of coolant flow
Control rods	X			X		Inadequate control of nuclear reaction
Emergency feed water system	X		X			Inadequate cooling of the reactor
Main steam isolation valves	X	X			X	Release of radioactive steam
Pressurized coolant injection system	X		X			Inadequate cooling of the reactor
Primary containment system	X				X	Containment breach
Secondary containment system	X				X	Containment breach
Emergency cooling system	X		X			Inadequate cooling of the reactor
Reactor coolant pressure control	X		X	X		Over-pressurization of reactor
Reactor coolant temperature control	X				X	Overheating of reactor
Reactor coolant flow control	X					Inadequate coolant flow
Reactor trip system	X			X		Failure to initiate a safe shutdown
Emergency shut-down system	X			X		Failure to initiate a safe shutdown
Auxiliary feed water system	X		X			Inadequate cooling of the reactor
Electrical power supply	X	X	X			Loss of power
Instrumentation and control system	X	X	X			Inadequate monitoring and control
Emergency diesel generators	X		X			Inadequate backup power
Containment spray system	X		X			Inadequate cooling of containment
Control room habitability system	X	X			X	Loss of operator support due to radiation exposure
Safety relief valves	X			X		Release of radioactive material

Table 6. Table unsafe control actions

Unsafe Control Actions
Failure to activate the emergency coolant system during a reactor shutdown leads to overheating and a potential meltdown hazard.
Inadequate monitoring of radiation levels in and around the plant, leading to potential health hazards for workers and nearby residents.
Failure to properly maintain backup power systems can lead to potential power loss during a blackout and loss of control over critical safety systems.
Lack of proper training and procedures for responding to emergencies leads to potential response delays and increased risk to personnel and the public.
Failure to properly inspect and maintain critical components such as valves and pumps leads to potential equipment failures and safety hazards.
Failure to properly manage and dispose of radioactive waste leads to potential environmental contamination and health hazards.
Inadequate protection against natural disasters such as earthquakes and floods lead to potential plant damage and safety hazards.
Inadequate security measures to protect against unauthorized access and sabotage, leading to potential risks of theft, vandalism, or terrorist attacks.

Table 7. Table of loss scenarios

Loss Scenario	Hazard
Loss of cooling system	Potential nuclear meltdown hazard
Radiation release	Potential health hazards for workers and nearby residents
Unauthorizedaccess or sabotage	Potential loss of control over safety systems, leading to a nuclear meltdown or other disaster
Failure to respond to emergencies	Potential delay in response, leading to increased loss of life or environmental damage
Environmental contamination	Potential health hazards for nearby residents and wildlife
Loss of backup power	Potential loss of control over critical safety systems, leading to a nuclear meltdown or other disaster

Loss scenarios that could result in the operation of a nuclear power station.

4.3 The limitations of STPA in nuclear power station safety analysis

Complexity: STPA's intricate nature can be challenging to implement, requiring a deep understanding of system behaviour and safety principles. This complexity may limit its accessibility to those without specialized expertise.

Resource Intensity: Conducting STPA analyses can be resource-intensive, demanding significant time and personnel with the necessary knowledge, which may not be feasible for organizations with limited resources.

Subjectivity: The process of identifying hazards and control structures in STPA involves a degree of subjectivity, which can introduce variability into the analysis. Ensuring consistent outcomes requires diligent oversight.

To address these limitations, the document suggests integrating STPA with other methods:

FBD: Combining STPA with FBD can provide a more comprehensive understanding by leveraging the strengths of both methods. FBD offers a visual representation of system functions and dependencies, enriching the hazard analysis provided by STPA.

Training and Expertise: Enhancing training programs to develop proficiency in STPA and FBD can help overcome the complexity and resource challenges. Organizations should ensure the presence of personnel skilled in both methodologies.

Complementary Methods: Using STPA in conjunction with other safety analysis methods like Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) can provide a more detailed component-level assessment, complementing the systemic insights of STPA

a) Recommendations:

The amalgamation of Functional Block Diagrams (FBD) and System-Theoretic Process Analysis (STPA) methodologies presents remarkable advantages in examining perils and evaluating hazards within intricate systems. Nevertheless, it is imperative to acknowledge potential complications and delineate strategies to overcome them. Presented below are comprehensive recommendations, elucidated in a paragraph format, that address these facets:

1. Holistic empowerment through comprehensive training and expertise advancement

To fully harness the advantages accrued from the synergy of FBD and STPA, comprehensive training becomes imperative, thus equipping professionals with adeptness in both methodologies. The challenge pertains to the potential need for such all-encompassing training avenues. To surmount this impediment, organizations should institute educational programs incorporating both methodologies, assuring that professionals are adequately prepared to employ them adeptly. Furthermore, the advocacy of certifications and immersive workshops shall be instrumental in nurturing competency within these methodologies.

2. Methodical imposition

Ensuring seamless integration of FBD and STPA necessitates embracing a systematic and sequential approach. This entails commencing with FBD and progressing methodically to STPA, facilitating a more profound comprehension of system-related perils. Challenges may emerge in instances of disparities or gaps in this systematic implementation. The formulation of lucid guidelines and comprehensive checklists outlining the sequential application of FBD and STPA is requisite to alleviate these difficulties. Continuous assessment and refinement of the implementation process, driven by the insights gleaned from experiences, become paramount.

3. Synergistic cross-disciplinary collaboration

Collaboration among luminaries from many domains augments the depth and breadth of hazard analysis, encompassing an extensive spectrum of potential risks. Nonetheless, hurdles such as communication impediments and divergent perspectives may ensue. To assuage these obstacles, organizations should establish perspicuous communication protocols and interdisciplinary teams. Encouraging regular congregations shall foster collaboration and serve as a forum to address potential conflicts, ensuring a shared comprehension of overarching objectives.

4. Dynamic surveillance and real-time adaptation

The importance of real-time monitoring must be balanced to uphold the relevance of risk assessment within the milieu of evolving systems. Refrain from accommodating updates might result in the obsolescence of risk mitigation strategies. In this regard, organizations should implement mechanisms that facilitate continual monitoring and the instantaneous reporting of system alterations. These mechanisms must be primed to trigger an immediate reassessment of risks in the wake of significant transformations.

5. Sustained enhancement endeavors

Regular audits and evaluations are catalysts for perpetuated amelioration within the risk assessment domain. The problem here lies in the potential need for adequate feedback mechanisms pinpointing areas requiring enhancement. To surmount this challenge, organizations should instate a feedback loop that entails engagement with experts and stakeholders, a conduit through which weaknesses within the approach can be accurately discerned. Periodic external audits should be convened to solicit fresh perspectives and novel insights.

6. The dissemination of knowledge

Sharing findings and experiences begets collective learning and augments our understanding of intricate system-associated risks. The crux lies in inadequate record-keeping and platforms for disseminating knowledge. To rectify this deficiency, organizations should inaugurate a centralized knowledge-sharing platform. Encouragement for the meticulous documentation of pivotal discoveries and case studies is imperative, fostering a culture wherein sharing best practices becomes second nature.

7. Alignment with regulatory conformity

Adherence to regulatory prerequisites ensures concurrent compliance with legal and operational imperatives. However, the dynamic panorama of regulatory mandates presents challenges in perpetuating alignment. Organizations should institute a dedicated team entrusted with the vigilant monitoring of regulatory alterations to address this predicament. Regular assessments should be conducted to ensure continual alignment and proactively address any compliance fissures. Through diligently implementing these recommendations and proactively mitigating associated challenges, organizations can optimize the benefits stemming from the fusion of FBD and STPA methodologies while prudently counteracting potential detriments. This comprehensive approach shall indubitably enhance safety, reliability, and the art of risk management within complex systems.

5. CONCLUSIONS

The research presented herein highlights the transformative potential of integrating FBD and STPA in hazard analysis and risk assessment, particularly within the context of nuclear power stations. This systematic and multifaceted strategy is essential for achieving the highest safety and reliability standards in complex energy systems.

To actualize the benefits of this integrated approach, several actionable recommendations are proposed:

Specialized training programs must be developed to enhance professional expertise in both FBD and STPA methodologies. Such initiatives will equip individuals with the necessary skills to navigate the complexities of safety analysis effectively. A methodological synergy should be fostered, encouraging adopting a combined approach that utilizes the

visual strengths of FBD and the systemic depth of STPA. This will enable analysts to gain a more nuanced understanding of system behaviours and potential failure modes. It is imperative to allocate adequate resources, including time, personnel, and financial investment, to manage the detailed application of these methodologies. This will address the challenges associated with the resource-intensive nature of comprehensive safety analyses. Cross-disciplinary collaboration should be promoted to enrich the hazard analysis process. The analysis will benefit from diverse perspectives by bringing together experts from various fields, leading to more robust safety solutions and innovative risk mitigation strategies. The adoption of continuous improvement practices is recommended. Feedback from safety analyses should inform the ongoing development and refinement of safety practices within nuclear power stations.

Advanced analytical tools should also be utilized to augment the FBD-STPA methodology. These tools can enhance accuracy, reduce subjectivity, and streamline analysis. Standardized procedures for conducting FBD-STPA analyses should be developed and disseminated. This will ensure consistency across different teams and projects, minimizing outcome variability.

The potential impact of this research is significant. By improving the framework for safety analysis, the likelihood of accidents and incidents within nuclear power stations can be substantially reduced. This protects human lives and the environment and contributes to the stability and reliability of global energy supplies. Moreover, the insights gained from this research can be applied to other industries, fostering a culture of safety and excellence.

Safety and reliability terms related to nuclear power station safety analysis:

Deterministic Safety Analysis: A method to ensure that safety functions are fulfilled and that releases of radioactive material are kept below acceptable limits.

Probabilistic Safety Analysis: An analysis that complements deterministic safety analysis by evaluating the likelihood and consequences of potential accidents.

Safety Functions: Actions required to maintain a safe state or to prevent, control, or mitigate the consequences of accidents.

Safety Margins: The extent to which a system can tolerate a deviation from normal operation before reaching a hazardous state.

Safety Assessment: The process of determining the safety of a system throughout its lifecycle.

Safety Verification: The confirmation that the design and operation of a system meet all the required safety standards.

Fault Monitoring: The process of detecting faults in a system to prevent accidents and ensure operational safety.

Reliability Analysis: The study of the dependability of system components, considering the likelihood of failures and their impacts.

Human Reliability Analysis: The assessment of the likelihood of human error and its impact on the safety and operation of nuclear power plants.

Risk Assessment: The systematic approach to understanding the risks associated with a system, including the identification of hazards and the analysis of their potential impacts.

Industrial Safety: The management of all operations and events within an industry to protect its employees and assets by minimizing hazards, risks, accidents, and near misses.

Radiological Consequences: The potential impact of radioactive releases on the environment and human health.

Source Term: The amount and type of radioactive material released from a nuclear power plant during normal operation or accidents.

Accidents: Unintended events that can cause significant harm to people, the environment, or the facility itself.

Operational Occurrences: Events that deviate from normal operation but do not necessarily lead to an accident.

Performance: The ability of a system or component to function under stated conditions for a specified period.

Hazards: Potential sources of harm or adverse health effects on a person or persons.

Safety Culture: The attitude, beliefs, perceptions, and values that employees share about safety within an organization.

Safety Case: A structured argument, supported by evidence, that provides a compelling, understandable, and valid case that a system is safe for a given application in a given environment.

Compliance Assessment: The evaluation of whether a system or component meets the relevant legal safety requirements.

Defence in Depth: A safety philosophy that employs multiple layers of protection to prevent accidents or to mitigate their consequences.

Emergency Preparedness: The capability to respond effectively to emergencies, including the existence of plans, procedures, equipment, and training.

Safety Instrumented Systems: Engineered systems designed to prevent or mitigate hazardous events.

Risk Monitors: Tools used to assess and monitor the risk level of a nuclear power plant in real time.

REFERENCES

[1] Alanne, K., Saari, A. (2006). Distributed energy generation and sustainable development. Renewable and Sustainable Energy Reviews, 10(6): 539-558. https://doi.org/10.1016/j.rser.2004.11.004

[2] An, F., An, G., An, Q., et al. (2016). Neutrino physics with JUNO. Journal of Physics G: Nuclear and Particle Physics, 43: 030401. https://doi.org/10.1088/0954-3899/43/3/030401

[3] Andrade, R.O., Yoo, S.G., Ortiz-Garces, I., Barriga, J. (2022). Security risk analysis in IoT systems through factor identification over IoT devices. Applied Sciences, 12(6): 2976. https://doi.org/10.3390/app12062976

[4] Aven, T. (2022). A risk science perspective on the discussion concerning Safety I, Safety II and Safety III. Reliability Engineering and System Safety, 217: 108077. https://doi.org/10.1016/j.ress.2021.108077

[5] Bjerga, T., Aven, T., Zio, E. (2016). Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. Reliability Engineering and System Safety, 156: 203-209. https://doi.org/10.1016/j.ress.2016.08.004

[6] Eddine, B.H., Riad, B., Youcef, Z., El-Arkam, M. (2023). Multiobjective Optimization of the Performance of Safety Systems. Engineering Proceedings, 29(1): 10. https://doi.org/10.3390/engproc2023029010

[7] Brown, J.H., Burger, J.R., Hou, C., Hall, C.A.S. (2022). The pace of life: Metabolic energy, biological time, and life history. Integrative and Comparative Biology, 62(5): 1479-1491. https://doi.org/10.1093/icb/icac058

[8] Čepin, M. (2019). Evaluation of the power system reliability if a nuclear power plant is replaced with wind power plants. Reliability Engineering and System Safety, 185: 455-464. https://doi.org/10.1016/j.ress.2019.01.010

[9] Chaal, M., Banda, O.A.V., Glomsrud, J.A., Basnet, S., Hirdaris, S., Kujala, P. (2020). A framework to model the STPA hierarchical control structure of an autonomous ship. Safety Science, 132: 104939. https://doi.org/10.1016/j.ssci.2020.104939

[10] Chino, M., Nakayama, H., Nagai, H., Terada, H., Katata, G., Yamazawa, H. (2011). Preliminary estimation of release amounts of 131i and 137cs accidentally discharged from the Fukushima Daiichi nuclear power plant into the atmosphere. Journal of Nuclear Science and Technology, 48(7). 1129-1134. https://doi.org/10.1080/18811248.2011.9711799

[11] Bouasla, S.E.I., Zennir, Y., Mechhoud, E.A. (2020). Risk analysis using HAZOP - fault tree - event tree methodology case study: Naphta stabilizer-a reflux drum (LPG separation) in RA1K. Algerian Journal of Signals and Systems, 5(2): 98-105.

[12] Hernández-Ceballos, M.A, Cinelli, G, Tollefsen, T, Marín-Ferrer, M. (2016). Identification of airborne radioactive spatial patterns in Europe - Feasibility study using Beryllium-7. Journal of Environmental Radioactivity, 155-156: 55-62. https://doi.org/10.1016/j.jenvrad.2016.02.006

[13] Cardis, E., Hatch, M. (2011). The Chernobyl accident--an epidemiological perspective. Clinical Oncology, 23(4): 251-260. https://doi.org/10.1016/j.clon.2011.01.510

[14] Hirose K. (2020). Atmospheric effects of Fukushima nuclear accident: A review from a sight of atmospheric monitoring. Journal of Environmental Radioactivity, 218: 106240. https://doi.org/10.1016/j.jenvrad.2020.106240

[15] Michaël, M., Dechy, N., Rousseau, J.M. (2020). Les accidents nucléaires de 1969 et 1980 à Saint-Laurent-des-Eaux: Quand la transition engendre l'oubli. Congrès Lambda Mu 22 « Les risques au cœur des transitions » (e-congrès) - 22e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Institut pour la Maîtrise des Risques, Oct, Le Havre (e-congrès), France. https://hal.science/hal-03477810/.

[16] Produção, G., Borges, S.F.D.S., Albuquerque, M.A.F., Cardoso-Junior, M.M., Belderrain, M.C.N., Loures, L. (2021). Systems theoretic process analysis (STPA): A bibliometric and patents analysis. Gestao e Producao, 28(2): e5073. https://doi.org/10.1590/1806-9649-2020V28E5073

[17] Dghaym, D., Hoang, T.S., Turnock, S.R., Butler, M., Downes, J., Pritchard, B. (2021). An STPA-based formal composition framework for trustworthy autonomous maritime systems. Safety Science, 136: 105139. https://doi.org/10.1016/j.ssci.2020.105139

[18] Greeff, G., Ghoshal, R., anjan. (2004). Practical E-Manufacturing and Supply Chain Management. Book, ScienceDirect, 462. https://doi.org/10.1016/B978-0-7506-6272-7.X5000-3

[19] Drozyner, P. (2020). Risk analysis in maintenance processes. Engineering Management in Production and Services, 12(4): 64-76. https://doi.org/10.2478/emj-2020-0028

[20] Podbregar, I., Šimić, G., Radovanović, M., Filipović, S., Maletič, D., Šprajc, P. (2020). The international energy security risk index in sustainable energy and economy transition decision making—a reliability analysis. Energies, 13(14): 3691. https://doi.org/10.3390/en13143691

[21] Global Energy Institute. (2020). International index of energy security risk: 2020 edition. This Report Provides an Updated Look at Energy Security Risks across Different Countries from 1980 Through 2018 and Calculates Risk Index Scores for a Large Energy User Group2.

[22] Mazidi, P., Sanz-Bobi, M.A., Shayesteh, E., Hilber, P. (2018). Risk index in economic generation operation in power systems with renewable sources. In 5th International Conference on Energy, Sustainability and Climate Change (ESCC), Mykonos, Greece.

[23] El-Sefy, M., Yosri, A., El-Dakhakhni, W., Nagasaki, S., Wiebe, L. (2021). Artificial neural network for predicting nuclear power plant dynamic behaviours. Nuclear Engineering and Technology, 53(10): 3275-3285. https://doi.org/10.1016/j.net.2021.05.003

[24] Leveson, N.G. (2012). Engineering a safer world: systems thinking applied to safety. Choice Reviews Online, 49(11). https://doi.org/10.5860/choice.49-6305

[25] Erixno, O., Rahim, N.A., Ramadhani, F., Adzman, N.N. (2022). Energy management of renewable energy-based combined heat and power systems: A review. Sustainable Energy Technologies and Assessments, 51: 101944. https://doi.org/10.1016/j.seta.2021.101944

[26] Faiella, G., Parand, A., Franklin, B.D., Chana, P., Cesarelli, M., Stanton, N.A., Sevdalis, N. (2018). Expanding healthcare failure mode and effect analysis: A composite proactive risk analysis approach. Reliability Engineering and System Safety, 169: 117-126. https://doi.org/10.1016/j.ress.2017.08.003

[27] Fedorets, A. (2022). A new method of occupational risk assessment, based on uncertainty. Reliability: Theory and Applications, 17. https://doi.org/10.24412/1932-2321-2022-366-59-64

[28] Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., Sezer, S. (2017). STPA-SafeSec: Safety and security analysis for cyber-physical systems. Journal of Information Security and Applications, 34(Part 2): 183-196. https://doi.org/10.1016/j.jisa.2016.05.008

[29] Fuentes-Bargues, J.L., González-Cruz, M.C., González-Gaya, C., Baixauli-Pérez, M.P. (2017). Risk analysis of a fuel storage terminal using HAZOP and FTA. International Journal of Environmental Research and Public Health, 14(7): 705. https://doi.org/10.3390/ijerph14070705

[30] Gil, M., Wróbel, K., Montewka, J. (2019). Toward a method evaluating control actions in STPA-based model of ship-ship collision avoidance process. Journal of Offshore Mechanics and Arctic Engineering, 141(5): 051105. https://doi.org/10.1115/1.4042387

[31] Goerlandt, F., Montewka, J. (2015). Maritime transportation risk analysis: Review and analysis in light of some foundational issues. Reliability Engineering and System Safety, 138: 115-134. https://doi.org/10.1016/j.ress.2015.01.025

[32] Liserre, M., Sauter, T., Hung, J.Y. (2010). Future energy systems: Integrating renewable energy sources into the smart power grid through industrial electronics. In.IEEE Industrial Electronics Magazine, 4(1): 18-37. https://doi.org/10.1109/MIE.2010.935861

[33] Hegde, J., Rokseth, B. (2020). Applications of machine learning methods for engineering risk assessment – A review. Safety Science, 122: 104492. https://doi.org/10.1016/j.ssci.2019.09.015
[34] Kazaras, K., Kirytopoulos, K., Rentizelas, A. (2012). Introducing the STAMP method in road tunnel safety assessment. Safety Science, 50(9): 1806-1817. https://doi.org/10.1016/j.ssci.2012.04.013
[35] Kim, S.C. (2019). Safety assessment of oil immersed transformer applying fault tree analysis and functional block diagram. Crisis and Emergency Management: Theory and Praxis, 15(8): 107-116. https://doi.org/10.14251/crisisonomy.2019.15.8.107
[36] Kim, S., Heo, G., Zio, E., Shin, J., Song, J.G. (2020). Cyber attack taxonomy for digital environment in nuclear power plants. Nuclear Engineering and Technology, 52(5): 995-1001. https://doi.org/10.1016/j.net.2019.11.001
[37] Kolb, V.M., Clark, B.C. (2023). Retrospective on the general applicability of our system functional block diagram. Systems Approach to Astrobiology, CRC Press. https://doi.org/10.1201/9781003225874-12
[38] Li, J.K., Lin, M., Li, Y.K., Wang, X. (2022). Transfer learning with limited labelled data for fault diagnosis in nuclear power plants. Nuclear Engineering and Design, 390: 111690. https://doi.org/10.1016/j.nucengdes.2022.111690
[39] Li, L., Dong, Y.Y., Chen, Y.T., Jiao, J., Zou, X.J. (2022). A new method for environmental risk assessment of pollutants based on multi-dimensional risk factors. Toxics, 10(11): 659. https://doi.org/10.3390/toxics10110659
[40] Liubarets, T.F., Shibata, Y., Saenko, V.A., Bebeshko, V.G., Prysyazhnyuk, A.E., Bruslova, K.M., Fuzik, M.M., Yamashita, S., Bazyka, D.A. (2019). Childhood leukaemia in Ukraine after the Chornobyl accident. Radiation and Environmental Biophysics, 58: 553-562. https://doi.org/10.1007/s00411-019-00810-4
[41] Oginni, D., Camelia, F., Chatzimichailidou, M., Ferris, T. L. (2023). Applying system-theoretic process analysis (STPA)-based methodology supported by systems engineering models to a UK rail project. Safety Science, 167: 106275. https://doi.org/10.1016/j.ssci.2023.106275
[42] Malça, J., Freire, F. (2004). Life cycle energy analysis for bioethanol: Allocation methods and implications for energy efficiency and renewability. In 17th International Conference on Efficiency, Costs, Optimization, Simulation and Environmental Impact of Energy and Process Systems, Mexico, pp. 1-13.
[43] Mayer, F.D., Brondani, M., Carrillo, M.C.V., Hoffmann, R., Lora, E.E.S. (2020). Revisiting energy efficiency, renewability, and sustainability indicators in biofuels life cycle: Analysis and standardization proposal. Journal of Cleaner Production, 252: 119850. https://doi.org/10.1016/j.jclepro.2019.119850
[44] Bensaci, C., Zennir, Y., Pomorski, D. (2018). A Comparative study of STPA hierarchical structures in risk analysis: The case of a complex multi-robot mobile system. In 2018 2nd European Conference on Electrical Engineering and Computer Science (EECS), Bern, Switzerland, pp. 400-405. https://doi.org/10.1109/EECS.2018.00080
[45] McInnes, A.I., Eames, B.K., Grover, R. (2011). Formalizing functional flow block diagrams using process algebra and metamodels. IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, 41(1): 34-49. https://doi.org/10.1109/TSMCA.2010.2048749
[46] Meng, X.K., Chen, G.M., Shi, J.H., Zhu, G.G., Zhu, Y. (2018). STAMP-based analysis of deepwater well control safety. Journal of Loss Prevention in the Process Industries, 55: 41-52. https://doi.org/10.1016/j.jlp.2018.05.019
[47] Mallya, A., Pantelic, V., Adedjouma, M., Lawford, M., Wassyng, A. (2016). Using STPA in an ISO 26262 compliant process. In: Skavhaug, A., Guiochet, J., Bitsch, F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science(), vol 9922. Springer, Cham, 117-129. https://doi.org/10.1007/978-3-319-45477-1_10
[48] La-Ngoc, T., Kwon, G. (2017). Comparing the effectiveness of SFMEA and STPA in software-intensive railway level crossing system. In: Park, J., Loia, V., Yi, G., Sung, Y. (eds) Advances in Computer Science and Ubiquitous Computing. CUTE CSA 2017 2017. Lecture Notes in Electrical Engineering, vol 474. Springer, Singapore, 1281-1288. https://doi.org/10.1007/978-981-10-7605-3_204
[49] Mueller, T.A., Lhuillier, D., Fallot, M., Letourneau, A., Cormon, S., Fechner, M., Giot, L., Lasserre, T., Martino, J., Mention, G., Porta, A., Yermia, F. (2011). Improved predictions of reactor antineutrino spectra. Physical Review C - Nuclear Physics, 83: 054615. https://doi.org/10.1103/PhysRevC.83.054615
[50] Mutlu, N.G., Altuntas, S. (2019). Risk analysis for occupational safety and health in the textile industry: Integration of FMEA, FTA, and BIFPET methods. International Journal of Industrial Ergonomics, 72: 222-240. https://doi.org/10.1016/j.ergon.2019.05.013
[51] Nabawy, M., Khodeir, L.M. (2020). A systematic review of quantitative risk analysis in construction of mega projects. Ain Shams Engineering Journal, 11(4): 1403-1410. https://doi.org/10.1016/j.asej.2020.02.006
[52] Papazoglou, I.A. (1998). Functional block diagrams and automated construction of event trees. Reliability Engineering and System Safety, 61(3): 185-214. https://doi.org/10.1016/S0951-8320(98)00011-8
[53] Niculescu, E., Iancu, E.P. (1999). Functional block diagram of the fourth-order PWM converters with DCM. Computers and Computational Engineering in Control. https://www.semanticscholar.org/paper/Functional-Block-Diagram-of-the-Fourth-Order-PWM-Niculescu-Iancu/380629d91e7c8c496504c861fa1cc5358f982c2d.
[54] Nosach, O.V., Sarkissova, E.O., Alyokhina, S.M., Pleskach, O.Y., Litvinets, O.M., Ovsyannikova, L.M., Chumak, A.A. (2021). Subclinical inflammation in non/alcoholic fatty liver disease at the remote period after the chornobyl accident. Problemy Radiatsiinoi Medytsyny Ta Radiobiolohii, 26(1): 437-448. https://doi.org/10.33145/2304-8336-2021-26-437-448
[55] Ong, A.K.S., Prasetyo, Y.T., Salazar, J.M.L.D., Erfe, J.J.C., Abella, A.A., Young, M.N., Chuenyindee, T., Nadlifatin, R., Redi, A.A.N.P. (2022). Investigating the acceptance of the Bataan nuclear power plant reopening: Integrating protection motivation theory and extended theory of planned behavior. Nuclear Engineering and Technology, 54(3): 1115-1125. https://doi.org/10.1016/j.net.2021.08.032

[56] Papazoglou, I.A., Ale, B.J.M. (2007). A logical model for quantification of occupational risk. Reliability Engineering and System Safety, 92(6): 785-803. https://doi.org/10.1016/j.ress.2006.04.017
[57] Peeters, J.F.W., Basten, R.J.I., Tinga, T. (2018). Improving failure analysis efficiency by recursively combining FTA and FMEA in a recursive manner. Reliability Engineering and System Safety, 172: 36-44. https://doi.org/10.1016/j.ress.2017.11.024
[58] Razmi, S.F., Moghadam, M.H., Behname, M. (2021). Time-varying effects of monetary policy on Iranian renewable energy generation. Renewable Energy, 177: 1161-1169. https://doi.org/10.1016/j.renene.2021.06.020
[59] Sulaman, S.M., Beer, A., Felderer, M., Höst, M. (2019). Comparison of the FMEA and STPA safety analysis methods–a case study. Software Quality Journal, 27: 349-387. https://doi.org/10.1007/s11219-017-9396-0
[60] Sultana, S., Okoh, P., Haugen, S., Vinnem, J.E. (2019). Hazard analysis: Application of STPA to ship-to-ship transfer of LNG. Journal of Loss Prevention in the Process Industries, 60: 241-252. https://doi.org/10.1016/j.jlp.2019.04.005
[61] Ye, H.F., Peng, H.W., Li, C.H., Li, Y.L., Li, Z., Yang, Q., Chen, G.Q. (2023). A demonstration concentrating solar power plant in China: Carbon neutrality, energy renewability and policy perspectives. Journal of Environmental Management, 328: 117003. https://doi.org/10.1016/j.jenvman.2022.117003
[62] Zhang, Z.G., Liu, X.R., Zhao, D., Post, S., Chen, J.S. (2023). Overview of the development and application of wind energy in New Zealand. Energy and Built Environment, 4(6): 725-742. https://doi.org/10.1016/j.enbenv.2022.06.009
[63] Zinkle, S.J., Was, G.S. (2013). Materials challenges in nuclear energy. Acta Materialia, 61(3): 735-758. https://doi.org/10.1016/j.actamat.2012.11.004
[64] Martin, W. (2024). Nuclear power. Encyclopedia Britannica. https://www.britannica.com/technology/nuclear-power.