POLITECNICO DI MILANO
DEPARTMENT OF ENERGY
DOCTORAL PROGRAMME IN ENERGY AND NUCLEAR SCIENCE AND TECHNOLOGY



ADVANCED METHODS FOR THE RISK ASSESSMENT AND MANAGEMENT OF DEGRADING ENERGY SYSTEMS

DOCTORAL DISSERTATION OF:
STEFANO MARCHETTI

SUPERVISORS:
PROF. FRANCESCO DI MAIO
PROF. ENRICO ZIO

TUTOR:
PROF. FRANCESCO DI MAIO

CHAIR OF THE DOCTORAL PROGRAMME:
PROF. FRANCESCO DI MAIO

XXXVIII CYCLE

Abstract

Safety critical energy systems (such as Nuclear Power Plants (NPPs), chemical and Oil & Gas facilities…) rely on safety barriers to avoid that accidents occur (preventive barriers) and to mitigate the consequences if they were to occur (mitigative barriers). However, safety barriers degrade in time, eventually leading to a larger risk of severe consequences. The typical approaches proposed in the literature for the assessment of safety barriers performance neglect the influence of such degradation, which, instead, has a great influence on the safety response of the system during an accident.

To address these limitations, this PhD thesis develops methods for the risk assessment and management of degrading energy systems, supporting both operational and design decisions. The main contributions of this work are:

- A Bayesian Network (BN)-based framework for the multi-hazard risk assessment of Oil & Gas (O&G) plants, which originally integrates time dependent Key Performance Indicators (KPIs) to model safety barriers degradation, a Bayesian Regularized Artificial Neural Network (BRANN) for the ignition probability estimation following a Loss Of Primary Containment (LOPC) and a multi-hazard and multi-source risk aggregation procedure to calculate the Location Specific Individual Risk (LSIR) accounting for the uncertainties on the frequency and severity of the accidental scenarios.
- A risk-based maintenance optimization framework, which originally embeds fragility surfaces that characterize the safety barriers time-dependent fragility to hazards within a Dynamic Bayesian Network (DBN) model for the risk assessment. The DBN is used as the environment within a Deep Reinforcement Learning (DRL) algorithm to find the optimal safety barrier maintenance policy.
- A risk-informed design framework for multi-unit systems, which combines global sensitivity indices based on Optimal Transport (OT) with a graphical visualization tool based on CUmulative SUm of NOrmalized Reordered Output (CUSUNORO). The OT-based indices allow the identification of the most important inputs, also in presence of multivariate and time-dependent inputs, whereas the CUSUNORO enables the identification of the safety critical ranges of these inputs, that ultimately enable targeted design improvements to keep the system far from the failure region.

The proposed methods have been successfully applied to realistic energy systems, namely NPPs, O&G plants and chemical storage facilities.

Keywords: Risk assessment; Risk management; Safety barriers degradation; Bayesian Networks (BN); Global Sensitivity Analysis (GSA); Maintenance optimization; Reinforcement Learning (RL); Nuclear Power Plants (NPP); Oil & Gas plants.

Sommario

I sistemi energetici critici (come le Centrali Nucleari (NPPs), gli impianti chimici e Oil & Gas…) sono equipaggiati con barriere di sicurezza per evitare il verificarsi di incidenti (barriere preventive) e per mitigarne le conseguenze qualora essi avvengano (barriere mitigative). Tuttavia, le barriere di sicurezza si degradano nel tempo, portando ad un aumento del rischio di conseguenze gravi. Gli approcci tipicamente proposti in letteratura per la valutazione delle prestazioni delle barriere di sicurezza trascurano l'influenza del degrado, che, invece, ha un impatto significativo sulla risposta di sicurezza del sistema durante un incidente.

Per superare queste limitazioni, questa tesi di dottorato sviluppa metodi per la valutazione e la gestione del rischio di sistemi energetici soggetti a degradazione, a supporto sia delle decisioni operative sia di quelle di progetto. I principali contributi di questo lavoro sono:

- Un framework basato su Reti Bayesiane (Bayesian Networks, BN) per la valutazione del rischio multi-hazard in impianti Oil & Gas (O&G), che integra in modo originale Key Performance Indicators (KPI) dipendenti dal tempo per modellare la degradazione delle barriere di sicurezza, una Bayesian Regularized Artificial Neural Network (BRANN) per la stima della probabilità di innesco a seguito di un Loss Of Primary Containment (LOPC) e una procedura di aggregazione del rischio multi-hazard e multi-sorgente per il calcolo del Location Specific Individual Risk (LSIR), tenendo conto delle incertezze sulla frequenza e sulla severità degli scenari incidentali.
- Un framework di ottimizzazione della manutenzione, che utilizza in modo originale superfici di fragilità per caratterizzare la fragilità tempo-dipendente delle barriere di sicurezza rispetto ai pericoli all'interno di una Dynamic Bayesian Network (DBN) per la valutazione del rischio. La DBN è poi utilizzata come ambiente all'interno di un algoritmo di Deep Reinforcement Learning (DRL) per individuare la politica ottimale di manutenzione delle barriere di sicurezza.
- Un framework di progettazione risk-informed per sistemi multi-unità, che combina indici di sensibilità globale basati sulla teoria dell'Optimal Transport (OT) con uno strumento di visualizzazione grafica basato sul CUmulative SUm of NOrmalized Reordered Output (CUSUNORO). Gli indici basati su OT consentono l'identificazione degli input più importanti anche in presenza di input multivariati e tempo-dipendenti, mentre il CUSUNORO permette di individuare gli intervalli di valori di tali input critici per la sicurezza.

I metodi proposti sono stati applicati con successo a sistemi energetici realistici, quali centrali nucleari (NPPs), impianti Oil & Gas e impianti di stoccaggio di sostanze chimiche.

Parole chiave: Valutazione del rischio; Gestione del rischio; Degradazione delle barriere di sicurezza; Reti Bayesiane; Analisi di Sensibilità Globale; Ottimizzazione della manutenzione; Reinforcement Learning; Energia nucleare.

Acknowledgements

This PhD would not have been possible without the support, guidance, and encouragement of many people.

First of all, I would like to thank my supervisors. Prof. Francesco Di Maio, for his insights, patience, and continuous support and guidance throughout my PhD. Prof. Enrico Zio, for the countless lessons, the occasional but necessary scolding, and for showing me that being a professor does not mean giving up one's fun side. You both ignited my passion for research and are examples to follow.

Thanks to all my friends in the LASAR^3 family. Giovanni, for all the fun and for being the best desk buddy. Dario, for being a mentor at the beginning of my PhD (y and for his wisdom. Pincio, captain of the Pokémon team, for the endless fun and games. Valentina, for all the aperitivi and the "promise". The Chilean mafia, Nicolas, Leonardo, and Juan Pablo, for all the fun and jokes in the office. Gianni, for his kindness. Thomas, for the stimulating discussions. Alice, for all the gossip while opening a "*pacchettino*" and drinking a "*lunghetto*". Prof. Piero Baraldi, for his always interesting insights and for trying to export the hypno-zone to the US. And all the others: Mei, Santiago, Rulan, Ludovico, Beatrice, Darien, Chenyang, Ali, Andre…

I would also like to thank Prof. Katrina Groth and all the SyRRA lab, for welcoming me first as a visiting PhD student and then as a postdoc, and for making me feel part of the group from the very beginning.

Thanks to Sara, for being my ray of light and my safe place. None of this would have been possible without your love and support.

I would like to thank Anna and Gabriele, my parents, and Francesca, my sister, for always encouraging me, especially when things were the most difficult. You are my greatest support, even when we are far apart.

I would also like to thank some of my friends. Enrico, for all the fun and the countless discussions on engineering. Gabriel, for being a dear friend, always ready to listen. Miki, for still being my friend after 25(!) years. Andrea, for all the shared memories and the laughs. Federico, for sharing the university journey and for inviting me to the (second) best lake in Italy.

Finally, a special mention goes to my friend Lisandro, for inviting me to be his "*paraninfo*". It was one of the strangest, but also one of the most fun, experiences of my life.

To all of you who made this journey lighter, richer, and more meaningful: thank you.

List of Acronyms

Acronym	Definition
ACS	Auxiliary Cooling System
AFS	Auxiliary Feedwater System
AGAN	As Good As New
AGAO	As Good As Old
AHP	Analytic Hierarchy Process
BN	Bayesian Network
BP	Blast Proofing
BRANN	Bayesian Regularized Artificial Neural Network
BT	Bow-Tie
CCF	Common Cause Failure
CCMT	Cell-to-Cell Mapping Technique
CDF	Cumulative Distribution Function
CFD	Computational Fluid Dynamics
CP	Coolant Pipe
CPT	Conditional Probability Table
CR	Critical failure Region
CUSUNORO	CUmulative SUm of NOrmalized Reordered Output
DBN	Dynamic Bayesian Network
DESD	Dynamic Event Sequence Diagram
DET	Dynamic Event Tree
DF	Dynamic Flowgraph
DHR	Decay Heat Removal
DI	Design Integrity
DNN	Deep Neural Network
DP	Dynamic Programming
DRL	Deep Reinforcement Learning
eBN	Enhanced Bayesian Network
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EM	Expectation Maximization
ERS	Emergency Response System
ESFR	Early Suppression Fast Response
ET	Event Tree
ETI	Emergency Team Intervention
EX	Explosion
FF	Flash Fire
FM	Fire Management
FP	Fire Proofing
FT	Fault Tree

FWS	Foam-Water Sprinkler system
GA	Genetic Algorithm
GNN	Graph Neural Network
GSA	Global Sensitivity Analysis
HD	High Dependency
HS	Health State
I&D	Isolation and Depressurization
IDPSA	Integrated Deterministic and Probabilistic Safety Assessment
IE	Initiating Event
IL	Imitation Learning
IP	Ignition Probability
IUQ	Inverse Uncertainty Quantification
JF	Jet Fire
KID	Knowledge, Information and Data
KPI	Key Performance Indicator
LBLOCA	Large Break Loss Of Coolant Accident
LD	Low Dependency
LOCA	Loss Of Coolant Accident
LOP	Loss Of Power
LOPA	Layer Of Protection Analysis
LOPC	Loss Of Primary Containment
LP	Linear Programming
LSIR	Location-Specific Individual Risk
LSTM	Long-Short Term Memory
LWR	Light Water Reactor
MAM	Multi-Agent Model
MD	Medium Dependency
MFM	Multilevel Flow Model
MFP	Melting Fuel Plug
MILP	Mixed-Integer Linear Programming
MSE	Mean Squared Error
MSR	Molten Salt Reactor
MU	Multi-Unit
MUPSA	Multi-Unit Probabilistic Safety Assessment
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OI	Operating Integrity
OT	Optimal Transport
PCS	Process Control System
PDF	Probability Density Function
PF	Pool Fire
PFD	Probability of Failure on Demand
PFP	Passive Fire Protection material

PGA	Peak Ground Acceleration
PHM	Prognostics and Health Management
PoF	Physics of Failure
PPO	Proximal Policy Optimization
PPS	Pressure Protection System
PPU	Pyrochemical Processing Unit
PSA	Probabilistic Safety Assessment
PSM	Probabilistic Safety Margin
PSMS	Process Safety Management System
PSO	Particle Swarm Optimization
PSV	Pressure Safety Valve
QRA	Quantitative Risk Assessment
RL	Reinforcement Learning
RNN	Recurrent Neural Network
SC	Spill Containment
SDP	Sequential Decision Problem
SMDFR	Small Modular Dual Fluid Reactor
SMR	Small Modular Reactor
SMS	Safety Management System
SSC	Structures, Systems and Components
TC	Toxic Containment
TFM	Time of Final Mitigation
TM	Task Management
WDS	Water Deluge System
ZD	Zero Dependency

Table of Contents

Abstract i
Sommario ii
Acknowledgements iv
List of Acronyms v
Chapter 1 Introduction 1
Chapter 2 Bayesian Network-based multi-hazard Quantitative Risk Assessment of hydrocarbon facilities 7
Chapter 3 Safety barriers maintenance optimization 25
Chapter 4 Risk-informed design of multi-unit Nuclear Power Plants 56
Chapter 5 Conclusions 99
References 109

Chapter 1
Introduction

1.1 Context and Motivation

Safety-critical energy systems, such as Nuclear Power Plants (NPPs), chemical processing facilities and Oil & Gas (O&G) installations, rely on layers of safety barriers to prevent accidents (preventive barriers) and mitigate their consequences (mitigative barriers) (Y. Liu, 2020; Sklet, 2006). Safety barriers may include technical systems, control and protection functions, passive protections, and emergency response measures that together form the defense-in-depth architecture of such systems. However, as all Structures, Systems, and Components (SSCs), safety barriers degrade in time (Xing et al., 2019b), so as their capability to deal with disruptive events, eventually leading to a larger risk of severe consequences.

A considerable body of literature has addressed the performance assessment of safety barriers. Several frameworks have been proposed, including approaches based on simplified risk indexes (Cozzani et al., 2009), Monte Carlo simulation (Abdolhamidzadeh et al., 2010) and Bow-Tie (BT) diagrams (Cherubin et al., 2011). Subsequent works introduced Layer of Protection Analysis (LOPA)-based frameworks, where independent protection layers are characterized through reliability indicators such as Probability of Failure on Demand (PFD) and effectiveness (Landucci et al., 2015), as well as simulation-based approaches integrating Event Tree Analysis (ETA), Computational Fluid Dynamics (CFD), and evacuation modeling to assess the effectiveness of technical safety barriers and emergency response measures (Yuan et al., 2022).

Safety barrier performance has also been investigated considering Natural hazard–triggered Technological accidents (NaTech scenarios). In this context, methods have been proposed to analyze how natural hazards affect safety barriers performance by modifying their PFD and effectiveness during accident scenarios (Misuri et al., 2020, 2021a), together with safety barriers management frameworks to prevent accident propagation and mitigate cascading effects (T. Zeng et al., 2022). Sensitivity analysis techniques have also been applied to identify the safety barrier performance parameters that most influence system risk and therefore should be investigated in greater detail to reduce model uncertainty (Di Maio et al., 2023a).

In addition, several methodologies have been proposed to evaluate the adequacy of safety barriers and to support their optimal allocation. For instance, some approaches assess the adequacy of preventive barriers by linking their performance to the frequency of hazardous events, thereby evaluating whether the implemented protection layers provide a sufficient level of risk reduction (Sobral & Guedes Soares, 2019). Building upon these assessments, optimization-based approaches have been

proposed to determine the most effective allocation of safety barriers for preventing and/or mitigating accident escalation under economic or operational constraints. For example, multi-objective optimization frameworks have been developed to determine the optimal allocation of protective safety barriers to mitigate domino effects under budget constraints (H. Chen et al., 2026; Janssens et al., 2015). Robust optimization approaches have also been proposed to determine optimal safety barrier performance parameters in presence of uncertainties (Di Maio et al., 2023b).

Despite these advances, most existing approaches still neglect the influence of age-related degradation of safety barriers on their performance and, consequently, on the evolution of system risk over time (Landucci et al., 2016). Thus, traditional (static) risk assessment techniques, such as Event Trees (ETs) (Huang et al., 2001) do not provide the necessary insights to make informed decisions on the re-design and maintenance scheduling of safety barriers, due to the different time constants characterizing their aging and response and mitigation times. Safety barriers degradation has, instead, a great influence on the safety response of the system during an accident, so that a risk assessment that accounts for the barriers degradation and updates the risk profile as they age is crucial to make informed decisions regarding any counteractive actions necessary to keep the risk at an acceptable level throughout the system life and/or any system design modification.

1.2 Overview of the Developed Framework

1.2.1 Problem Statement and Technical Challenges

The risk assessment and management of degrading energy systems pose the following Technical Challenges (TC):

- **TC1**: conventional (i.e., static) risk assessment methodologies are not designed to incorporate evolving information on barrier condition, thus preventing the dynamic updating of the system risk profile as safety features age.
- **TC2**: maintenance planning must be addressed in the presence of degradation dynamics whose effects propagate over time. Existing optimization approaches for safety barrier maintenance typically rely on fixed inspection or replacement intervals and do not account for the sequential nature of maintenance decisions under uncertainty.
- **TC3**: system design must be risk-informed to ensure that safety-critical energy systems operate sufficiently far from critical failure conditions. However, when risk assessments rely on complex, high-fidelity simulators to realistically replicate system physics, it becomes difficult to identify which uncertain input parameters most influence safety-related outcomes and, consequently, to ensure adequate safety margins at the design stage.

These challenges highlight the need for dynamic, condition-informed risk assessment frameworks capable of i) updating risk estimates as barrier condition evolves, ii) supporting adaptive operational decisions over time, and iii) extracting design-relevant insights from complex accident simulations.

1.2.2 Research Objectives and Proposed Methodology

In this context, the objective of this PhD thesis is to develop risk assessment and management methods for degrading energy systems, explicitly accounting for the time-dependent performance of safety barriers and supporting both operational decisions (e.g., maintenance and inspection planning) and design decisions (e.g., installation of additional safety barriers). The thesis addresses the aforementioned challenges through three main research activities shown in **Fig. 1**, which constitute its core contributions.

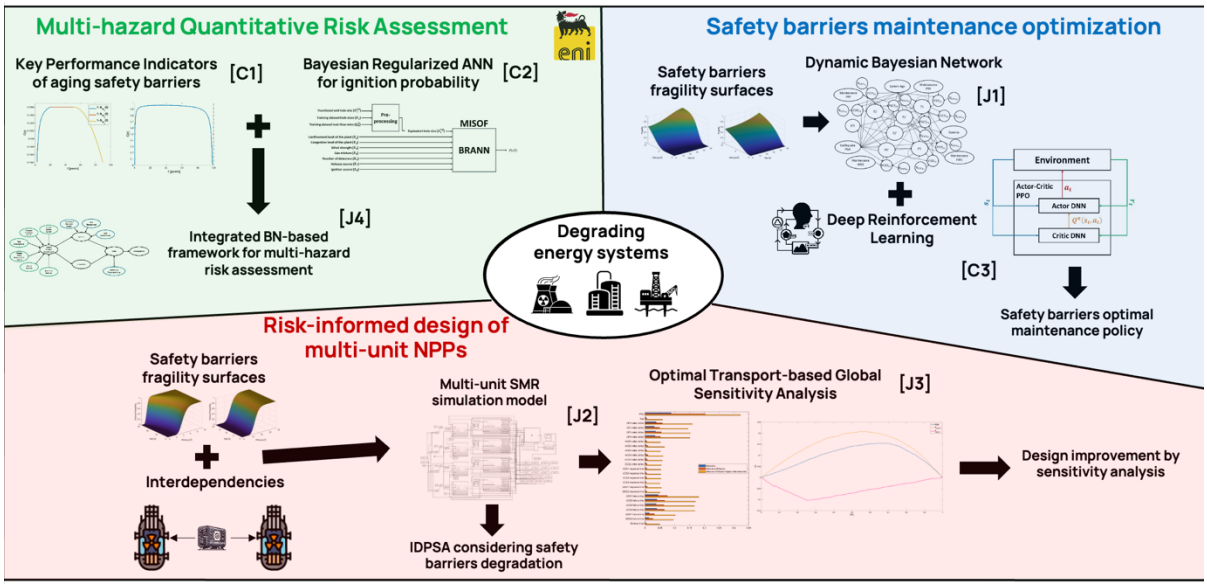


Figure 1. Overview of the research activities.

To address TC1, namely the dynamic updating of system risk in the presence of degrading safety barriers, a Bayesian Network (BN)–based framework for the multi-hazard risk assessment of O&G plants is proposed. The framework explicitly integrates time-dependent KPIs to model the degradation of safety barriers and their evolving effectiveness. To realistically estimate the probability of ignition following a Loss of Primary Containment (LOPC), a Bayesian Regularized Artificial Neural Network (BRANN) is developed and embedded within the BN structure. Furthermore, the framework uses a multi-hazard, multi-source risk aggregation procedure to compute the Location-Specific Individual Risk (LSIR), while explicitly accounting for uncertainties in both scenario frequency and severity.

To address TC2, namely the need for adaptive maintenance strategies under time-dependent degradation, a risk-based maintenance optimization framework for degrading safety barriers is proposed. In this framework, fragility surfaces are introduced to characterize the time-dependent fragility of safety barriers to hazards within a Physics-of-Failure (PoF)-based framework. These fragility models are

embedded within a Dynamic Bayesian Network (DBN), which models the accidental scenario evolution. The DBN is then used as the environment of a Deep Reinforcement Learning (DRL) algorithm, enabling the identification of optimal maintenance policies that balance risk reduction and maintenance effort over time.

Finally, to address TC3, namely the extraction of design-relevant insights from complex simulation outputs of multi-unit systems, first an Integrated Deterministic and Probabilistic Safety Assessment (IDPSA) framework is developed to dynamically assess how the age-dependent degradation of shared safety features impacts system risk. Then, a risk-informed design framework for multi-unit energy systems is developed by combining Global Sensitivity Analysis (GSA) indices based on Optimal Transport (OT) with a graphical visualization tool based on the CUmulative SUm of NOrmalized Reordered Output (CUSUNORO). The OT-based indices enable the identification of the most influential input parameters, even in the presence of multivariate, non-linear, and time-dependent inputs. The CUSUNORO visualization, in turn, allows the identification of safety-critical ranges of these inputs, providing actionable insights for design modifications and system optimization.

Related publications in academic journals and conference proceedings are shown in **Tab. 1**.

Table 1. Publication list.

ID	Title	Authors	Status
J1	A Physics-of-Failure (PoF) model-based Dynamic Bayesian Network for considering the aging of safety barriers in the risk assessment of industrial facilities	Stefano Marchetti, Francesco Di Maio, Enrico Zio	Published in *Journal of Loss Prevention in the Process Industries, volume 91, 2024. DOI: 10.1016/j.jlp.2024.105402*
J2	An Integrated Deterministic and Probabilistic Safety Assessment of Multi-Unit Small Modular Reactors Considering the Degradation of Shared Safety Features	Stefano Marchetti, Francesco Di Maio, Enrico Zio	Published in *Nuclear Science and Engineering, 2025. DOI: 10.1080/00295639.2025.2515349*
J3	A global sensitivity analysis framework for guiding the design improvement of new	Stefano Marchetti, Francesco Di Maio, Enrico Zio,	Published in *Nuclear Engineering and Design, volume 444, 2025.*

	concepts of small modular reactors	Emanuele Borgonovo, Elmar Plischke	*DOI: 10.1016/j.nucengdes.2025.114398*
J4	A Bayesian Network Framework for Multi-Hazard Quantitative Risk Assessment of Oil and Gas Facilities Undergoing Degradation	Stefano Marchetti, Francesco Di Maio, Enrico Zio, Luca Decarli, Laura La Rosa, Giuseppe Nicotra, Andrea Tortora	Under review in *Reliability Engineering and System Safety*
J5	Risk assessment for modern industry	Luca Pinciroli, Seyed Ali Hosseini, Mei Chen, Maria Valentina Clavijo Mesa, Thomas Matteo Coscia, Juan-Pablo Futalef, Stefano Marchetti, Leonardo Miqueles, Santiago Taguado Menza, Enrico Zio	Published in Reliability Engineering and System Safety, volume 269. DOI: 10.1016/j.ress.2025.112126
J6	Risk-informed design of coupled High Temperature Electrolysis Facilities and Nuclear Power Plants by Enhanced Bayesian Networks	Stefano Marchetti, Andrea Perin, Francesco Di Maio, Enrico Zio	Under internal review
J7	A time-dependent Global Sensitivity Analysis framework for passive safety systems in Nuclear Power Plants	Stefano Marchetti, Francesco Di Maio, Enrico Zio, Emanuele Borgonovo, Elmar Plischke	Under internal review
C1	Key performance indicators for aging safety barriers in oil and gas facilities	Stefano Marchetti, Francesco Di Maio, Enrico Zio, Luca Decarli, Laura La Rosa, Giuseppe Nicotra	Published in *European Conference On Safety And Reliability (ESREL), 2023, 2230–2235. DOI: 10.3850/978-981-18-8071-1_P708-cd*
C2	A Bayesian Regularized Artificial Neural Network For Estimating The Ignition Probability In Oil And Gas Plants	Stefano Marchetti, Francesco Di Maio, Enrico Zio, Luca Decarli, Laura La Rosa, Giuseppe Nicotra, Andrea Tortora, Anna Crivellari, Salvatore Cincotta	Published in *European Conference On Safety And Reliability (ESREL), 2024.* ISBN 978-83-68136-03-6
C3	A Deep Reinforcement Learning method for finding the risk-based optimal prescriptive maintenance policy of degrading safety barriers	Stefano Marchetti, Francesco Di Maio, Enrico Zio	Published in *International Conference on System Reliability and Safety (ICSRS), 2024. pp. 177-183, doi: 10.1109/ ICSRS63046.2024.10927451*

C4	Preliminary hazard analysis for hydrogen production by coupled High Temperature Electrolysis Facilities and Nuclear Power Plants	Stefano Marchetti, Francesco Di Maio, Samantha E. Wismer, Katrina M. Groth, Enrico Zio	Published in *European Conference On Safety And Reliability (ESREL), 2025. doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4661-cd*
C5	Computational risk assessment framework for coupled High Temperature Electrolysis Facilities powered by Nuclear Power Plants	Stefano Marchetti, Francesco Di Maio, Samantha E. Wismer, Katrina M. Groth, Enrico Zio	Accepted in *European Conference On Safety And Reliability (ESREL), 2026*

1.2.3 Case Studies

For demonstration purposes and without loss of generality, the proposed frameworks have been applied on the following realistic case studies:

- *Onshore hydrocarbon facility*: a real facility composed of 15 functional units, each equipped with several preventive and mitigative safety barriers has been considered for showcasing the applicability of the BN-based framework developed to address TC1.
- *Chemical storage facility*: a realistic chemical facility storing flammable substances exposed to earthquakes and equipped with active, passive and procedural safety barriers has been considered to demonstrate the Physics-of-Failure (PoF)-based dynamic risk assessment and maintenance optimization framework developed to address TC2.
- *Multi-unit Nuclear Power Plant (NPP)*: an NPP composed by four units of Small Modular Dual Fluid Reactor (SMDFR) with shared safety systems and exposed to earthquakes has been considered to showcase the applicability of the IDPSA and the subsequent GSA framework developed to address TC3.

1.3 Thesis Structure

The remainder of the thesis is structured as follows:

- Chapter 2 presents a BN-based multi-hazard QRA framework, demonstrated through its application to a real hydrocarbon processing facility.
- Chapter 3 introduces a PoF-based dynamic risk assessment framework to account for the degradation of safety barriers and its integration within a RL environment for risk-informed safety barriers maintenance optimization.
- Chapter 4 presents an IDPSA framework for multi-unit NPPs with shared safety barriers, alongside a GSA approach for risk-informed system design.
- Chapter 5 summarizes the main findings and conclusions of the thesis.

Chapter 2
Bayesian Network-based multi-hazard Quantitative Risk Assessment of hydrocarbon facilities

Contents of this Chapter have been adapted from:

[C1] *S. Marchetti, F. Di Maio, E. Zio, L. Decarli, L. La Rosa, and G. Nicotra, "Key performance indicators for aging safety barriers in oil and gas facilities," in European Conference On Safety And Reliability (ESREL), 2023, pp. 2230–2235. doi: 10.3850/978-981-18-8071-1_driver.*

[C2] *S. Marchetti, F. Di Maio, E. Zio, L. Decarli, L. La Rosa, G. Nicotra, A. Tortora, A. Crivellari and S. Cincotta, "A Bayesian Regularized Artificial Neural Network For Estimating The Ignition Probability In Oil And Gas Plants" in European Conference On Safety And Reliability (ESREL), 2024.*

[J4] *S. Marchetti, F. Di Maio, E. Zio, L. Decarli, L. La Rosa, G. Nicotra, A. Tortora, "A Bayesian Network Framework for Multi-Hazard Quantitative Risk Assessment of Oil and Gas Facilities Undergoing Degradation" under review in Reliability Engineering and System Safety.*

2.1 Introduction

Safety-critical energy systems, such as hydrocarbon facilities, are equipped with preventive and mitigative safety barriers for reducing the likelihood of process safety incidents and mitigating their consequences (Di Maio, Marchetti, et al., 2023a, 2023b; ISO 17776, 2016). To assess and manage the risk, periodic Quantitative Risk Assessments (QRAs) are carried out (Kalantarnia et al., 2009). Such QRAs are intended to provide the current risk profile, given the current state of health of the plant components and systems ((Marchetti, Di Maio, & Zio, 2024a; Marchetti et al., 2023, 2025)). However, conventional methodologies of QRA (Ab Rahim et al., 2024; Andonov, 2017; "Guidelines for Risk Based Process Safety," 2010; Khakzad et al., 2013) present a number of limitations in doing that, as they:

I. for the assessment of safety barriers performance, rely on approaches (to name a few, simplified risk indexes (Cozzani et al., 2009), Monte Carlo simulation (Abdolhamidzadeh et al., 2010) and Bow-Tie (BT) diagrams (Cherubin et al., 2011), which i) do not allow the integration of various forms of dynamically available Knowledge, Information and Data (KID) (Zio, 2016) collected on the plant by inspections and/or measurements by digital systems (Aneziris et al., 2017; Goble & Bier, 2013; Villa et al., 2016) and ii) still neglect the influence of the safety barriers degradation on their performance (Landucci

et al., 2016), which instead has a great influence on the safety response of the system during an accident (Di Maio, Scapinello, Zio, Ciarapica, et al., 2021);

II. aggregate the risk arising from different hazards by summing the frequencies and severities of the individual hazards (Bjørnsen & Aven, 2019), neglecting their uncertainty.

While some approaches have been proposed in the literature to account for the degradation of safety barriers using the available KID (Di Maio, Scapinello, Zio, Ciarapica, et al., 2021) and others for the quantification of uncertainty when aggregating risk from multiple hazards (Decarli et al., 2021), an integrated framework that addresses both limitations has not been proposed. With respect to the KID integration, Bayesian Networks (BNs) have been used to represent component degradation by integrating condition monitoring and inspection data (Xing et al., 2019a); Dynamic Bayesian Networks (DBNs) have been adopted to model fatigue crack growth in structural components (D. Lee & Kwon, 2023) and chemical degradation of concrete structures exposed to climate change (Hosseini et al., 2026); DBNs have also been applied to model the degradation of safety barriers subjected to external hazards, such as earthquakes (Marchetti, Di Maio, & Zio, 2024a). However, a comprehensive BN-based framework that integrates safety barriers degradation modeling within a multi-hazard QRA workflow and enables plant-level Location Specific Individual Risk (LSIR) estimation, while remaining computationally tractable for large facilities and heterogeneous KID sources, has not yet been proposed. BNs have been here chosen, as we shall see in what follows, because of their ability to explicitly represent causal relationships between initiating events, safety barriers, and accident consequences, while allowing the integration of heterogeneous sources of KID. Also, BNs allow for both forward and backward inference, enabling not only the estimation of consequence frequencies given barrier health states, but also diagnostic reasoning to identify critical combinations of barrier degradations. Finally, BN inference is computationally efficient once the network structure is defined, making the approach suitable for repeated evaluations across multiple functional units and hazard types, as required for LSIR assessment in large-scale hydrocarbon facilities. In this work we propose a BN-based framework that addresses these limitations, by originally using:

I. a set of BNs (one for each functional unit of the plant) to calculate the frequency of the consequences following a LOPC event. The nodes of the BNs are the LOPC event, the allocated safety barriers and the consequences. Each node of the safety barriers can have multiple states, to describe their Health States (HSs) with reference to their functional performance (i.e., High (H), Medium (M) and Low (L); to each HS corresponds an associated Failure Probability (FP), i.e., the probability of failing to perform the safety function given the HS, and an effectiveness η to represent the effect of the safety function when performed at that HS. in terms of the probability that the barrier, once activated, is successful in mitigating the accident (Sklet, 2006). Depending on the safety barrier, the

functional performance is characterized based on process monitoring data or specific Key Performance Indicators (KPIs) (Di Maio, Scapinello, Zio, Ciarapica, et al., 2021);

II. a multi-hazard and multi-source risk aggregation procedure to calculate the LSIR accounting for the uncertainties on the frequency and severity of the accidental scenarios (Decarli et al., 2021);

III. a Bayesian Regularized Artificial Neural Network (BRANN) (J. Shi et al., 2018), to efficiently and accurately estimate the Ignition Probability (IP) following a LOPC (Marchetti, Di Maio, Zio, et al., 2024);

2.2 The proposed framework

Let us consider a hydrocarbon facility composed of $i = 1,2, \dots, N_F$ functional units and exposed to a set of possible accidental scenarios (e.g., LOPC leading to fire or explosion). Each functional unit is characterized in terms of:

- position in the system layout;
- level of confinement (e.g., non-confined, confined on one side, confined on two sides…);
- level of congestion (e.g., high congestion, typical congestion, low congestion…);
- exposure to wind strength;
- type of fluid processed (and, if gaseous, type of gas mixture);
- possible release sources (e.g., pump, other);
- possible ignition sources (e.g., electrical machinery, rotating machinery, other).

Each *i-th* functional unit is equipped with $N_{p,i}$ preventive safety barriers and $N_{m,i}$ mitigative safety barriers. Let us assume that we have available the following KID:

- condition monitoring data of the process variables (e.g., pressure, temperature…);
- specific KPIs regarding the safety barriers performance, evaluated either through safety-relevant event reports or structured questionnaires;
- characteristics of the accidental scenarios: i) consequence type (e.g., Jet Fire (JF), Pool Fire (PF), Flash Fire (FF) and Explosion (EX), ii) baseline LOPC frequency $F_{LOPC,0}$ (i.e., without considering any safety barrier) and iii) relevant impact parameters (e.g., heat radiation for fire scenarios, overpressure for explosions…).

The proposed framework, sketched in **Fig. 2**, elaborates the KID through:

- one BN for each functional unit (i.e., $BN_1, BN_2, \dots, BN_{N_F}$); the Conditional Probability Tables (CPTs) of the nodes of the BNs are estimated:
    - for the safety barriers nodes, using process monitoring data and KPIs;

- for the ignition node, using a BRANN trained on data from Computational Fluid Dynamics (CFD) simulations of the ignition process;

- a multi-source and multi-hazard procedure to aggregate the output of the BNs for providing the plant-level aggregated LSIR.

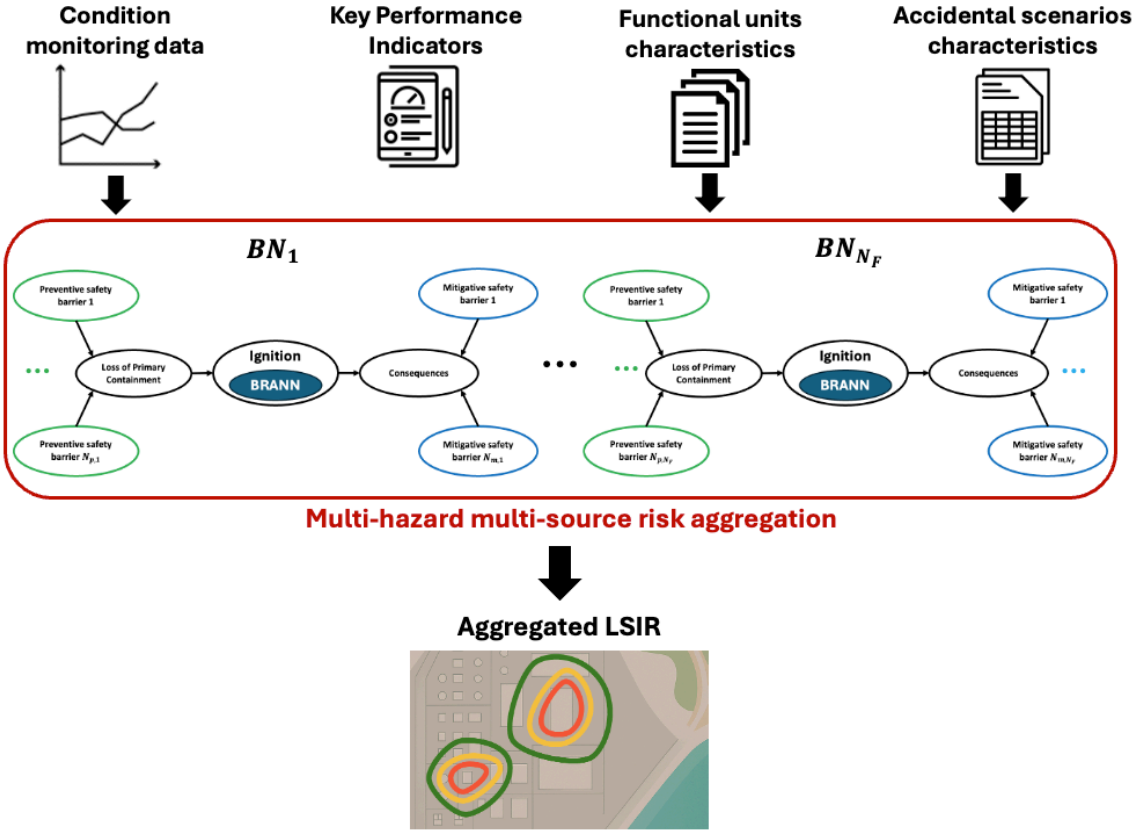


Figure 2. The proposed framework of analysis.

2.2.1 Bayesian Networks of the functional units

For each of the $i = 1,2,\dots,N_F$ functional units of the system, a BN_i structure is defined based on an expert-based causal dependency assessment among the following nodes, also shown in **Fig. 3**:

- *Preventive safety barriers*: discrete multi-state nodes with three states (H, M, L), one for each HS, in line with the industrial partner standard practice;
- *Loss of Primary Containment*: binary node for the occurrence or not of a LOPC;
- *Ignition*: discrete multi-state node with three states (immediate, delayed and no ignition), to describe the ignition event following a LOPC;
- *Mitigative safety barriers*: discrete multi-state nodes with three states (H, M, L), one for each HS, in line with the industrial partner standard practice;
- *Consequences*: discrete multi-state node with four states (i.e., JF, PF, FF and EX) to represent the consequent process following an ignition event.

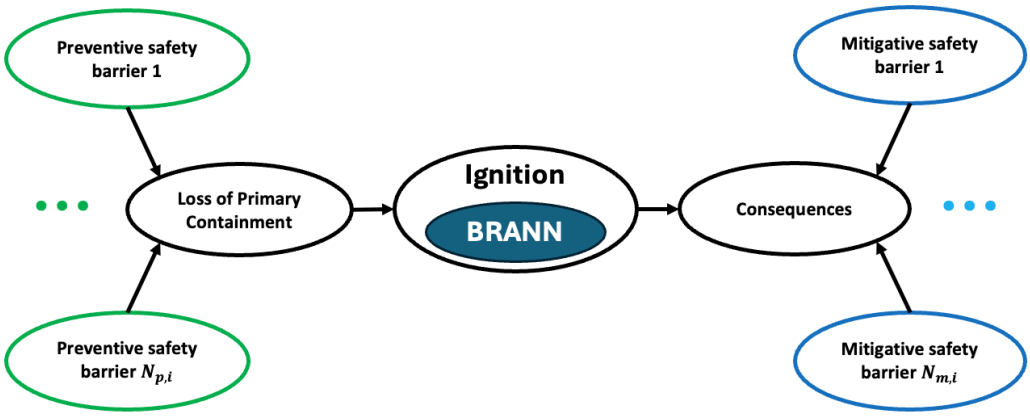


Figure 3. BN structure of a generic i-th functional unit with its preventive and mitigative safety barriers.

The CPTs of the BN nodes are defined as follows:

- *Preventive safety barriers*: the failure to function of the generic *j-th* preventive safety barrier is described in terms of the probability P_j that the barrier is in the *j-th* HS, $j \in \{H, M, L\}$, and of the failure probability FP_j when the barrier is in the *j-th* HS. For the safety barriers that are continuously monitored, P_j is estimated by means of multi-dimensional Probabilistic Safety Margins (PSMs) that are calculated using process monitoring data (as in (Zio et al., 2010). In case of scarcity of data, Order Statistics (OS) can be employed to obtain statistically sound estimates of the PSMs (Nutt & Wallis, 2004). For event-based safety barriers, the P_j calculation method is tailored on each specific KPI, as discussed in (Di Maio, Scapinello, Zio, Ciarapica, et al., 2021). When quantitative data are scarce, expert knowledge can be systematically integrated within the BN to calculate P_j, which can be eventually updated by Bayesian inference when data becomes available (Podofillini et al., 2023). FP_j is estimated using either failure data, when available, or an Analytic Hierarchy Process (AHP)-informed expert elicitation (as in (R. W. Saaty, 1987). More details about the safety barriers functional failure process characterization can be found in **Appendix A**.

- *Loss of Primary Containment:* in this work, we assume that LOPC occurs only when all preventive safety barriers fail, and that safety barriers failures are conditionally independent, based on the industrial partner defense-in-depth approach that assumes all the safety systems are to be designed to be functionally independent and sufficient to prevent the accident (International Atomic Energy Agency, 1996). For illustrative purposes, considering a generic *i-th* functional unit with two preventive safety barriers, the LOPC frequency (F_{LOPC}) is:

$$F_{LOPC,i} = F_{LOPC,0,i} \cdot \sum_{j,l} P_j^1 \cdot FP_j^1 \cdot P_l^2 \cdot FP_l^2 \qquad (1)$$

where $F_{LOPC,0,i}$ is the baseline frequency of LOPC at the *i-th* functional unit without considering any safety barrier, $P_{j(l)}^{p}$ is the probability that the *p-th* preventive barrier is in HS *j (l)* and $FP_{j(l)}^{p}$ is the FP associated with the *p-th* preventive barrier in HS *j (l)*, with $p = 1{,}2$ and $j, l \in \{H, M, L\}$.

- *Ignition*: for the ignition, we follow the MISOF approach (MISOF, 2018), splitting the IP into two contributions: the probability P_{imm} of immediate ignition occurring immediately after the LOPC, and the probability P_{del} of delayed ignition occurring after the formation of a flammable cloud following the LOPC (MISOF, 2018). For functional units processing gas, we assume $P_{imm} = 7.2 \cdot 10^{-2}$ if the ignition source is a pump and $P_{imm} = 7 \cdot 10^{-4}$ for any other ignition source (MISOF, 2018). To estimate P_{del}, following (Di Maio, Scapinello, Zio, Cincotta, et al., 2021), a BRANN is trained using a dataset of CFD simulations run with 14263 random configurations of the input variables of **Tab. 1**, where the discrete values have been chosen by expert judgement to represent the operating conditions that are expected to occur at the industrial partners plant sites

Table 2. Inputs of the BRANN model.

Input variable	Input name	Values
X_1	LOPC hole size input range	$\in [1{,}200]\ mm$
X_1^{train}	LOPC hole size in the training dataset	$5\ mm$ $20\ mm$ $50\ mm$ $100\ mm$
X_2	Confinement level	"A" "B" "C" "D"
X_3	Congestion level	0 0.3 0.7 1 1.3 1.7
X_4	Wind strength	"5D" "2F"
X_5	Type of gas mixture	"Light" "Neutral"

		“Heavy”
X_6	Release source	“Pump” “General” “Other”
X_7	Ignition source	“Electrical machinery” “Rotating machinery” “All” “Other”

To use the trained BRANN, the following input pre-processing strategy is adopted (**Fig. 4**) (Marchetti, Di Maio, Zio, et al., 2024):

1. a suitable simulation consequence modeling software (Y. Chen, 2020) is run to calculate the peak gas leak flow rate Q_0^{FU} (i.e., the leak flow rate at $t = 0$) resulting from a LOPC of given hole size in the selected functional unit;
2. Q_0^{FU} is compared with the peak gas leak flow rate values Q_0^T resulting from the hole sizes (X_1^{train}) used to train the BRANN;
3. a conservative (i.e., with a larger leak flow rate) equivalent hole size (X_1^{EQ}) is calculated and fed to the BRANN by selecting the smallest X_1^{train} generating $Q_0^T \geq Q_0^{FU}$.

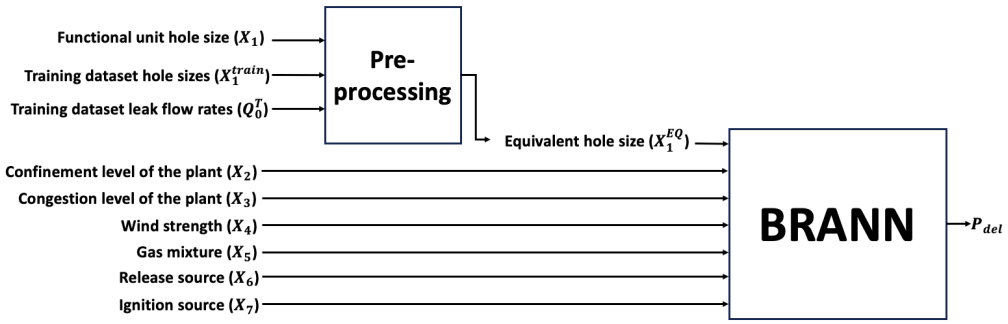


Figure 4. BRANN preprocessing strategy.

A detailed description of the BRANN model architecture, training dataset, preprocessing steps, and validation procedure is provided in (Di Maio, Scapinello, Zio, Cincotta, et al., 2021; Marchetti, Di Maio, Zio, et al., 2024).

For functional units processing oil, a commercial consequence modeling software is run to calculate Q_0^{FU} resulting from a LOPC of given hole size; then, $P_{del} = P_{imm}$ is extrapolated from empirical data, which relate P_{del} with the leak flow rate (Energy Institute, 2006), as shown in **Fig. 5**.

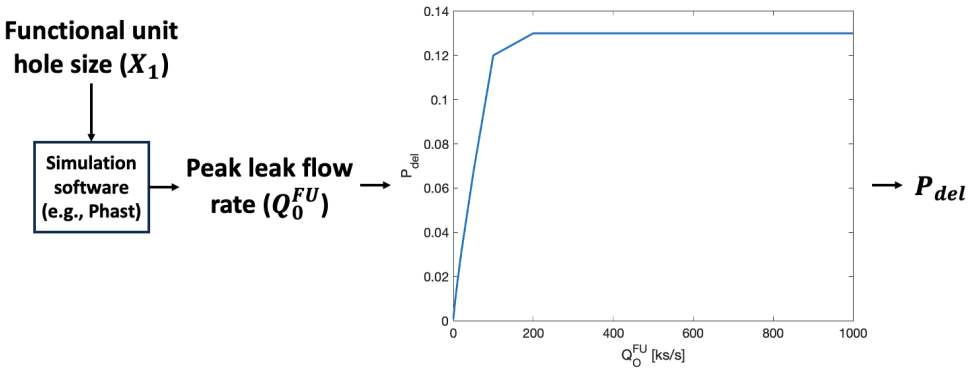


Figure 5. P_{del} estimation procedure for functional units processing oil.

- *Mitigative safety barriers*: the failure to function of the mitigative safety barriers is characterized in terms of P_j, FP_j and η_j. P_j and FP_j are estimated as for preventive safety barriers; depending on availability of data, η_j is estimated using either the available failure data or an AHP-informed expert elicitation for barriers lacking data (Karayalcin, 1982; T. L. Saaty, 2002).
- *Consequences*: the frequencies of the four possible consequences (i.e., F_c with $c \in \{PF, JF, FF, EX\}$) are calculated following (Di Maio, Scapinello, Zio, Ciarapica, et al., 2021):
  - immediate ignition:

$$F_{PF} = F_{LOPC} \cdot P_{imm} \cdot P_{PF|imm} \cdot \mu_b \quad (2)$$

$$F_{JF} = F_{LOPC} \cdot P_{imm} \cdot P_{JF|imm} \cdot \mu_b \quad (3)$$

where $P_{PF|imm} = \frac{1}{6}$ is the probability of PF given an immediate ignition (Di Maio, Scapinello, Zio, Ciarapica, et al., 2021), $P_{JF|imm} = 1 - P_{PF|imm} = \frac{5}{6}$ is the probability of JF given an immediate ignition and μ_b is a factor accounting for the action of mitigative safety barriers; considering the action of two preventive safety barriers, μ_b is calculated as (Decarli et al., 2021):

$$\mu_b = \sum_{j \in \{H,M,L\}} \sum_{w \in \{H,M,L\}} P_j^1 \cdot \left(FP_j^1 + \left(1 - \eta_j^1\right)\right) \cdot P_l^2 \cdot \left(FP_w^2 + (1 - \eta_w^2)\right) \quad (4)$$

where η_j^p is the effectiveness associated with the *p-th* mitigative safety barrier in HS *j (l)*, with $p = 1,2$ and $j, l \in \{H, M, L\}$.

  - delayed ignition:

$$F_{FF} = F_{LOPC} \cdot P_{del} \cdot P_{FF|del} \cdot \mu_b \quad (5)$$

$$F_{EX} = F_{LOPC} \cdot P_{del} \cdot P_{EX|del} \cdot \mu_b \quad (6)$$

where $P_{FF|del}$ is the probability of FF given a delayed ignition and $P_{EX|del} = 1 - P_{FF|del}$ is the probability of EX given a delayed ignition. $P_{FF|del}$ is a function of the congestion level of the plant:

$$\begin{cases} P_{FF|del} = 1 & if\ congestion = 0 \\ P_{FF|del} = 0.9 & if\ congestion = 0.3 \\ P_{FF|del} = 0.7 & if\ congestion = 0.7\ or\ congestion = 1 \\ P_{FF|del} = 0.5 & if\ congestion = 1.3 \end{cases} \quad (7)$$

2.2.2 Aggregated LSIR assessment

The aggregated LSIR represents the individual risk at a specific location within the plant layout, accounting for all potential hazardous events. To assess the LSIR, it is necessary to calculate and aggregate the frequency and severity of all the possible accidental scenarios. To do so, here we adopt the procedure in (Decarli et al., 2021), wherein the following steps are performed for each $i = 1,2,\dots,N_F$ functional unit, each $c = 1,2,3,4$ hazard type (respectively PF, JF, FF, EX) and each $h = 1,2,\dots,N_H$ LOPC hole dimension:

- calculate $F_{i,c,h}$ with the BN defined in Section 2.2.1;
- calculate the severity of the accidental scenario $S_{i,c,h}$ with the following probit models from (Health and Safety Executive (HSE), 2013):

$$\begin{cases} S_{i,c,h} = -14.9 + 2.56 \ln\left(t_{exposure} \cdot I^{\frac{4}{3}}\right) & if\ c = PF, JF, FF \\ S_{i,c,h} = 5.13 + 1.37 \ln(O) & if\ c = EX \end{cases} \quad (8)$$

  where $t_{exposure} = 60\ s$ is the time of exposure, $I\ \left[\frac{kW}{m^2}\right]$ is the heat radiation due to the fire and $O\ [barg]$ is the overpressure due to the explosion;

- to account for uncertainties in frequency and severity, two noninformative prior probability distributions are adopted, constrained on $F_{i,c,h}$ and $S_{i,c,h}$ (Atwood, 1996; Syversveen, 1998). In particular, a gamma distribution for the frequency and a beta distribution for the severity are adopted, in line with (Decarli et al., 2021). Then, a Monte Carlo simulation with M trials is performed, and for each *m-th* trial:
  - sample a frequency value $f_{i,c,h,m}$ and a severity value $s_{i,c,h,m}$ from Eq. 9 and Eq. 10, respectively:

$$p(F_{i,c,h}) = Gamma\left(0.5, \frac{1}{2F_{i,c,h}}\right) \quad (9)$$

$$p(S_{i,c,h}) = Beta\left(0.5, \frac{1 - S_{i,c,h}}{2S_{i,c,h}}\right) \quad (10)$$

  - calculate the aggregated multi-hazard and multi-source frequency f_m and severity s_m with Eq. 11 and Eq. 12, respectively:

$$f_m = \sum_{i=1}^{N_F} \sum_{c \in \{PF,JF,FF,EX\}} \sum_{h=1}^{N_H} f_{i,c,h} \quad (11)$$

$$s_m = \bigcup_{i,c,h} s_{i,c,h} \tag{12}$$

where $\bigcup_{i,c,h}$ is the union operator over i, c and h The aggregation assumes that accidental scenarios are mutually exclusive and conditionally independent. As a result, combined or cascading accident sequences (e.g., domino effects or multi-event escalation) are not explicitly accounted for, and the analysis focuses on the contribution of individual scenarios to the overall LSIR.

- fit the M values of f_m and s_m to a frequency distribution $F \sim Gamma(\alpha, \beta)$ and severity distribution $S \sim Beta(\gamma, \theta)$;
- use the expected values of f and s (i.e., $\mathbb{E}[F] = \frac{\alpha}{\beta}$ and $\mathbb{E}[S] = \frac{\gamma}{\gamma+\theta}$, respectively) to calculate the aggregated LSIR as follows:

$$LSIR = \mathbb{E}[F] \cdot \mathbb{E}[S] \tag{13}$$

The procedure is repeated for each $k = 1,2, \dots, N_k$ coordinate of the system layout, to provide a system-level risk profile. The aggregated LSIR should be interpreted as the expected individual risk at a given location under the current state of knowledge, conditional on the assumed model structure and available data. Uncertainty is explicitly propagated through the risk aggregation procedure by assigning probability distributions to scenario frequencies and severities. These distributions primarily represent epistemic uncertainty arising from limited knowledge, data scarcity, and model assumptions, while aleatory variability is embedded in the baseline frequencies of the accidents and in the consequence models adopted.

The proposed Bayesian framework can be scaled up to larger systems, since each functional unit is modeled through a BN of limited and manageable size, leading (each one independently) to fast inference times. Thanks to the modular structure of the BNs, the overall inference computational cost increases linearly with the number of functional units; this avoids the construction of a single BN, whose inference would become computationally intractable as system complexity grows. Also, it is worth mentioning that the proposed framework makes the BN suitable to be applied to other plants with similar purposes (i.e., equipped with some functional units though arranged differently on the plant site).

Finally, regarding the validation of the proposed framework, the BN structure and safety barriers performance characterization adopted have been benchmarked against existing QRA frameworks in (Di Maio, Scapinello, Zio, Ciarapica, et al., 2021), while the multi-hazard aggregation procedure has been validated in (Decarli et al., 2021).

2.2.3 Risk updating

As new data on the safety barriers HS becomes available during the system life, the proposed framework allows a straightforward update of the system risk-profile, by

using the data to update the CPTs of the safety barriers nodes and consequently the aggregated LSIR.

2.3 Case study

The case study is a real hydrocarbon facility, which has been anonymized for confidentiality reasons.

The anonymized facility layout is shown in **Fig. 6**.

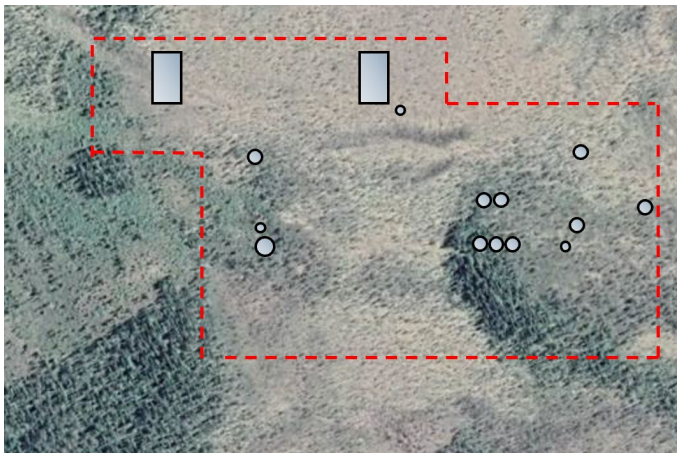


Figure 6. Case study layout.

The safety barriers are listed in **Tab. 3**.

Table 3. Safety barriers.

Safety barrier	Classification	Description
Process Control System (PCS)	Preventive, Continuously monitored	Process variables monitoring and control
Design Integrity (DI)	Preventive, Event-based	Definition of specific mitigation requirements during operations, maintenance, inspection and control
Operating Integrity (OI)	Preventive, Event-based	Ensures the timely action of all safeguarding systems and the mechanical integrity of the equipment
Pressure Protection System (PPS)	Preventive, Event-based	Relieves the system from excessive pressure
Task Management (TM)	Preventive, Event-based	Ensures the fulfillment of operating procedures and requirements, enforces safety rules and provides staff training
Process Safety Management System (PSMS)	Preventive, Event-based	Application of high-level standards (e.g., best practice on the design, operational management…)
Fire Management (FM)	Mitigative, Event-based	Several means to extinguish a fire outbreak
Emergency Response System (ERS)	Mitigative, Event-based	Systematic response to unexpected and/or dangerous occurrence
Fire Proofing (FP)	Mitigative, Event-based	Passive fire protection (e.g., fire wall)

Blast Proofing (BP)	Mitigative, Event-based	Passive explosion protection (e.g., blast wall)
Isolation and Depressurization (I&D)	Mitigative, Event-based	Emergency shutdown, isolation and depressurization
Spill Containment (SC)	Mitigative, Event-based	Confine spillages within a barrier or drainage area
Toxic Containment (TC)	Mitigative, Event-based	Confine releases of toxic gases

The facility is composed of $N_F = 15$ functional units, as listed in **Tab. 4** together with their working fluids and corresponding safety barriers.

Table 4.Functional units with working fluid and equipped safety barriers.

Safety barrier	Classification	Description
Process Control System (PCS)	Preventive, Continuously monitored	Process variables monitoring and control
Design Integrity (DI)	Preventive, Event-based	Definition of specific mitigation requirements during operations, maintenance, inspection and control
Operating Integrity (OI)	Preventive, Event-based	Ensures the timely action of all safeguarding systems and the mechanical integrity of the equipment
Pressure Protection System (PPS)	Preventive, Event-based	Relieves the system from excessive pressure
Task Management (TM)	Preventive, Event-based	Ensures the fulfillment of operating procedures and requirements, enforces safety rules and provides staff training
Process Safety Management System (PSMS)	Preventive, Event-based	Application of high-level standards (e.g., best practice on the design, operational management…)
Fire Management (FM)	Mitigative, Event-based	Several means to extinguish a fire outbreak
Emergency Response System (ERS)	Mitigative, Event-based	Systematic response to unexpected and/or dangerous occurrence
Fire Proofing (FP)	Mitigative, Event-based	Passive fire protection (e.g., fire wall)
Blast Proofing (BP)	Mitigative, Event-based	Passive explosion protection (e.g., blast wall)
Isolation and Depressurization (I&D)	Mitigative, Event-based	Emergency shutdown, isolation and depressurization
Spill Containment (SC)	Mitigative, Event-based	Confine spillages within a barrier or drainage area
Toxic Containment (TC)	Mitigative, Event-based	Confine releases of toxic gases

The analysis is performed using a KID over an assumed 18-month period. For each functional unit, the data considered for the safety barriers assessment consists in:

- for continuously monitored safety barriers (i.e., PCS), illustrative time series of the relevant process variables (e.g., pressure, temperature, oil level…) within the considered time window; an example is shown in **Fig. 7**, where the quantitative axes have been omitted for confidentiality reasons;

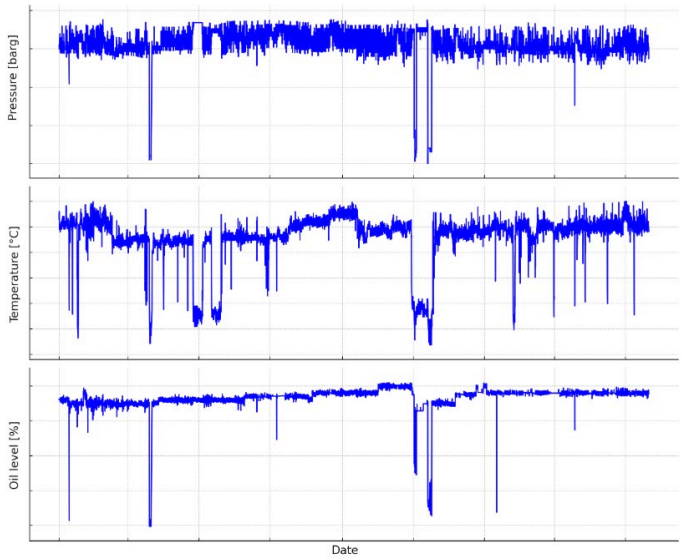


Figure 7. An example of process variables time series.

- for the event-based safety barriers (i.e., DI, OI, PPS, TM, PSMS, FM, ERS, FP, BP, I&D, SC, TC), specific KPI values are defined to represent the barriers performance during the considered time window. In practice, such KPIs could be assigned. through the analysis of safety-relevant reports or structured questionnaires to the plant managers. As an illustrative example, **Tab. 5** reports tentative KPI values for the EP functional unit together with the values assumed to be collected from a previous monitoring/inspection interval (when available) and the corresponding reasonably realistic distribution used to characterize the safety barriers performance (as described in **Appendix A**). The distribution can be either Gaussian $N(\mu, \sigma)$ (where μ is the mean and σ is the standard deviation) in case of normally distributed KPIs, or Kronecker delta $\delta_{KPI,KPI_{opt}}$ (where KPI_{opt} is the optimal value of the KPI) in case of binary KPIs. No distribution is associated to KPIs evaluated through a questionnaire.

Table 5. Example of KPI values and distributions for the EP.

Safety barrier	KPI	Value	Previous value	Distribution
DI	Emergency/process shutdown indicator	40	Not available	$N(53,26)$

DI	Assessment findings	100	Not available	$\delta_{100,100}$
DI	LCI	59	Not available	$N(80,39)$
DI	Tier 3.5	0	101	$N(84,64)$
DI	Tier 4.5	95	100	$N(80,39)$
DI	I&O>30 days	0	0	$\delta_{0,0}$
OI	Leak indicator	58.2	38.35	$N(62,90)$
OI	G1 indicator	93	93	$N(87,13)$
PPS	Tier 4.2	0	Not available	$\delta_{0,0}$
TM	Permit to work	0.27	0.51	$N(4.3,2.5)$
TM	Tier 3.6	2.59	2,4	$N(9.7,9)$
TM	Tier 4.6	2.72	3.5	$N(4,1.9)$
TM	Training parameter	24.7	22	$N(83,26)$
TM	Average training indicator	31	24	$N(45,19)$
PSMS	Leak indicator	58.2	38.35	$N(62,90)$
PSMS	Standard Level of Maturity	63.7	67.14	$N(40,38.5)$
FM	Backlog on preventive maintenance	100	Not available	$N(87,13)$
FM	Backlog on corrective maintenance	100	Not available	$N(87,13)$
FM	Deluge valve indicator	1.96	Not available	$N(1,0.39)$
FM	Start indicator	0	Not available	$N(0.53,0.19)$
FM	Fire detection functional test	0	Not available	$N(1,0.39)$
ERS	Backlog on preventive maintenance	100	Not available	$N(87,13)$
ERS	Backlog on corrective maintenance	100	Not available	$N(87,13)$
ERS	Drills indicator	118	Not available	$N(83,26)$
ERS	Emergencies indicator	2.16	Not available	$N(1.2,0.45)$
FP	Questionnaire	H	Not applicable	Not applicable
BP	Questionnaire	H	Not applicable	Not applicable
I&D	Backlog on preventive maintenance	0	Not available	$N(87,13)$
I&D	Backlog on corrective maintenance	0	Not available	$N(87,13)$
I&D	Emergency shutdown/blowdown indicator	0	Not available	$N(3,1.1)$
SC	Questionnaire	H	Not applicable	Not applicable
TC	Questionnaire	L	Not applicable	Not applicable
TC	Gas detection indicator	16.67	Not available	$N(1,0.39)$

The data assumed to be available for the IP estimation and for the characterization of the accidental scenarios are listed in **Tab. 6** and **Tab. 7**, respectively, considering *EP* as the example functional unit.

Table 6. IP estimation data for the EP.

Input variable	Input name	Values
X_1	LOPC hole size	$7\ mm$ $22\ mm$ $100\ mm$
X_2	Confinement level	"A"
X_3	Congestion level	0.7
X_4	Wind strength	"5D"
X_5	Type of gas mixture	"Light"

X_6	Release source	"General"
X_7	Ignition source	"All"

Table 7. Accidental scenario characteristics for the EP.

Consequence	**Hole size** $[mm]$	$F_{LOPC,0}\ [\frac{1}{y}]$	$Q_0^{FU}\ \left[\frac{kg}{s}\right]$	**Heat radiation** $I\ \left[\frac{kW}{m^2}\right]$
PF	7	$2.71 \cdot 10^{-2}$	0.6	$\begin{cases} 37.5, & at\ a\ distance\ of\ 5.11\ m \\ 12.5, & at\ a\ distance\ of\ 11.29\ m \\ 7, & at\ a\ distance\ of\ 14.05\ m \\ 5, & at\ a\ distance\ of\ 16.03\ m \\ 3, & at\ a\ distance\ of\ 20.29\ m \end{cases}$
PF	22	$2.40 \cdot 10^{-4}$	59.2	$\begin{cases} 37.5, & at\ a\ distance\ of\ 10.39\ m \\ 12.5, & at\ a\ distance\ of\ 22.34\ m \\ 7, & at\ a\ distance\ of\ 30.11\ m \\ 5, & at\ a\ distance\ of\ 34.92\ m \\ 3, & at\ a\ distance\ of\ 45.21\ m \end{cases}$
PF	100	$1.04 \cdot 10^{-3}$	120.8	$\begin{cases} 37.5, & at\ a\ distance\ of\ 33.2\ m \\ 12.5, & at\ a\ distance\ of\ 44.62\ m \\ 7, & at\ a\ distance\ of\ 58.21\ m \\ 5, & at\ a\ distance\ of\ 72.65\ m \\ 3, & at\ a\ distance\ of\ 94.78\ m \end{cases}$

Finally, to perform the multi-hazard aggregation, the system layout has been discretized into $N_k = 10^4$ coordinates, and, for each coordinate, $M = 10^4$ Monte Carlo trials of the procedure described in Section 2.2.2 have been performed to estimate the aggregated LSIR.

2.4 Results

The framework presented in Section 2.2 has been applied to the case study of Section 2.3. N_F BNs have been defined with the procedure described in Section 2.3. As an example, in **Fig. 8** the BN for the *EP* functional unit is shown, with the CPTs of its safety barriers.

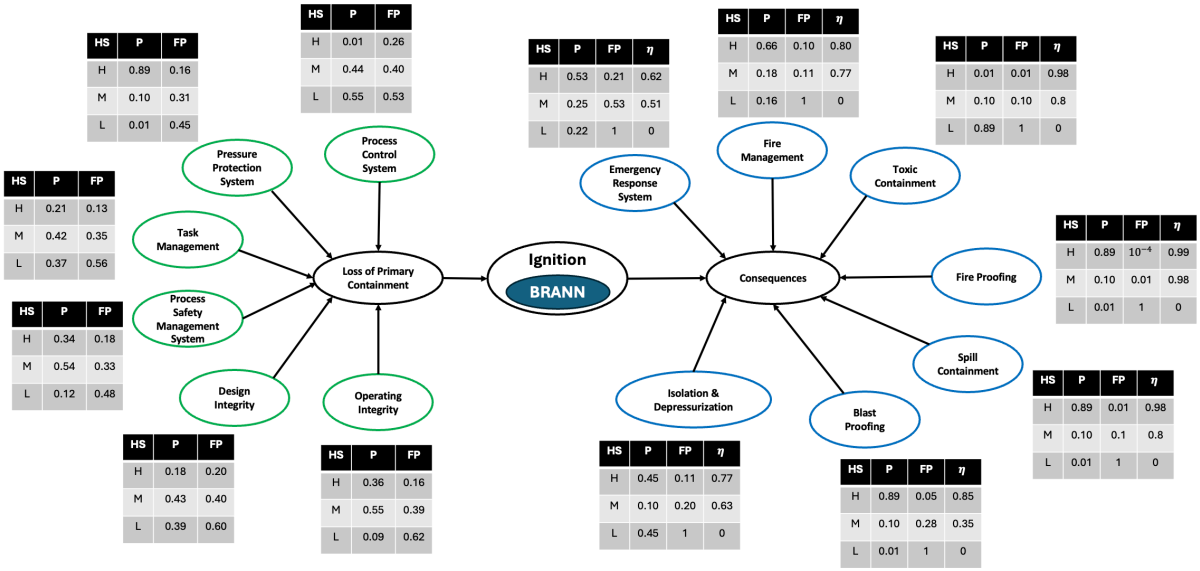


Figure 8. BN of the EP functional unit.

The estimated LSIR is shown in **Fig. 9**, only on a qualitative scale (high, medium, low) due to confidentiality reasons: the area of the plant bearing the largest risk is, as expected, the one with the largest density of functional units. Nevertheless, the LSIR remains within commonly adopted individual risk acceptability criteria (i.e., lower than $4.3 \cdot 10^{-5}$ (Center for Chemical Process Safety, 2009) throughout the plant site. These results allow targeted maintenance planning and/or design improvements to the corresponding functional units.

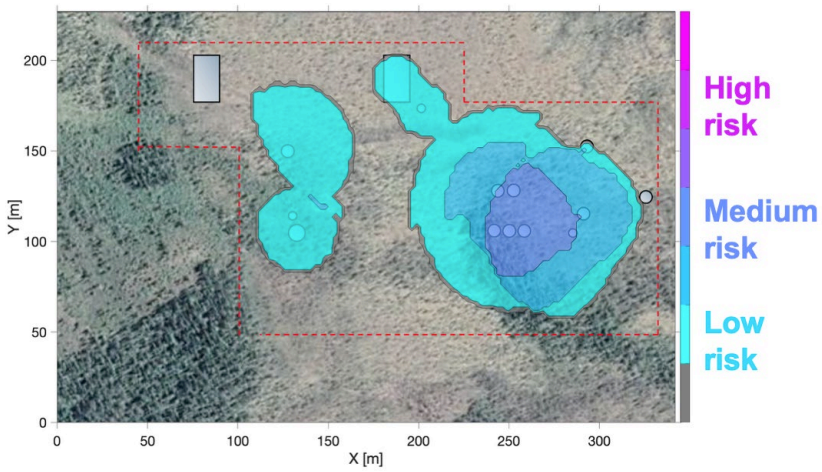


Figure 9. Aggregated LSIR.

For showing the dynamic risk profile updating capability of the proposed framework, let us now assume that new KID about the HS of the safety barriers becomes available once every month, revealing a decrease of the performance of the barriers (that is mapped into a linear decrease of the probabilities of being in states H and M and an increase of the probability of being in state L, over 10 years of operation as shown in **Fig. 10**, without loss of generality, for the OI barrier).

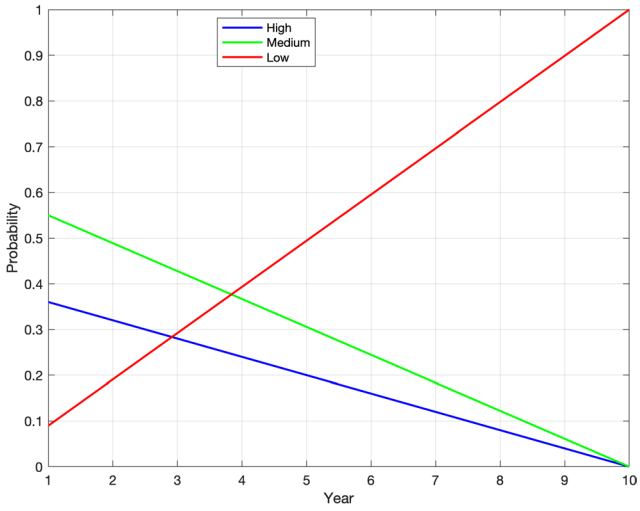


Figure 10. Degradation of the OI safety barrier.

At each month, the CPTs of the BNs would be updated following the procedure described in **Appendix A**, a new aggregated LSIR estimated and plotted, resulting in that shown in **Fig. 11** at 1,4,7 and 10 years of operation. For clarity sake, the evolution of the maximum LSIR throughout the years is plotted in **Fig. 12** (continuous line): it can be seen that it would exceed the acceptability threshold (dashed red line) already after 3 years of operation, which confirms the impact on the risk of the degradation of safety barriers on the LSIR and the importance of relying, within a Safety Management Systems (SMS), on frameworks of analysis that can effectively support dynamic decision making.

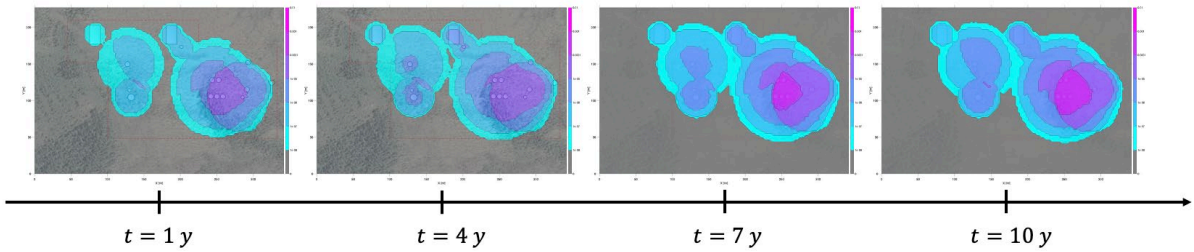


Figure 11. Time evolution of the LSIR.

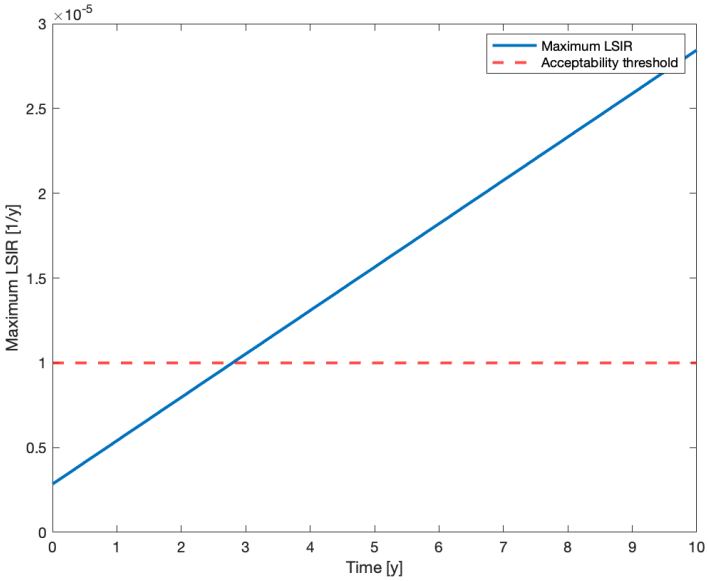


Figure 12. Time evolution of the maximum LSIR.

Chapter 3 Safety barriers maintenance optimization

Contents of this Chapter have been adapted from:

[J1] *S. Marchetti, F. Di Maio and E. Zio, "A Physics-of-Failure (PoF) model-based Dynamic Bayesian Network for considering the aging of safety barriers in the risk assessment of industrial facilities", Journal of Loss Prevention in the Process Industries, Volume 91, 2024. DOI: 10.1016/j.jlp.2024.105402.*

[C3] *S. Marchetti, F. Di Maio and E. Zio, "A Deep Reinforcement Learning method for finding the risk-based optimal prescriptive maintenance policy of degrading safety barriers" International Conference on System Reliability and Safety (ICSRS), 2024.*

3.1 Introduction

Maintenance of safety barriers contrasts their age-related performance degradation for ensuring that the risk remains acceptable throughout the whole life of the system (Pitblado et al., 2016). Maintenance should be optimized to control the risk while keeping the costs as low as possible ((Pinciroli et al., 2023; Yuan et al., 2023)). Existing approaches for safety barriers maintenance optimization concern the optimization of fixed-interval schedules for each barrier ((Han et al., 2022; Yuan et al., 2023; Z. Zeng & Zio, 2018; Zhen et al., 2021)), which is often inefficient (Matyas et al., 2017). Indeed, such approaches do not account for time-dependent degradation processes and might result in inadequate maintenance strategies if the barriers degradation rates change significantly during the system life (e.g., due to worsened operational conditions (Barrelas et al., 2021). To overcome this limitation, we define the problem of finding the optimal safety barriers maintenance policy as a Sequential Decision Problem (SDP) (Hao et al., 2023), in which the goodness of each decision does not depend solely on the goodness of the actual action, but on the whole sequence of actions taken and corresponding plant states resulting from the decided actions, leading to a prescriptive maintenance policy (Pinciroli et al., 2023), which accounts for the potential worsening in time of the operational conditions.

SDPs have been solved by Dynamic Programming (DP) (Howard, 1966), Linear Programming (LP) (Benayoun et al., 1971), Mixed-Integer Linear Programming (MILP) (Floudas & Lin, 2005) and Reinforcement Learning (RL) (Sutton & Barto, 2018). However, DP, LP and MILP all suffer from the curse of dimensionality (De Farias & Van Roy, 2003; Lincoln & Rantzer, 2006), making them not suitable in presence of large action and/or state spaces, which are typical in many real-world applications. RL, on the other hand, has shown promising results in solving such complex SDPs (Gershman & Daw, 2017) and has emerged as a powerful tool in the field of maintenance optimization, as evidenced by several studies in recent literature

(Compare et al., 2020; Hao et al., 2023; Hu et al., 2021; Knowles et al., 2011; Pinciroli et al., 2022; Rocchetta et al., 2019). Within the framework of RL, the behavior of an agent is trained by means of consecutive trial and error interactions with an environment (i.e., the function that models the effects of actions on the system states) to find the optimal policy (Grondman et al., 2012). When the SDP state space and action space are small enough to be represented as a table, tabular RL allows finding the exact solution of SDPs (Sutton & Barto, 2018). However, most practical cases are characterized by high dimensional spaces and/or long decision horizons, leading to unfeasible computational times for tabular RL (Driessens & Matwin, 2004). RL has been used to develop frameworks to optimize the maintenance of power grids (Rocchetta et al., 2019), aircrafts (Hu et al., 2021), sewer networks (Kerkkamp. et al., 2022), production systems (Kuhnle et al., 2019) and gas turbines (Compare et al., 2020). However, the use of RL for the optimization of the maintenance of safety barriers is largely unexplored.

In the case of high dimensional spaces and long time horizons, one can resort to Deep Reinforcement Learning (DRL), which makes use of Deep Neural Networks (DNNs) for finding approximate solutions of SDPs (Arulkumaran et al., 2017). Among the many available DRL implementations, the Proximal Policy Optimization (PPO) algorithm has been chosen in this work due to its ease of implementation and use, its proven ability to outperform many state-of-the-art approaches on several benchmark applications (Schulman et al., 2017) and its success in the field of prescriptive maintenance (Hao et al., 2023; Pinciroli et al., 2022). PPO is an on-policy DRL algorithm belonging to the class of actor-critic methods, in which an actor DNN is trained to learn the optimal policy and a critic DNN is trained to estimate the expected future rewards from the current state (i.e., how promising the current state is) (Sutton et al., 1999). The actor network is updated based on the feedback of the critic to improve the policy, and the critic is updated based on the environment rewards to estimate better the expected returns of a given state. In our case, the environmental reward accounts for both the risk of the system and the cost resulting from the maintenance actions, so that the optimal maintenance policy can minimize both terms. In presence of large state and/or action spaces, however, it can still be difficult for the agent to find the optimal actions starting from a random initialization of the neural network weights (Pinciroli et al., 2022). To tackle this problem, we resort to Imitation Learning (IL) (Hussein et al., 2017), which consists in pre-training the agent with supervised learning to reproduce a state-of-the-art policy. Then, to improve and fine-tune the learnt policy, the agent is trained by DRL using a model of the system as the environment, since training it by direct interaction with the physical system is unfeasible due to safety, economic and time issues (Hao et al., 2023). To model the environment to be used within the SDP, we propose a novel framework to integrate in the traditional fragility models of safety barriers the Physics-of-Failure (PoF) models of their aging (i.e., physical models of the aging processes that lead to their failure (Lemoine & Wenocur, 1985). Since domino effects among the involved SSCs are a main concern for many industrial systems (Abdolhamidzadeh et al., 2011; Cozzani et

al., 2014; Landucci et al., 2016b), the framework has to explicitly model these and their time-dependent impacts. With the traditional risk assessment techniques, such as Event Trees (ETs) (Huang et al., 2001) and Fault Trees (FTs) (Flage et al., 2013), it is difficult to do this. Then, a feasible dynamic model must be developed (such as a Dynamic Flowgraph (DF) (Tripathi et al., 2020), a Multi-Agent Model (MAM) (Kanj et al., 2022), a Multilevel Flow Model (MFM) (Zhu et al., 2018), a Dynamic Event Tree (DET) (J. H. Lee et al., 2020), a Dynamic Event Sequence Diagram (DESD) (Parhizkar et al., 2021)…). In this work, we use Dynamic Bayesian Networks (DBNs) [22], which have been shown successful in various contexts, for example for digital twins development [23], Prognostics and Health Management (PHM) [24], and also for risk assessment [25]. DBNs extend the traditional Bayesian Networks (BNs) to capture temporal dependencies and model dynamic systems. For completeness of the paper, a description of DBNs is provided in **Appendix B**. The graphical structure of the DBN can be, in general, determined by system and process expert analysis or learned from data. The safety barriers feature of interest is the Probability of Failure on Demand (PFD), whose value can be eventually modified by a factor ϕ, to consider the impact of an external event (Misuri et al., 2020). In this work, this factor value is originally derived from the barrier fragility surfaces that are obtained by embedding the PoF models into the barriers fragility models that, ultimately, provide fragility surfaces as functions of both the hazard magnitude and the barrier age. The Conditional Probability Tables (CPTs) for the quantitative DBN models are learned from data using the Expectation Maximization (EM) algorithm (Dempster et al., 1977), where the data is generated by a suitable (but computationally expensive) dynamic model. The DBN is, then, used to calculate the system failure probability under accidental scenarios, and a Probit model is used to assess the severity of the accident. As knowledge and information on the components states and hazards become available during the system life, the DBN is updated to provide estimates of the actual risk profile which the operators can use to decide on the most proper actions to implement for keeping the risk to the desired level.

The proposed method has been tested on a case study of literature (Di Maio, Marchetti, et al., 2023b, 2023a), in which a chemical facility composed by three tanks of flammable substances is exposed to Natural hazard-induced Technological (NaTech) risk due to earthquakes. This is a particularly relevant example because NaTech scenarios are a primary concern in industry due to their significant probability of escalation to severe consequences, which must be mitigated by the action of properly maintained safety barriers. The facility is equipped with different safety barriers (active, passive and procedural): Water Deluge System (WDS), Passive Fire Protection material (PFP), Pressure Safety Valve (PSV), Emergency Team Intervention (ETI) and Foam-Water Sprinkler system (FWS). A Physics-of-Failure (PoF) model-based Dynamic Bayesian Network (DBN) of literature (Marchetti, Di Maio, & Zio, 2024a) is used as the environment for the training of the DRL agent. The performance of the barriers is expressed in terms of their Probability of Failure on Demand (PFD), which is modified, as customary (Misuri et al., 2020; Misuri & Cozzani,

2021), with a performance modification factor ϕ to account for the impact of earthquakes. For each i-th safety barrier, a fragility surface is tailored to calculate ϕ_i, accounting for the age-dependent fragility of the barriers to the natural hazard (i.e., the earthquake). The prescriptive maintenance policy found by the DRL is compared to fixed-interval maintenance schedules of literature (Guojin et al., 2021; Linder et al., 2002; Marchetti, Di Maio, & Zio, 2024c); the results of the comparison show that DRL performs better both in terms of cost and risk minimization, while being able to adapt to changes in degradation rates during the system lifetime because of changing operational conditions.

3.2 The proposed PoF-based modelling framework

The proposed PoF-based modelling framework for accounting for the aging of safety barriers of a system exposed to an extreme natural event is structured in the following steps (**Fig. 13**). With reference to a generic risk update time t:

1) Characterize:
    a. the natural hazard, by the magnitude-frequency curve;
    b. the system, by defining its physical properties;
    c. the safety barriers performance, by age-dependent fragility surfaces;
2) Define:
    a. the structure of the DBN;
    b. the CPTs of the DBN;
3) Calculate the system failure probability and the severity of the accidental scenarios, to obtain the Location Specific Individual Risk (LSIR): if safety limits are not respected, take decisions to implement suitable actions and return to 1);
4) As the system is operating for a time Δt, new information on the hazard is collected and knowledge on the system state is gained, so return to 1) to update the model and the assessment.

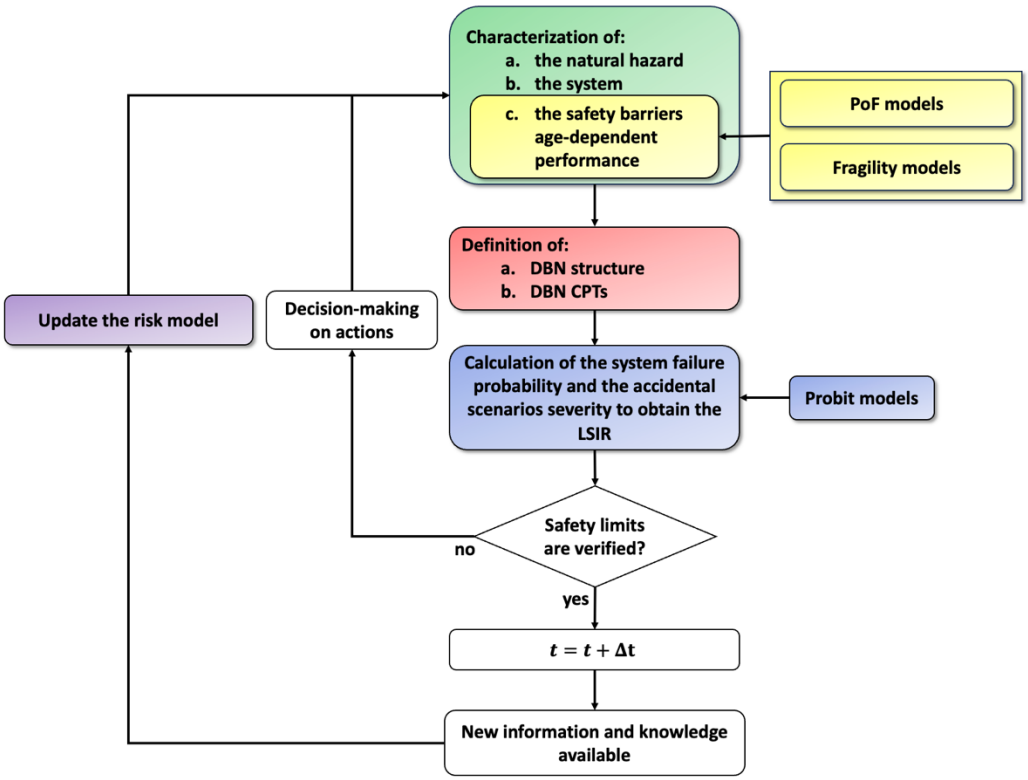


Figure 13. The proposed PoF-based framework.

3.2.1 Hazard and system characterization

The natural hazard is characterized by the magnitude-frequency curve, based on historical data. The system is characterized in relation to its physical properties, layout and the relevant subsystems and components.

The $i = 1,2,\dots,N$ safety barriers in the system are characterized by their specific nominal PFD ($PFD_{0,i}$) and the modified PFD_i considering the modification factor ϕ_i, to account for the impact of the natural event, as follows (Di Maio, Marchetti, et al., 2023b):

- Active and procedural barriers:

$$PFD_i = 1 - (1 - \phi_i)\left(1 - PFD_{0,i}\right) \tag{14}$$

- Passive barriers:

$$PFD_i = \phi_i \tag{15}$$

The modification factor ϕ_i represents the timed contribution of the natural event to the fragility of the barriers. With respect to this, safety barriers can be divided into three different categories:

1. Safety barriers that are unaffected by the natural event ($\phi_i = 0$).

2. Safety barriers that are affected by the natural event irrespectively of their age ($\phi_i = f(M)$): the fragility of these barriers can, thus, be expressed by custom fragility curves.

3. Safety barriers for which the impact of the natural event is affected by their age ($\phi_i = f(t, M)$: the fragility of these barriers, thus, requires the definition of tailored fragility surfaces, for which it is necessary:

- a PoF model, which describes how the barrier degrades in time and how such degradation can eventually lead to failure;
- a fragility model, which describes how the failure probability of the barrier changes with the natural event magnitude.

To integrate the PoF and the fragility models that define the fragility surface, the result of the PoF model (i.e., the degradation state of the barrier, expressed in terms of a suitable physical damage parameter $D_i(t)$ is used as input to the fragility model used to assess $\phi_i(t, M)$. As an illustrative example, let us consider, without loss of generality, the assessment of the fragility of a fire sprinkler system to an earthquake: in a nutshell, the system may fail if the seismic demand (function of the earthquake magnitude) exceeds the sprinkler seismic resistance capacity (X. Liu et al., 2021); as the sprinkler system ages, its pipes may suffer of pitting corrosion (Van Der Schijff & Bodemann, n.d.), resulting in thinner pipe walls and lower yield and ultimate strengths, thus lowering the seismic resistance capacity and increasing the failure probability. To describe this, a pipe corrosion model must be integrated into the fragility model, to calculate the pipe wall thickness as a function of the sprinkler age. In case of unavailability of the PoF model for one or more safety barriers, the corresponding fragility surfaces cannot be built, and traditional fragility curves must be used.

3.2.2 DBN definition

The second step of the framework concerns the definition of the DBN for the calculation of the system failure probability. Constructing a DBN involves two main steps (Kenneth Kitson et al., 2022):

- defining the DBN graphical structure;
- determining the CPTs of the DBN nodes (i.e., the DBN parameters).

The graphical structure can either be defined by expert knowledge or learned from data.

DBN parameters can be determined by expert elicitation, data-driven learning, or a combination of the two (Neapolitan, 2004). Since eliciting DBN parameters from experts can be a difficult procedure (Neapolitan, 2004), especially in case of large networks, in this work the EM algorithm (Dempster et al., 1977; Romaric et al., 2016) is used to learn the DBN parameters from data. For this, the uncertain inputs and parameters of the dynamic model used (e.g., the natural event magnitude, the safety barriers response times, the environmental conditions…) are sampled from their probability distributions and given to the model to generate N_S accidental sequences;

these are split into a training dataset (with N_{train} samples) to be used for the parameter learning, and a validation dataset (with N_{val} samples) to be used for validation; the Mean Squared Error (MSE) between the DBN prediction of the failure probability (P_f) and the true value (P_f^*) is taken as the validation metric.

3.2.3 System failure probability and accidental scenarios severity calculation

The third step of the framework aims at quantifying the system failure probability and the severity of the accidental scenario at the current system age t during the life of the system, to eventually obtain the LSIR. The system failure probability at any system age can be calculated using the DBN described in Section 3.2.2, whereas the severity using a suitable Probit model that provides the dose-effect relation for human responses to toxic substances, thermal radiation and overpressure (Cozzani & Salzano, 2004). The obtained quantities are used to obtain the LSIR of the system, which is compared against predefined safety limits to determine risk acceptability. In case of exceedance of the acceptable risk limits, various actions can be taken in the different stages of the system life (e.g., re-designing safety barriers, optimizing maintenance schedules…).

3.2.4 Updating risk assessment

After operating the system for a time Δt, the new information acquired on the natural event occurrence frequency and/or the new knowledge of the components states degradation are used to update the risk assessment model and its outcomes are verified to ensure that the risk is still acceptable.

3.3 Sequential Decision problem formulation and Reinforcement Learning algorithm definition

The barriers degradation state D_i is assumed to be a continuous variable and its value known at each decision time t, either by inspection or by sensor measurements. Without loss of generality, maintenance of the barriers is considered perfect, i.e., the barrier is restored As Good As New (AGAN) when maintained, and is performed by only one maintenance crew (i.e., only one safety barrier can be maintained at each decision time).

In this context, the SDP can be defined by the set $S, A, P, r, \gamma,$ where:

- S is the state space (i.e., the set of all possible system states, where each state is a vector of variables that fully describes the state of the system);
- A is the action space (i.e., the set of possible maintenance actions);
- P is the set of transition probabilities (i.e., $p(\boldsymbol{s}'|\boldsymbol{s}, \boldsymbol{a}) \in P$ is the probability to make a transition from state $\boldsymbol{s}$ to state $\boldsymbol{s}'$ when an action $\boldsymbol{a}$ is performed);

- r is the reward function (i.e., $r(\boldsymbol{s}'|\boldsymbol{s},\boldsymbol{a})$ is the reward corresponding to the state change from $\boldsymbol{s}$ to $\boldsymbol{s}'$ because of $\boldsymbol{a}$);
- $\gamma \in [0,1]$ is the discount factor, which is used to evaluate the present value of future rewards.

Furthermore, a set of constraints on the budget and/or the risk can be integrated into the SDP, if needed (as we shall see in Section 3.3.4). The SDP aims at finding the optimal maintenance policy $\pi^*(\boldsymbol{a},\boldsymbol{s})$, which determines, for each state $\boldsymbol{s}$, the sequence of actions $\boldsymbol{a}$ to be adopted at each decision time t to maximize the reward (i.e., to minimize both maintenance cost and risk) over the mission time T_M.

3.3.1 The state space

Each state $\boldsymbol{s} \in S$ must contain all the information needed for the agent to make a decision. In our case, at each decision time t the state is characterized by the vector $\boldsymbol{s}_t = [\boldsymbol{D}, T] \in \mathbb{R}^{N+1}$, obtained appending the actual age of the system (i.e., T) to the vector containing the degradation state of the safety barriers (i.e., $\boldsymbol{D}$).

3.3.2 The action space

The maintenance actions are defined at each decision time t by vector $\boldsymbol{a}_t = [a_1, a_2, \dots, a_N]$, in which $a_i = 1$ if the *i-th* safety barrier is maintained, leading to $\boldsymbol{a}_t = [0, \dots, 0, a_i = 1, 0, \dots, 0]$. If no maintenance is performed $\boldsymbol{a}_t = [0, \dots, 0]$.

3.3.3 The transition probabilities and the environment model

The optimal policy could be learned by direct interaction with the physical system. However, in case of industrial systems, such training is unfeasible due to economic, safety and time issues, since at the beginning of the agent training, the maintenance actions would be suboptimal and the system would be exposed to a larger risk of severe consequences in case of an accidental scenario. Therefore, a virtual environment (e.g., a physical model (Hao et al., 2023), a Bayesian Network (BN)…) is needed to model the system transitions caused by the execution of the agent actions and their effects on the system, as we shall see in Section 3.4.3, for the model of the case study.

3.3.4 The reward function

At each decision time t, the decision maker (i.e., the agent) receives a reward r_t, which is defined by:

$$r_t(\boldsymbol{s}'|\boldsymbol{s},\boldsymbol{a}_w) = L(\boldsymbol{s}) - L(\boldsymbol{s}') - \langle \boldsymbol{C}, \boldsymbol{a}_t \rangle \quad (16)$$

where $L(\boldsymbol{s})$ and $L(\boldsymbol{s}')$ are the expected economical losses due to accidents occurring before or after the action $\boldsymbol{a}_t$ is performed, respectively, $\boldsymbol{C} = [C_1, \dots, C_N]$ is the vector of the cost of the maintenance actions, and the operator $\langle \cdot \rangle$ is the dot product. When, as in most practical cases, the maintenance cost at time t must comply with the available

budget C_B, a penalty coefficient λ_c is introduced to modify the reward r_t (Calvo-Fullana et al., 2021):

$$r_t^c = r_t - \lambda_c \cdot \min[0, (C_B - C_t)] \tag{17}$$

To avoid preferring economic savings (i.e., risk-prone policies) to safety compliance (i.e., risk-adverse policies), a trade-off reward is required. Considering $m = 1, \dots, M$ risk metrics σ_m, the trade-off reward is expressed by Eq. (18) (Calvo-Fullana et al., 2021):

$$r_t^{c,R} = r_t^c - \sum_{m=1}^{M} \lambda_m \cdot \min\left[0, \left(\sigma_{m,t} - \sigma_m^*\right)\right] \tag{18}$$

where λ_m is the penalty term associated with the risk metric σ_m, the parameter σ_m^* is the considered threshold and $\sigma_{m,t}$ is the value of σ_m at decision time t. The selection of the values of λ_m and σ_m^* allows modelling different risk attitudes of the decision maker.

3.3.5 Reinforcement Learning algorithm

In general, RL algorithms can be classified in three groups: policy search, value function and actor-critic (Konda & Tsitsiklis, 1999), with the following characteristics:

1. Policy search (i.e., actor-only) methods work with a parameterized policy $\pi(\boldsymbol{a}|\boldsymbol{s};\boldsymbol{\theta})$ and aim at finding the optimal policy $\pi^*(\boldsymbol{a}|\boldsymbol{s})$ by updating the parameters $\boldsymbol{\theta}$ (Jaakkola et al., 1994). The drawbacks of these methods are the large variance of the gradient estimators (Konda & Tsitsiklis, 1999), the independence of each gradient estimation from past estimates, and the typical convergence to a local optimum rather than to a global one (Grondman et al., 2012).

2. Value function (i.e., critic-only) methods rely exclusively on value function approximation and aim at learning an approximate solution $Q^\pi(\boldsymbol{s}, \boldsymbol{a})$ of the Bellman equation (Bellman, 1952), which represent the expected future rewards obtained performing action $\boldsymbol{a}$ in state $\boldsymbol{s}$. Such methods may construct a satisfactory approximation of the value function, but they lack reliable guarantees for the optimality of the resulting policy (Konda & Tsitsiklis, 1999).

3. Actor-critic methods aim at combining the advantages of actor-only and critic-only methods (Grondman et al., 2012). These methods learn both the policy (through an actor model) and the value function (through a critic model). The actor is updated based on the feedback of the critic to improve the policy, and the critic is updated based on the environment rewards to estimate better the value function.

In this work, the actor-critic DRL algorithm PPO is used, which utilizes two DNNs as the actor and the critic (Schulman et al., 2017). The novelty of this approach is the

introduction of a surrogate clipped objective to be maximized, for disincentivizing too large policy updates so as to avoid accidental performance collapse and leading to an improved stability and convergence of the training process (more details about PPO can be found in **Appendix B**). PPO is considered relatively easy to implement and use, and has been shown to outperform many state-of-the-art approaches on several benchmark applications (Schulman et al., 2017). A schematic view of the PPO implementation used in this work is provided in **Fig. 14**. At each decision time t, both the actor and the critic receive the representation of the environment state $\boldsymbol{s}_t$ (i.e., the degradation state of the safety barriers and the age of the system). The actor, then, selects the action $\boldsymbol{a}_t$, which corresponds to the maintenance decision to be taken, and the environment model simulates the system response when the selected maintenance action is enforced, moves to the new state $\boldsymbol{s}_{t+1}$ and returns a reward r_t. Then, the critic is updated using r_t and the actor is updated using both r_t and the feedback of the critic. By iteratively repeating this procedure, the critic learns to accurately estimate the value function, and the actor reaches the optimal policy $\pi^*(\boldsymbol{a}|\boldsymbol{s})$ which links each possible state $\boldsymbol{s}$ with the action $\boldsymbol{a}$ that maximizes the expected cumulative sum of rewards over the time horizon $\mathbb{E}\left[\sum_{t=0}^{T_M} \gamma^t \cdot r_t(\boldsymbol{a}_t, \boldsymbol{s}_t, \boldsymbol{s}_{t+1})\right]$.

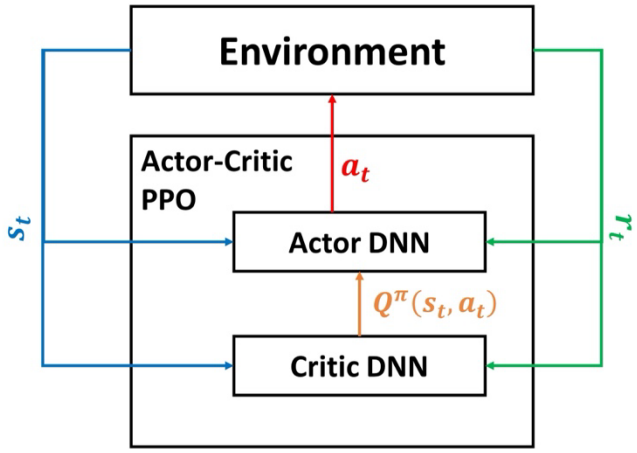


Figure 14. Schematic representation of the PPO algorithm.

Since in many applications the state space and/or the action space are very large, it may be difficult for the agent to discover the optimal policy starting from a random initialization of the DNN weights. Therefore, in this work we resort to IL to pre-train the agent with supervised learning to reproduce a state-of-the-art policy. IL is a powerful approach in scenarios with large state spaces, since it provides a practical starting point for agents to learn, reducing the initial exploration complexity and directioning the learning process (Okumura et al., 2020).

3.4 Case study

The case study regards a chemical facility of literature (Misuri et al., 2021b) composed of two atmospheric tanks (T1 and T2) that store liquid flammable substances and one pressurized vessel (P1) that contains liquid petroleum gas (**Fig. 15**). The design life is

50 years (National Research Council (US), 1999). Following (Center for Chemical Process Safety, 2009), the acceptable LSIR threshold for the considered facility is $LSIR_{max} = 4.3 \cdot 10^{-5} \frac{fatality}{year}$.

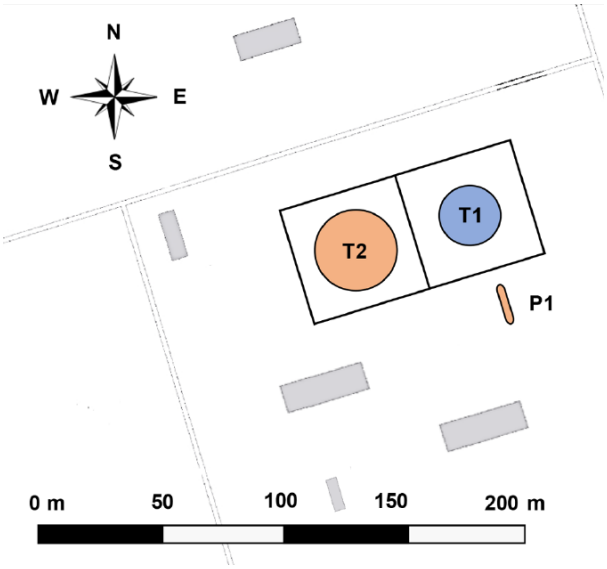


Figure 15. Layout of the chemical facility.

3.4.1 Hazard and system characterization

The Initiating Event (IE) considered is the occurrence of earthquake with Peak Ground Acceleration (PGA) $PGA \in [1, 9.81] \frac{m}{s^2}$. The magnitude-frequency curve is taken from (J. P. Wang et al., 2012) and shown in **Fig. X**.

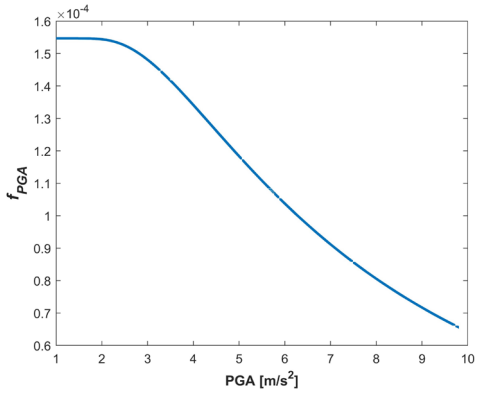


Figure 16. Earthquake magnitude-frequency curve.

For illustrative purposes we assume that when one of the tanks fails it always leads to a pool fire (in case of T1 and T2) or to a jet fire (in case of P1), with a Time of Final Mitigation (TFM) of 150 min in both cases, which is the time needed for the accident to reach a safe state after implementing all the necessary mitigation actions (Di Maio, Marchetti, et al., 2023b).

The physical properties of the three tanks are reported in **Tab. 8**.

Table 8. Physical properties of the tanks.

Tank	Volume	Thickness	Diameter	Specific Heat	Density	Storage Mass	Op. Pressure	Yield Strength
T1	$5000\ m^3$	$0.01\ m$	$24.4\ m$	$0.5\frac{kJ}{kg \cdot K}$	$7900\frac{kg}{m^3}$	$3000\ ton$	$1\ bar$	$235\ MPa$
T2	$4300\ m^3$	$0.01\ m$	$32\ m$	$0.5\frac{kJ}{kg \cdot K}$	$7900\frac{kg}{m^3}$	$3000\ ton$	$1\ bar$	$235\ MPa$
P1	$105\ m^3$	$0.007\ m$	$2.6\ m$	$0.5\frac{kJ}{kg \cdot K}$	$7900\frac{kg}{m^3}$	$52\ ton$	$8.34\ bar$	$235\ MPa$

The safety barriers designed to protect T1, T2 and P1 (Misuri et al., 2021b) are listed in **Tab. 9**. Among these, WDS, FWS and PSV are active, PFP is passive and ETI is a procedural barrier.

Table 9. Safety barriers configuration.

Safety Barrier	Classification	T1	T2	P1	Description
Water deluge system (WDS)	Active			X	Water delivery during fire
Passive fire protection material (PFP)	Passive			X	Coating fireproof material
Pressure safety valve (PSV)	Active	X	X	X	Valve designed to relieve excess pressure
Emergency team intervention (ETI)	Procedural	X	X	X	Emergency firefighter team intervention
Foam-Water Sprinkler system (FWS)	Active	X	X		Foam delivery during fire

For the considered safety barriers, the base values of the Probability of Failure on Demand $PFD_{0,i}$, the intervals of the uncertain response times $t_{r,i}$ (defined as the time between the detection of the hazard and the activation of the safety barrier, here assumed to follow a uniform distribution), the scheduled times between two successive maintenance interventions $\Delta t_{m,i}$ and the maintenance cost are reported in **Tab.10**, for all barriers, $i = 1, \dots, 5$.

Table 10. Safety barriers characterization.

Safety barrier	$PFD_{0,i}$	$t_{r,i}$ (Di Maio, Marchetti, et al., 2023b)	$\Delta t_{m,i}$	Maintenance cost
WDS	0.0433	$t_{r,WDS} \in [182, 272]$ s	3 months (Linder et al., 2002)	10^3 € (Yuan et al., 2023)
PFP	-	$t_{r,PFP} = 0$	15 years (Marchetti, Di Maio, & Zio, 2024a)	$6 \cdot 10^4$ € (Di Maio, Marchetti, et al., 2023b)
PSV	0.01	$t_{r,PSV} \in [5.9, 7.8]$ ms	1 year (Guojin et al., 2021)	500 € (Xing et al., 2020)
ETI	0.1	$t_{r,ETI} \in [420, 1020]$ s	-	-
FWS	0.0053	$t_{r,FWS} \in [182, 272]$ s	3 months (Linder et al., 2002)	$1.5 \cdot 10^3$ € (Yuan et al., 2023)

It is proper to specify that $\Delta t_{m,i}$ for $i = 1,3,5$, (WDS, PSV and FWS, respectively) is the time between two inspections (during which maintenance may be enforced),

whereas for $i = 2$ (PFP) it is the time between replacements, and that no maintenance is foreseen for $i = 4$ (ETI), since it is assumed to be maintained by the local government.

The PoF-based safety barriers fragility characterization is based on the following considerations:

- WDS and FWS degradation is due to pitting corrosion (Van Der Schijff & Bodemann, n.d.), which leads to thinner pipe walls and to a larger seismic fragility, with $\phi_{WDS/FWS} = f(t, PGA)$. To obtain the fragility surface, first the experimental data from (Van Der Schijff & Bodemann, n.d.) have been used to calculate the corrosion rate $C_r(t)$ (**Tab. 11**), then the seismic fragility has been calculated as follows (X. Liu et al., 2021):

$$\phi_{WDS/FWS}(t, PGA) = \varphi\left[\frac{\ln\left(m_{D|PGA}\right) - \ln\left(m_c(t)\right)}{\sqrt{\beta^2_{D|PGA} + 0.1025}}\right] \tag{19}$$

where $\varphi[\cdot]$ is the standard normal Cumulative Distribution Function (CDF), $\ln\left(m_{D|PGA}\right) = 0.9724 \cdot PGA + 5.4554$ is the logarithmic median seismic demand, $m_c(t) = 1 - 0.879 \cdot C_r(t) \cdot t$ is the sprinkler system seismic capacity and $\beta_{D|PGA} = 0.3535$ is the logarithmic standard deviation of the seismic demand. The fragility surface is reported in **Fig. 17**.

Table 11. Sprinkler corrosion rates.

Exposure time t_e $[days]$	**Corrosion rate C_r $[mm/y]$**
$t_e \leq 497$	0.52
$497 < t_e \leq 759$	0.52
$759 < t_e \leq 780$	0.42
$780 < t_e \leq 1116$	0.43
$1116 < t_e \leq 7300$	0.42

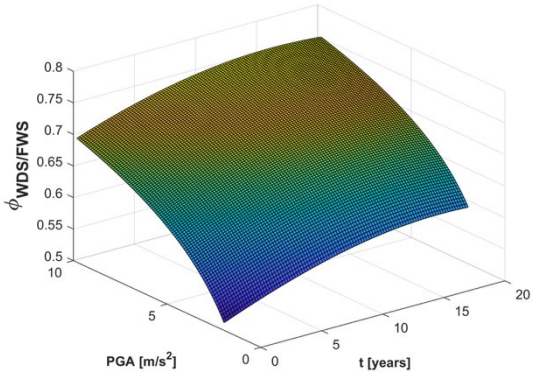


Figure 17. WDS and FWS fragility surface.

- PFP degradation is due to atmospheric conditions and leads to a lower tensile strength σ_s (J. Wang & Zhao, 2020), ultimately causing a larger seismic fragility, with $\phi_{PFP} = f(t, PGA)$. To obtain the fragility surface, the experimental data obtained using accelerated weathering in (J. Wang & Zhao, 2020) have been interpolated to find the relationship between tensile strength σ_s and aging: since it typically takes around 30 years of natural weathering for PFP to reach ineffective fireproofing (Maciulaitis et al., 2018), whereas it took 600 hours of accelerated weathering, it is concluded that one hour of accelerated weathering corresponds to 18 days and 6 hours of natural weathering; this allows us to relate t and σ_s as summarized in **Tab. 12** and plotted in **Fig. 18**.

Table 12. PFP tensile strength.

$\boldsymbol{t}$ $[\boldsymbol{y}]$	**Tensile Strength** $\boldsymbol{\sigma_s}$ $[\boldsymbol{MPa}]$
0	0.70
6	1.03
12	0.68
24	0.59
30	0.30

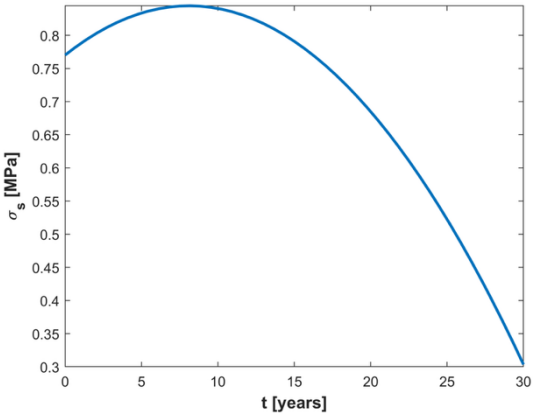


Figure 18. Tensile strength as a function of PFP age.

The tensile stress σ_T, on the other hand, has been calculated as described in (Meier, 2020):

- calculate the hydrostatic force:

$$N_h = \rho_c g h S_c \tag{20}$$

where $\rho_c = 0.493 \frac{kg}{m^3}$ is the density of the tank content, $g = 9.81 \frac{m}{s^2}$ is the gravitational acceleration, $h = 4\ m$ is the content level and $S_c = 22\ m^2$ is the tank cross section

;

- calculate the impulsive hoop force:

$$N_i = 5.54 A_i g D^2 \tag{21}$$

where $A_i = 0.07$ is the impulsive spectral acceleration parameter and $D = 2.625\ m$ is the tank diameter.

- calculate the convective hoop force:

$$N_c(PGA) = \frac{33.1 A_c C_c PGA g D^2 \cosh\left[\frac{3.68(H-Y)}{D}\right]}{\cosh\left[\frac{3.68H}{D}\right]} \tag{22}$$

where $A_c = 0.07$ is the convective spectral acceleration parameter, $C_c = 7$ is the tank convective parameter, $H = 5\ m$ is the height of the tank and $Y = 1\ m$ is the distance between the content level and the top of the tank.

- calculate the tensile stress:

$$\sigma_T(PGA) = \frac{N_h + \sqrt{N_i^2 + N_c^2(PGA)}}{s_T} \tag{23}$$

where $s_T = 0.0324\ m$ is the sum of the thicknesses of the tank and of PFP.

Finally, the PoF-based fragility is calculated as follows:

$$\phi_{PFP}(t, PGA) = \begin{cases} 1 - \dfrac{\sigma_s(t) - \sigma_T(PGA)}{\sigma_s(t)} & if\ \sigma_s(t) \geq \sigma_T(PGA) \\ 1 & if\ \sigma_s(t) < \sigma_T(PGA) \end{cases} \quad (24)$$

and the corresponding fragility surface is plotted in **Fig. 19**.

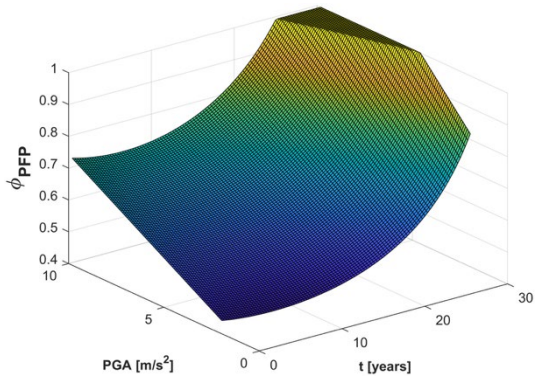


Figure 19. PFP fragility surface.

- The impact of the earthquake on PSV can be neglected as explained in previous studies (Di Maio, Marchetti, et al., 2023a, 2023b; Misuri et al., 2020, 2021), with $\phi_{PSV} = 0$. Therefore, no fragility curve (or surface) is needed, though PSV degradation is modelled as described in (Laskowska & Vatn, 2019) with the Markov model shown in **Fig. 20** and the associated transition rates and PFDs presented in **Tab. 13**.

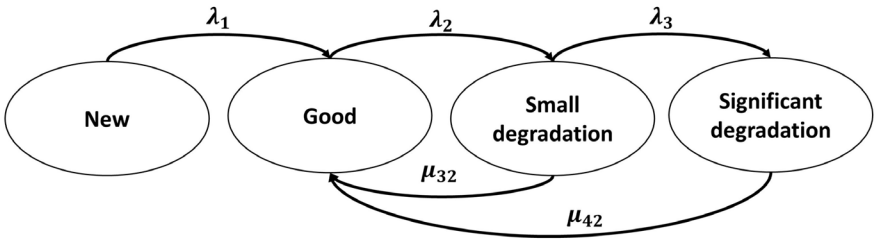


Figure 20. PSV Markov degradation model.

Table 13. PSV transition rates.

State	Transition rate $[h^{-1}]$	PFD_{PSV}
New	$\lambda_1 = 10^{-4}$	$PFD_{PSV,1} = 4.3 \cdot 10^{-4}$
Good	$\lambda_2 = 10^{-4}$	$PFD_{PSV,2} = 1.97 \cdot 10^{-2}$

Small degradation	$\lambda_3 = 3.4 \cdot 10^{-3}$ $\mu_{32} = 0.1250$	$PFD_{PSV,3} = 0.598$
Significant degradation	$\mu_{42} = 0.0268$	$PFD_{PSV,3} = 0.813$

- The unavailability of ETI due to the earthquake is caused by damage to the roads leading to the site. As already said, it is assumed that their fragility does not increase with aging, with $\phi_{ETI} = f(PGA)$ because we assume that roads are properly maintained by the local government, leading to the fragility curve of **Fig. 21** (D. Wang et al., 2021).

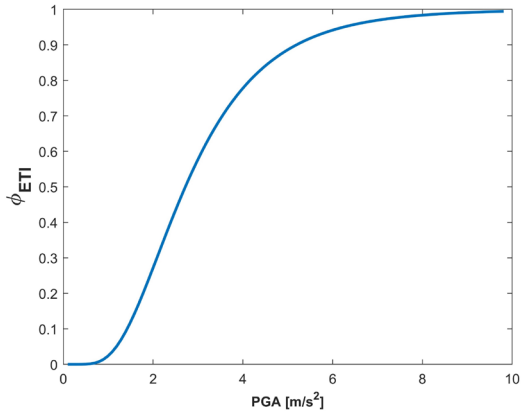


Figure 21. ETI fragility curve.

Finally, to calculate the probability of failure of T1, T2 and P1 due to the impact of the earthquake ($P_{f_j}^0$ with $j = T1, T2$ and $P1$, respectively) as a function of both the PGA and their age, the fragility is calculated as follows (Nie et al., 2011):

$$\phi_j(t, PGA) = \varphi\left[\frac{\log\frac{PGA}{g\sigma_{c,j}(t)}}{0.336}\right] \tag{25}$$

where $\sigma_{c,j}(t)$ is the tank seismic capacity whose values are obtained from the data of **Tab 14** by linear interpolation.

Table 14. Values of σ_c (Nie et al., 2011).

t [y]	$\sigma_{c,T1/T2}(t)$ [MPa]	$\sigma_{c,P1}(t)$ [MPa]
0	0.426	0.426
5	0.426	0.409
10	0.426	0.393
15	0.426	0.376
20	0.426	0.350
25	0.424	0.343

30	0.416	0.326
35	0.399	0.310
40	0.371	0.294
45	0.330	0.278
50	0.240	0.218

The fragility surfaces of **Fig. 22** are, then, obtained.

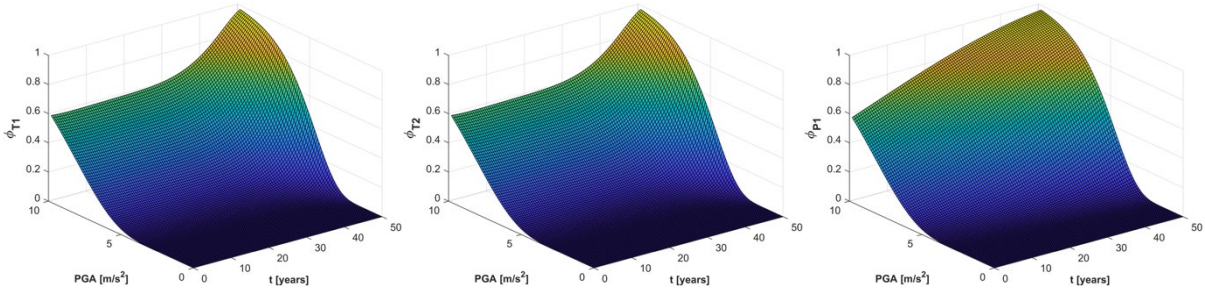


Figure 22. T1 (left), T2 (center) and P1 (right) fragility curves.

As shown in **Fig. 22**, for fixed large values of the PGA, T1 and T2 show a constant fragility value for the first $20\ y$ of age, whereas P1 undergoes a faster degradation, since its fragility early increases. As an example, fixing $PGA = 7\frac{m}{s^2}$, T1 and T2 reach a fragility value of 0.8 after $40\ y$ of aging, whereas P1 reaches the same value only after $20\ y$.

3.4.2 DBN definition

The expert-defined DBN developed to model the phenomena occurring in the facility of **Fig. 15** is shown in **Fig. 23**: continuous lines are static arcs (i.e., conditional dependencies among nodes at the same time step) whereas dashed lines are temporal arcs (i.e., conditional dependencies among nodes at different time steps); the nodes are:

- Root nodes (i.e., nodes with no parent nodes):
  - *System Age*: discrete node with 51 states (from 0 to 50, one for each of the 50 years of the facility lifetime).
  - *Earthquake PGA*: continuous node that describes the magnitude of the earthquake triggering the NaTech scenarios according to the magnitude-frequency curve of **Fig. 16**.
  - *Maintenance on PSV*, *Maintenance on PFP*, *Maintenance on FWS* and *Maintenance on WDS*: continuous nodes that model $\Delta t_{M,i}$.
- Intermediate nodes (i.e., nodes with at least one parent node and one child node):

- *T1*, *T2* and *P1*: binary nodes modelling the tanks states, namely “Safe” or “On Fire”.
- *T1’*, *T2’* and *P1’*: continuous nodes modelling the heat radiation emitted by T1, T2 and P1 (i.e., h_{T1}, h_{T2} and h_{P1}, respectively).
- *WDS*, *FWS*, *PFP*, *ETI* and *PSV*: binary nodes modelling the safety barriers states, namely “Working” or “Failed”. The sprinkler systems (WDS and FWS) are connected to the tank nodes, since they activate when the corresponding tank node is in the state “on fire”, and to the heat radiation nodes, since they mitigate the heat radiation emitted by the tanks. Conversely, PFP and PSV are connected only to the tank nodes, since they only prevent their respective tank to fail, without reducing the emitted heat radiation if it were to fail.

- Terminal nodes (i.e., nodes with no child nodes):
  - *Domino effect*: discrete node with four states (i.e., D_0, D_1, D_2, D_3) that model the four possible domino scenarios (i.e., no tanks failed, one tank failed, two tanks failed, and three tanks failed, respectively).

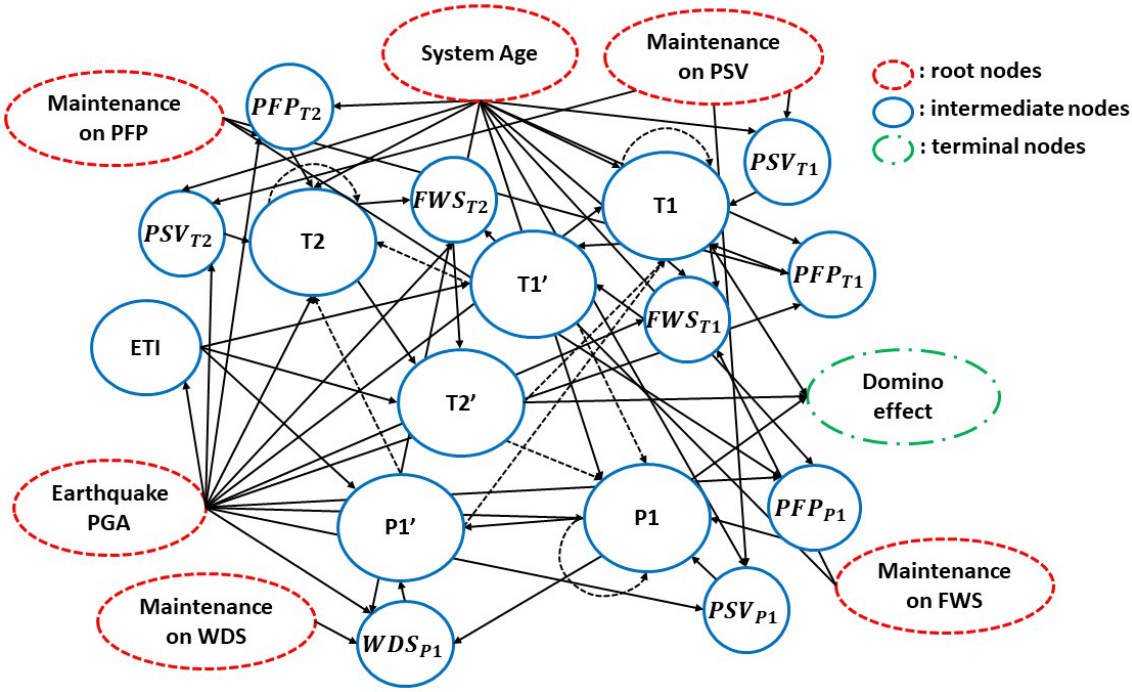


Figure 23. DBN structure.

The accidental scenario triggered by an event occurring in the node *Earthquake PGA* starts at $\tau = 0\,min$ and lasts until $\tau = TFM = 150\,min$. The accidental scenario evolution is discretized within the DBN using a time step $d\tau = 1\,min$, leading to $N_\tau = 151$ time steps.

The CPTs of the DBN nodes (except for *System Age, Maintenance on PSV*, *Maintenance on PFP*, *Maintenance on FWS* and *Maintenance on WDS*, whose states

are to be set manually) are learned from a database of $N_S = 10^5$ simulations run on a phenomenological dynamic model of literature (Di Maio, Marchetti, et al., 2023b) (sketched in the flowchart of **Fig. 24**), where the uncertain variables (i.e., PGA, t_r and W) have been sampled, respectively, from the magnitude-frequency curve of **Fig. 16**, the uniform distributions characterized in **Tab. 10** and the following Weibull distribution:

$$f_W(w) = \frac{k}{\alpha}\left(\frac{w-\mu}{\alpha}\right)^{k-1} \exp\left[-\left(\frac{x-\mu}{\alpha}\right)^{k}\right] \tag{26}$$

where $\alpha = 2.83$, $k = 1.49$ and $\mu = -0.12$ (H. Shi et al., 2021). The dataset of 10^5 samples is split into a training dataset of $N_{train} = 9 \cdot 10^4$ samples and a validation dataset of $N_{val} = 10^4$ samples, where the former is used for learning the DBN CPTs and the latter is used for validating the goodness of the training process. The learning of the CPTs is performed using the EM algorithm embedded in the Genie software (*GeNie*, n.d.). Then, the MSE between the probability of failure of T1, T2 and P1 predicted by the DBN ($P_{f_{T1}}, P_{f_{T2}}$and $P_{f_{P1}}$, respectively), which correspond to the probabilities of the state "On Fire" of their respective nodes, and the true values from the validation dataset ($P^*_{f_{T1}}, P^*_{f_{T2}}$and $P^*_{f_{P1}}$, respectively) is used as validation metric, and is calculated as follows:

$$MSE_j = \frac{1}{N_{val}} \sum_{v=1}^{N_{val}} \left(P_{f_j} - P^*_{f_j}\right)^2 \tag{27}$$

The low value of the average MSE (**Tab. 15**) confirms the goodness of the developed metamodel.

Table 15. Results of the validation of the DBN training.

Tank	MSE
T1	$2.6 \cdot 10^{-4}$
T2	$2.7 \cdot 10^{-4}$
P1	$2.1 \cdot 10^{-4}$

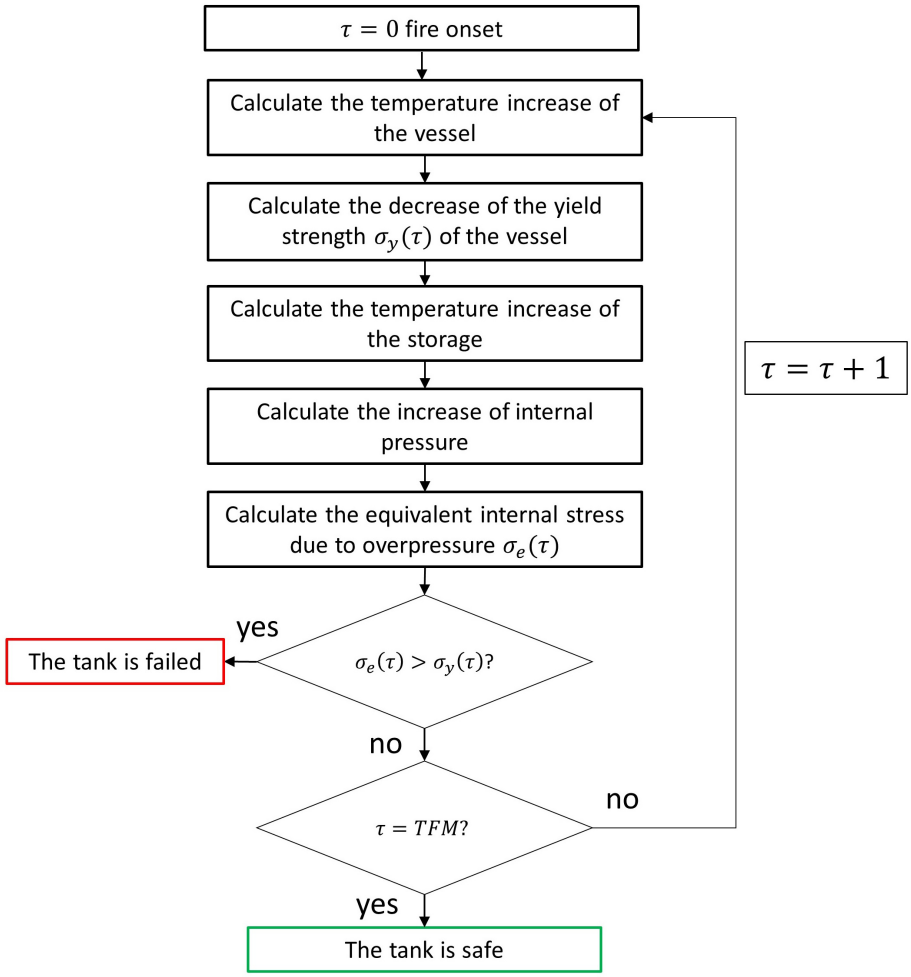


Figure 24. Flowchart of the dynamic model (Di Maio, Marchetti, et al., 2023b)

3.4.3 The RL environment model

To assess the impact of the maintenance actions on the system response to the accidental scenario, the DBN model of Section 3.4.2 has been used to calculate the failure probability of the three tanks (i.e., $P_{T1}(\tau, T), P_{T2}(\tau, T)$ and $P_{P1}(\tau, T)$) as a function of the accidental scenario evolution at the generic time τ and of the system age T.

3.4.4 Reward calculation

The reward is calculated with Eq. (18), since the maintenance policy is assumed to be constrained by the penalty terms listed in **Tab. 16**. The maintenance costs of **Tab. 10** are used to find $\boldsymbol{C}$ and the expected losses $L(\boldsymbol{s})$ are calculated as follows:

$$L(\boldsymbol{s}) = P^*_{T1}(\boldsymbol{s}) \cdot L_{T1} + P^*_{T2}(\boldsymbol{s}) \cdot L_{T2} + P^*_{P1}(\boldsymbol{s}) \cdot L_{P1} \quad (28)$$

where $P^*_j(\boldsymbol{s})$ (with $j = T1, T2$ and $P1$) is the failure probability of the *j-th* tank within the end of the accidental scenario ($\tau = 150\ min$), considering the environment state $\boldsymbol{s}$, and $L_{T1} = 1.5 \cdot 10^6$€, $L_{T2} = 1.2 \cdot 10^6$€ and $L_{P1} = 7.5 \cdot 10^5$€ are the economic losses

associated with the failure of T1, T2 and P1, respectively (Di Maio, Marchetti, et al., 2023a).

Table 16. Constraints and penalty terms (Di Maio, Marchetti, et al., 2023a).

Tank	MSE
T1	$2.6 \cdot 10^{-4}$
T2	$2.7 \cdot 10^{-4}$
P1	$2.1 \cdot 10^{-4}$

3.5 Results

3.5.1 Dynamic risk assessment with the PoF-based DBN framework

In this Section, it will be shown that the proposed PoF-based framework of analysis accounts for the safety barriers aging. As a benchmark, in **Fig. 25** and **Fig. 26** we show the risk assessment results assuming at $t = 0$ the deployment of the safety barriers configuration by-design (**Tab. 10**).

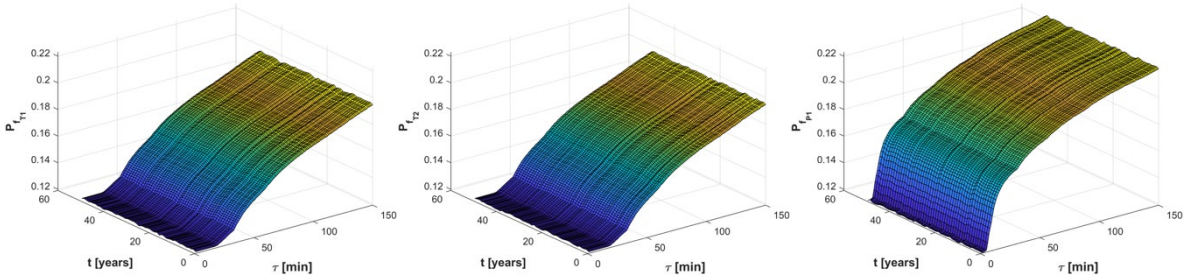


Figure 25. Results of $P_{f_{T1}}$ (left), $P_{f_{T2}}$ (center) and $P_{f_{P1}}$ (right) for the system used as by-design.

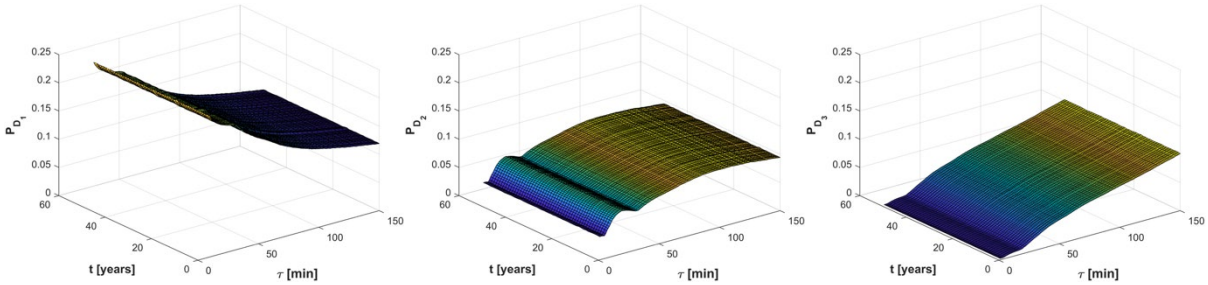


Figure 26. Results of P_{D_1}(left), P_{D_2}(center) and P_{D_3}(right) for the system used as by-design.

As shown in **Fig. 25**, the effect of aging on P_{f_j} is mitigated upon the adoption of the maintenance strategy of **Tab. 10** (i.e., P_{f_j} is constant at constant τ). The different evolution during the accidental scenario of $P_{f_{P1}}$ with respect to $P_{f_{T1}}$ and $P_{f_{T2}}$ is due to the higher operating pressure of P1, which makes it more vulnerable to failure due to overpressure (Xie, 2013), leading to a steeper increase in failure probability as the accidental scenario progresses.

For completeness of the analysis, the LSIRs obtained at the start and at the end of the system lifetime when the system is used as by-design, are shown in **Fig. 27**.

For clarity sake, to calculate the LSIR a Probit model of literature is used (C. Chen et al., 2021):

$$S = -14.9 + 2.56 \cdot \ln(6 \cdot 10^{-3} \cdot Q^{1.33} \cdot t_e) \tag{29}$$

where S is the human vulnerability to fire, Q is the heat radiation $\left[\frac{kw}{m^2}\right]$ at each location in the area surrounding the chemical facility and t_e is the time of exposure, which is assumed to be equal to the time needed for people to go from their location to a distance from the closest burning tank equal to 7 times its diameter (Sudheer et al., 2013), considering a pre-movement time of $120\ s$ and a walking speed of $1.5\frac{m}{s}$ (The Swedish National Board of Housing, 2011). The heat radiation $Q(P)$ for a generic point in space P Q decreases with the inverse square of the distance from the emission point (Stoffen, n.d.), and is defined as follows:

$$Q(P) = \frac{\overline{h_{T1}}}{d(P,T1)^2} + \frac{\overline{h_{T2}}}{d(P,T2)^2} + \frac{\overline{h_{P1}}}{d(P,P1)^2} \tag{30}$$

where $d(P,T1)$, $d(P,T2)$ and $d(P,P1)$ are the distances from P to T1, T2 and P1, respectively, and $\overline{h_{T1}}$, $\overline{h_{T2}}$ and $\overline{h_{P1}}$ are calculated as follows:

$$\overline{h_j} = \int_0^{\infty} h^* \cdot p_j(h^*)\ dh^* \tag{31}$$

where $p_j(h^*)$ is the probability that the *j-th* tank will emit a heat radiation equal to h^* (i.e., the probability of the state corresponding to the value h^* of the node that models h_j).

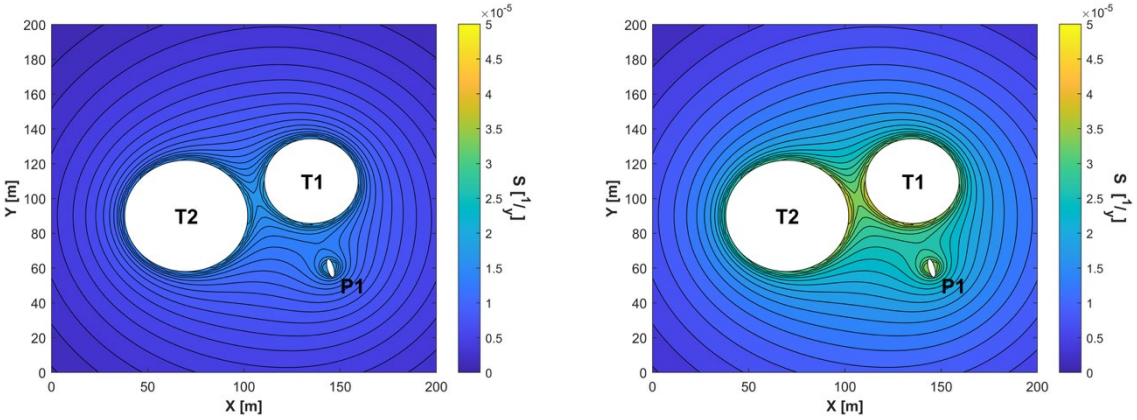


Figure 27. LSIR contour at $t = 0\ y$ (left) and $t = 50\ y$ (right) for the system used as by-design.

As shown in **Fig. 27**, the LSIR at the end of the design life of the tanks remains within the acceptable limit of $4.3 \cdot 10^{-5}$. The largest increase of LSIR is recorded within T1 and T2, due to the proximity of the two tanks and the possible interactive effects.

To show the risk updating allowed by the proposed framework and its practical use in informing the operators regarding the most proper actions to be implemented, the following information is assumed to become available:

1. at $t = 8\ y$, it becomes evident that the interval of the uncertain response time of ETI has increased from $t_{r,ETI} \in [420, 1020]$ s to $t^*_{r,ETI} \in [820, 1420]$ s, *due to the relocation of the closest emergency team station;*

2. at $t = 14\ y$, a global seismic hazard map is made available, that updated the magnitude-frequency curve (shown in **Fig. 28**) modelling the occurrence of PGA due to an earthquake nearby the facility;

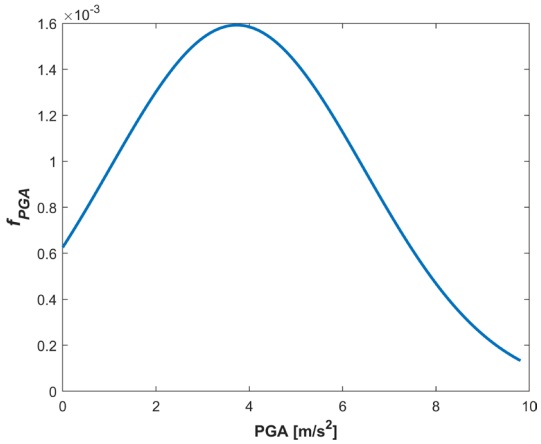


Figure 28. Updated magnitude-frequency curve of the earthquake PGA.

3. at $t = 23\ y$, the tanks are required to store a larger quantity of flammable substances than by-design (**Tab. 9**), because of the adoption of a more aggressive business strategy than before.

Table 17. Updated tanks storage mass.

Tank	Initial storage mass	Updated storage mass
T1	$3000\ ton$	$4000\ ton$
T2	$3000\ ton$	$3500\ ton$
P1	$52\ ton$	$60\ ton$

Then, after operating the system for $\Delta t = 8\ y$, the LSIR contour is updated as shown in **Fig. 29**. The LSIR at $t = 50\ y$ would exceed the acceptable threshold for distances from the tanks lower than $11\ m$ without the adoption of a proper action (e.g., reducing the maintenance intervals of the barriers, adding PFP to T1 and T2, upgrading the sprinkler systems…). The effects on the LSIR of whatever action to be taken can be evaluated with the developed DBN. If the chosen action is adding PFP on T1 and T2 to withstand the large heat radiation for long periods of time due to the long response time of ETI, the risk remains acceptable throughout the entire life of the system, as shown in the bottom row of **Fig. 29**.

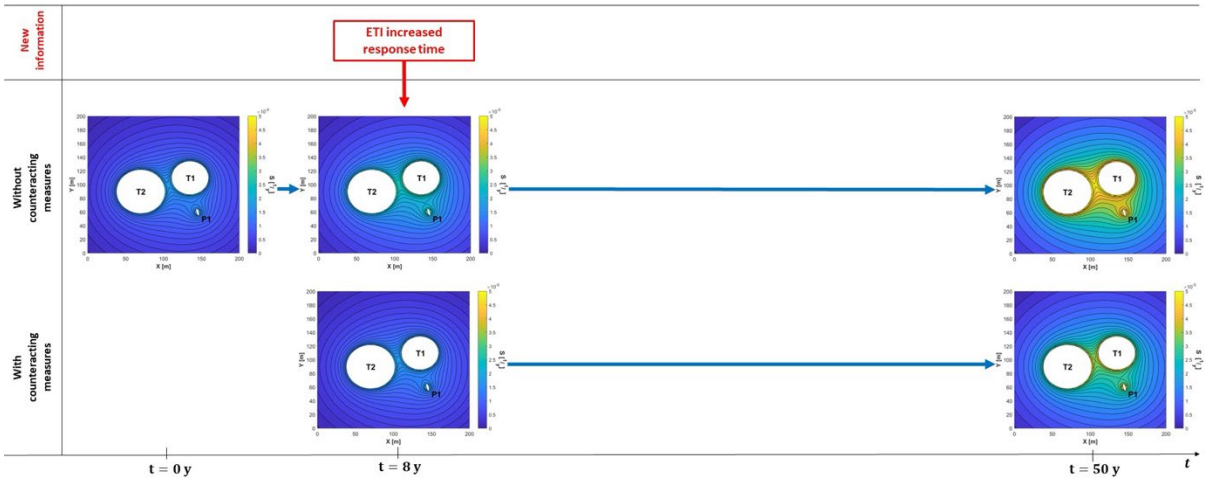


Figure 29. Updated LSIR contour at $t = 8\ years$ with and without proper actions.

At $t = 14\ y$, when the new earthquake magnitude-frequency curve is considered, the tanks seismic fragility could be reduced by anchoring them to their foundations with energy-dissipating anchors, and the LSIR can be updated as in **Fig. 30**.

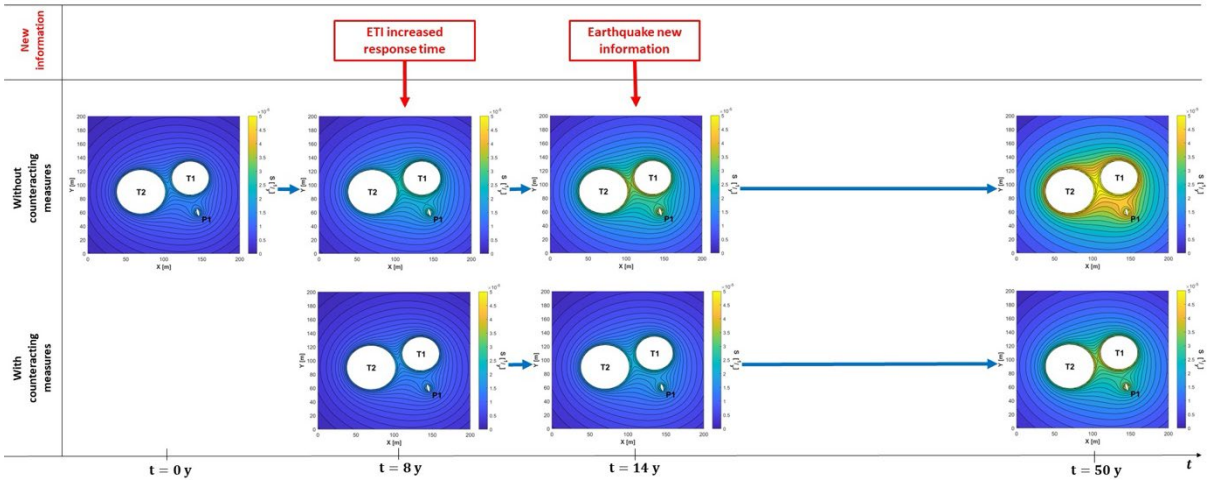


Figure 30. Updated LSIR contour at $t = 14\ years$ with and without proper actions.

At $t = 23\ y$, the tanks storage is increased and to keep risk to acceptable levels, the sprinkler systems (i.e., WDS and FWS) can be upgraded to Early Suppression Fast Response (ESFR) sprinklers (Palenske & Ornelas, 2023), which are designed to control and suppress fires faster than regular sprinklers. The resulting LSIR, is shown in **Fig. 31**. Note that in the case of no adoption of the ESFR sprinklers, the LSIR would exceed the acceptable threshold for distances from the tanks lower than $30\ m$.

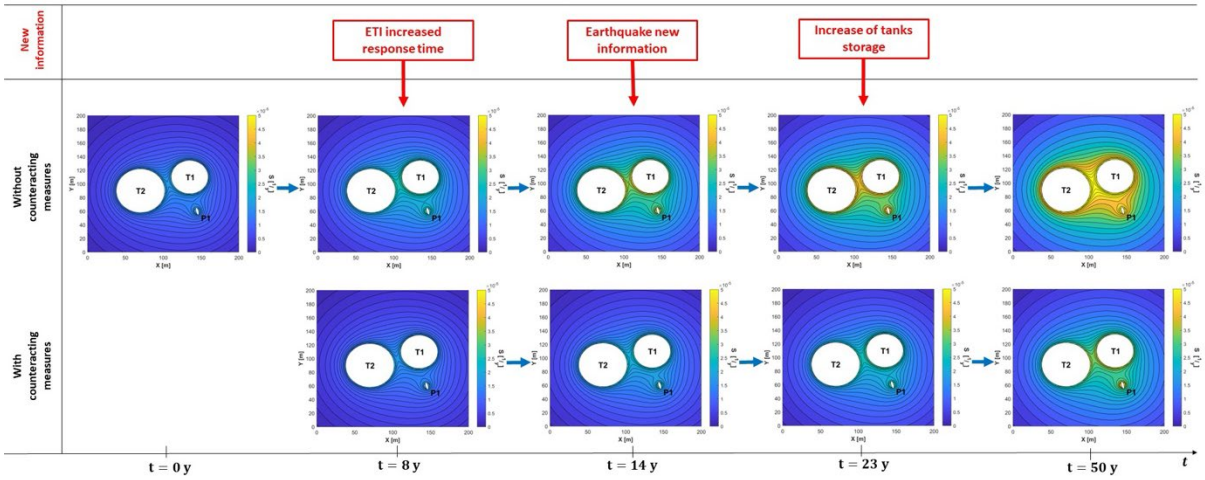


Figure 31. Updated LSIR contour at $t = 23\ years$ with and without proper actions.

The results of the case study presented show the capability of the framework of updating the system risk profile as new information is collected during its life; the updated information obtained can be used to identify proper actions for actively controlling the risk of accidents. The framework makes use of models of the aging safety barriers degradation in time, which may not always be available. In this case, dynamic risk assessment can still be performed using the DBN framework by feeding it with the time-dependent characteristics of the hazards and the time (age)-independent fragility curves of the safety.

3.5.2 Maintenance optimization by DRL

The hyperparameters of the PPO algorithm have been found by grid search (Friedrichs & Igel, 2005), leading to the following values:

- Actor DNN: two hidden layers with 64 neurons each, learning rate $lr = 3 \cdot 10^{-5}$;
- Critic DNN: two hidden layers with 64 neurons each, learning rate $lr = 10^{-4}$;
- Discount factor $\gamma = 0.99$;
- Clipping parameter $\epsilon = 0.2$.

The time between each maintenance decision is $dt = 60\ days$, leading to a total of $N_D = 300$ decision times, each with $N + 1 = 8$ possible actions, leading to $(N+1)^{N_D} = 8.45 \cdot 10^{270}$ different action sequences. To help tackle the complexity of the problem, the RL agent has been pretrained with a typical expert-based maintenance schedule (**Tab. 10**) (Marchetti, Di Maio, & Zio, 2024a), which serves as the starting point for the RL training. Then, the RL agent has been trained until convergence of the reward (shown in **Fig. 32**) over $N_{train} = 1200$ training epochs.

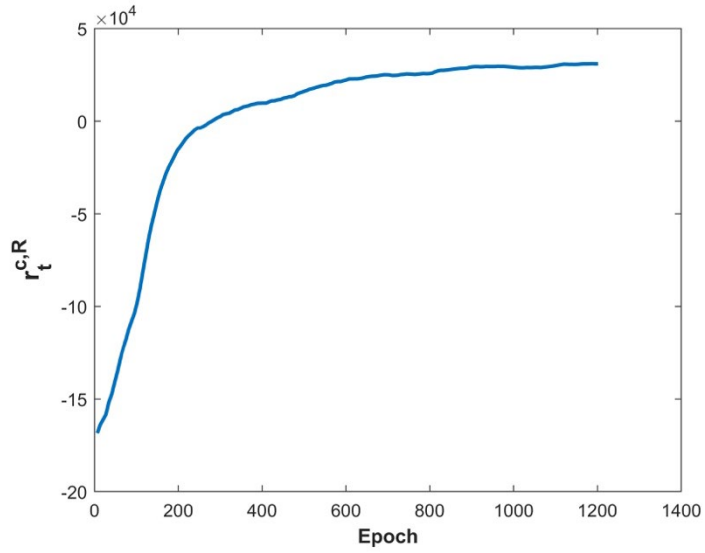


Figure 32. Reward of the RL agent during training.

Finally, the fine-tuned RL policy obtained has been compared with the expert-based schedule to find improvements in terms of risk and/or costs. In **Fig. 33**, $P_{T1}(\tau, T)$, $P_{T2}(\tau, T)$ and $P_{P1}(\tau, T)$ are shown for the RL policy (blue surface) and the expert-based policy (orange surface). For clarity sake, in **Fig. 34** it is plotted the sign of the difference between $P_{T1}(\tau, T)$, $P_{T2}(\tau, T)$ and $P_{P1}(\tau, T)$ of the two policies, i.e.:

$$sgn\left(\Delta P_j(\tau, T)\right) = \begin{cases} +1 & if\ P_j^{EB}(\tau, T) - P_j^{RL}(\tau, T) > 0 \\ 0 & if\ P_j^{EB}(\tau, T) - P_j^{RL}(\tau, T) = 0 \\ -1 & if\ P_j^{EB}(\tau, T) - P_j^{RL}(\tau, T) < 0 \end{cases} \quad (32)$$

where $P_j^{EB}(\tau, T)$ and $P_j^{RL}(\tau, T)$ are the values of the failure probabilities of the *j-th* tank at time τ and age T for the expert-based policy and for the RL policy, respectively. The RL policy is shown to outperform the expert-based one, since it achieves a lower failure probability for the tanks for most of their design life. To highlight this, the accidental scenario time has been fixed without loss of generality at $\tau = 150\ min$ to obtain P_{T1}^*, P_{T2}^* and P_{P1}^* as a function of age. As shown in **Fig. 35**, the RL policy achieves a lower failure probability for all the tanks and for almost all the considered ages. Furthermore, the RL policy achieves also a lower total maintenance cost, equal to $C_{RL} = 3.59 \cdot 10^5$€, than the one of the expert-based policy, which is equal to $C_{EB} = 5.26 \cdot 10^5$€. It is worth noting that while the difference in the cost of the two policies is significant, the difference in failure probability is almost negligible, especially in the few cases in which the expert-based policy achieves a lower failure probability than the RL policy.

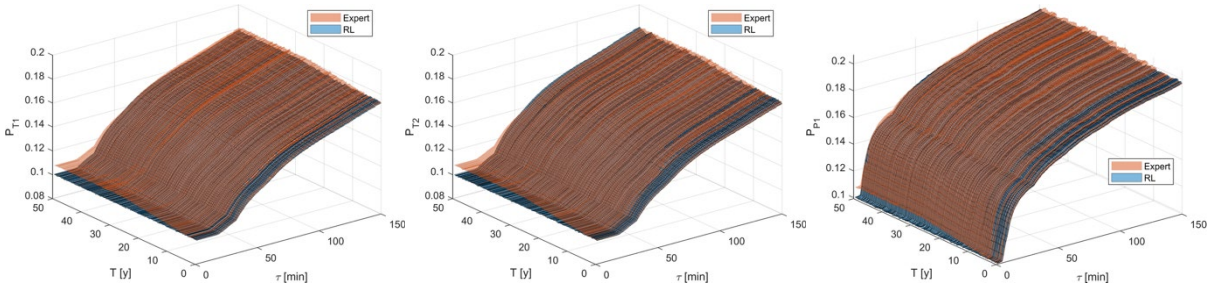


Figure 33. Time evolution of tanks failure probabilities.

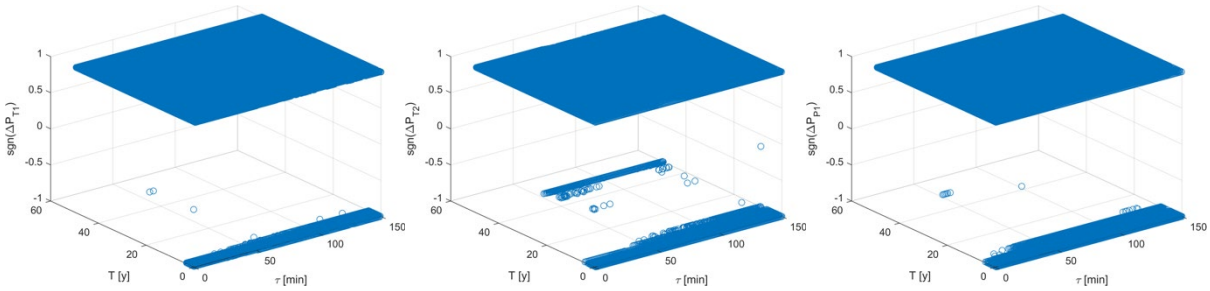


Figure 34. Time evolution of $sgn(dP_{T1})$, $sgn(dP_{T2})$ and $sgn(dP_{P1})$.

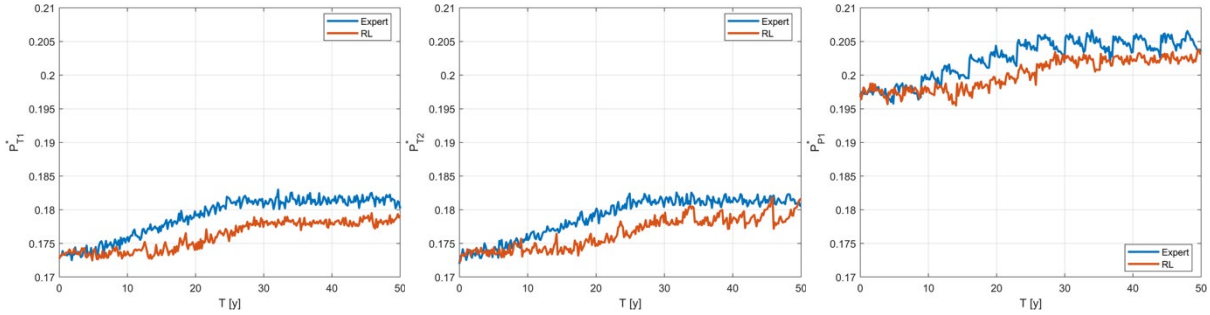


Figure 35. P^*_{T1}, P^*_{T2} and P^*_{P1} as a function of age.

The safety barriers more frequently maintained by the expert-based policy and by the optimal policy found are mined out by calculating the number of actions performed on each safety barrier throughout the system life. As shown in **Fig. 9**, PFP is the least maintained safety barrier in both policies, due to its large maintenance cos(Marchetti, Di Maio, & Zio, 2024a)archetti, Di Maio, & Zio, 2024a). The inefficiency of the expert-based policy is demonstrated by the small number of occurrences of the “No maintenance” action and by the over-prioritization of the maintenance of the sprinkler systems (i.e., WDS and FWS). Conversely, the agent has been successfully learning that maintenance actions are to be performed only when strictly necessary, as shown by the large number of occurrences of the “No maintenance” action, and has been learning to prioritize the maintenance of PSV of T1, due to its low maintenance cost and the significant economic losses associated with the failure of T1.

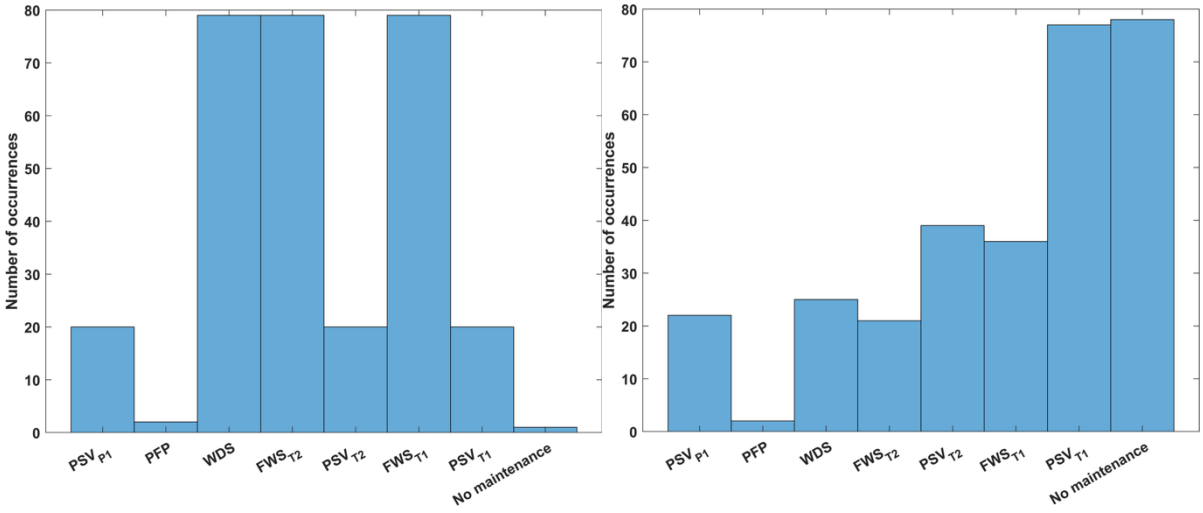


Figure 36. Number of occurrences of maintenance actions in the expert-based policy (left) and in the optimal policy (right).

To show the effectiveness of the RL in providing the operators with a prescriptive policy that adapts to changes in the degradation rates of the safety barriers, let us assume that the facility is exposed to the occurrence of two earthquake events, one at $t_1 = 10\,y$ and the other at $t_2 = 30\,y$, and that the earthquakes do not lead to the tanks failure but only to an increase of the degradation of the safety barriers. A shock model (Iervolino et al., 2013) is introduced to describe the increase in degradation under the following assumptions:

- PSV is not affected by earthquakes (Di Maio, Marchetti, et al., 2023a, 2023b; Misuri et al., 2020) and, therefore, its degradation does not increase;
- PFP, WDS and FWS are affected by earthquakes, leading to a decrease of their seismic capacity $\Delta\mu_1$ and $\Delta\mu_2$, as reported in **Tab. 18**, for the first and second earthquakes, respectively;
- ETI is affected by earthquakes because of the damage of the roads that allow the firefighting team to reach the site (Di Maio, Marchetti, et al., 2023a): however, it is assumed that roads are, in such circumstances, rapidly repaired by the local government.

Table 18. Decrease in seismic capacity due to earthquakes.

Safety barrier	$\Delta\boldsymbol{\mu_1}$	$\Delta\boldsymbol{\mu_2}$
PFP	30%	60%
WDS	20%	40%
ETI	20%	40%

Under these assumptions, the optimal policy found has been compared with the expert-based one, for which it is assumed that inspection and maintenance are promptly performed after each earthquake. In **Fig. 37-39**, P^*_{T1}, P^*_{T2} and P^*_{P1} are shown together with the actions performed by the RL agent as a function of age. As shown,

the RL policy is able to achieve a lower risk of failure that the expert-based one for all of the tanks. The adaptability of the RL agent to the sudden increase in degradation is shown by the execution of maintenance actions shortly after the earthquake occurrence, which is particularly evident in **Fig. 39**, where on P1 the maintenance of PFP is done at $T = 3720\ days$ (i.e., shortly after the earthquake) even if it was already performed at $T = 3540\ days$ (i.e., shortly before the earthquake). Furthermore, the RL policy achieves a lower total maintenance cost, equal to $C_{RL,2} = 5.17 \cdot 10^5$ €, than the one of the expert-based policy, which is equal to $C_{EB,2} = 6.46 \cdot 10^5$€.

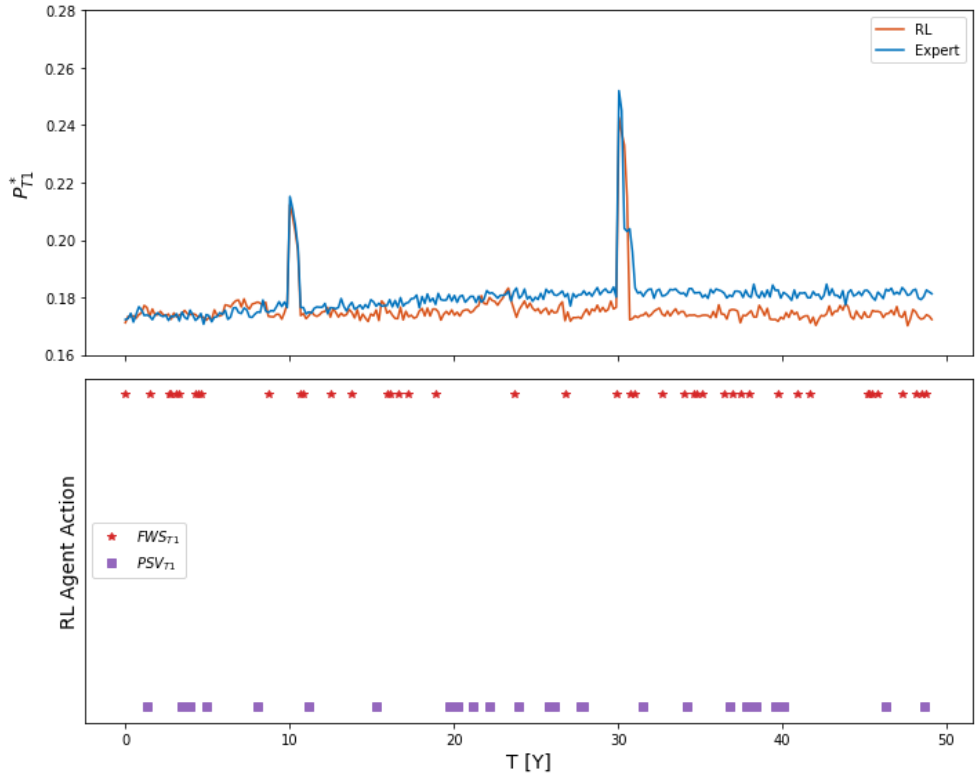


Figure 37. P^*_{T1} and RL agent actions as a function of age.

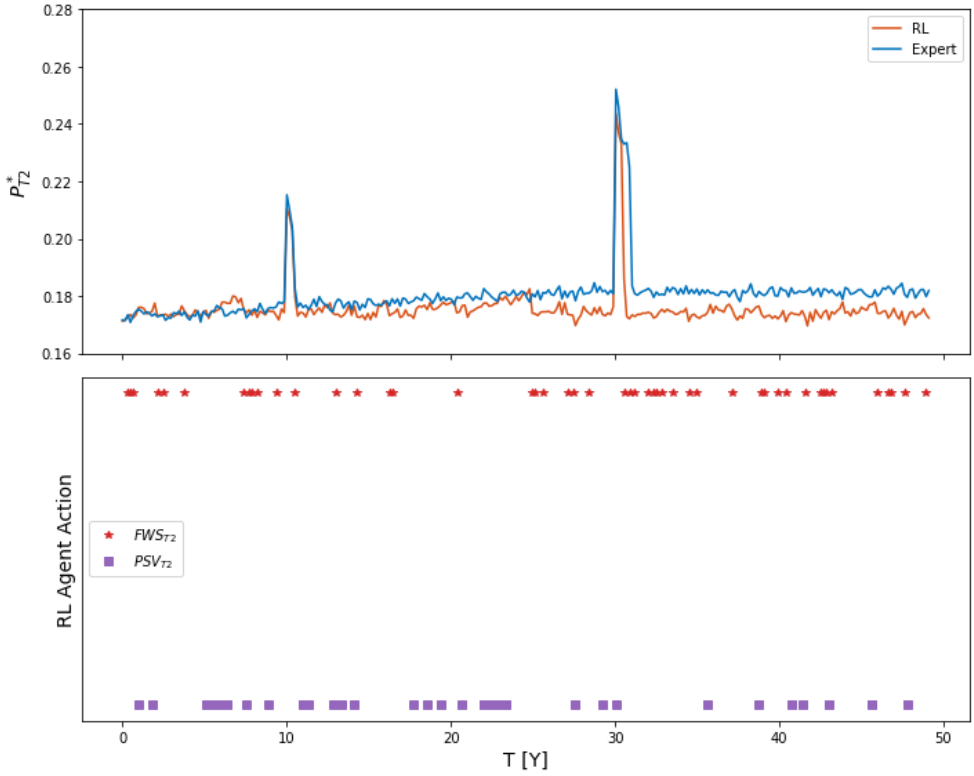


Figure 38. P^*_{T2} and RL agent actions as a function of age.

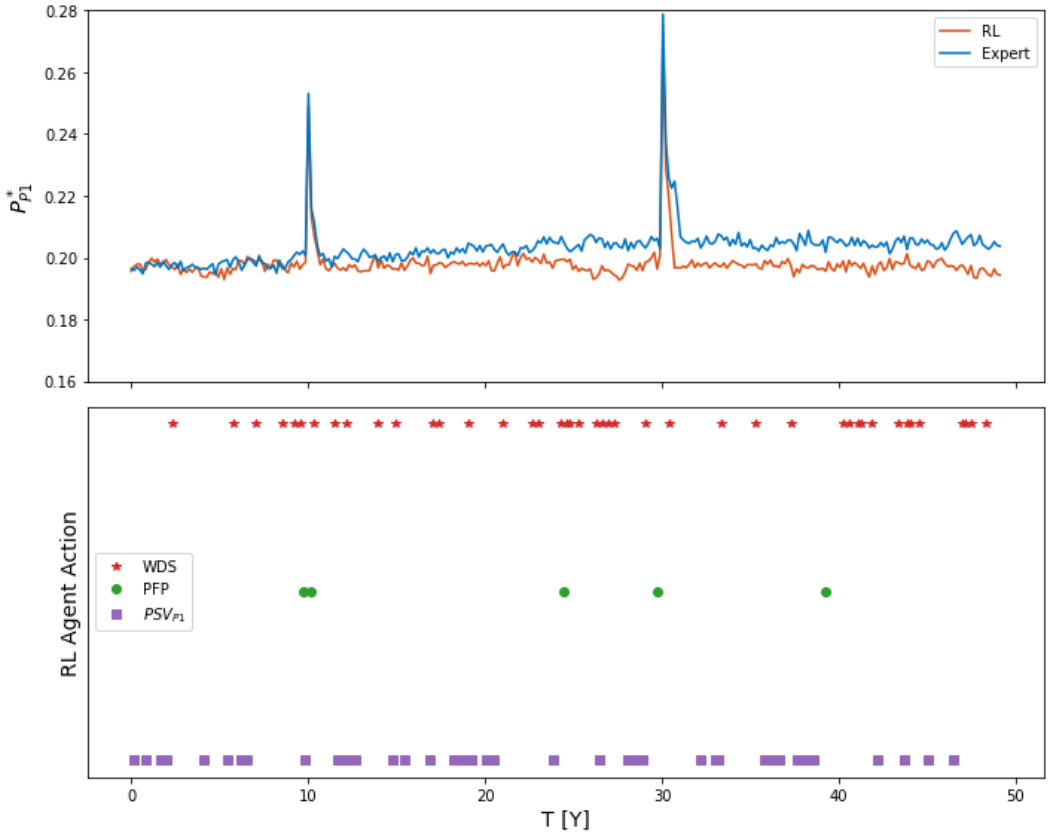


Figure 39. P^*_{P1} and RL agent actions as a function of age.

Chapter 4 Risk-informed design of multi-unit Nuclear Power Plants

Contents of this Chapter have been adapted from:

[J2] *S. Marchetti, F. Di Maio and E. Zio, "An Integrated Deterministic and Probabilistic Safety Assessment of Multi-Unit Small Modular Reactors Considering the Degradation of Shared Safety Features", Nuclear Science and Engineering, 2025. DOI:10.1080/00295639.2025.2515349.*

[J3] *S. Marchetti, F. Di Maio, E. Zio, E. Borgonovo and E. Plischke, "A global sensitivity analysis framework for guiding the design improvement of new concepts of small modular reactors", Nuclear Design and Engineering, Volume 444, 2025. DOI: 10.1016/j.nucengdes.2025.114398.*

4.1 Introduction

Small Modular Reactors (SMRs) promise lower construction and operational costs, enhanced safety features with respect to traditional large-sca(Z. Liu & Fan, 2014)nts (NPPs) (Z. Liu & Fan, 2014), and flexible power capacity through modular Multi-Unit (MU) configurations (Vujić et al., 2012). MU-SMRs, and MU-NPPs in general, share some safety features (e.g., Emergency Core Cooling System (ECCS), Decay Heat Removal (DHR)…) (Di Maio, Bani, et al., 2023; Hassija et al., 2014; Lamarsh, 1981; Xing et al., 2020). To achieve safety enhancements, the design of SMRs must prioritize safety since the very early stages, implementing comprehensive defense-in-depth strategies for preventing severe accidents and mitigating their consequences (International Atomic Energy Agency (IAEA), 2016). In this regard a rigorous assessment of the Critical failure Region (CR), i.e., the boundary of the reactor parameter space beyond which failure may lead to unacceptable consequences (Puppo et al., 2021), is needed to risk-inform the effective deployment of defense-in-depth principles. At the same time, the degradation of shared safety features must be accounted for in the risk assessment (Aumeier et al., 2006; Di Maio, Marchetti, et al., 2023b, 2023a; Marchetti et al., 2023; Unwin et al., 2012).

Within this perspective, an Integrated Deterministic and Probabilistic Safety Assessment (IDPSA) framework is first developed to dynamically assess how the age-dependent degradation of shared safety features impacts system risk. IDPSA combines deterministic and probabilistic approaches of safety assessment to overcome the limitations of static logic models (Zio, 2014) (such as Fault Trees (FTs) (Flage et al., 2013) and Event Trees (ETs) (Huang et al., 2001). Typically, dynamic simulators of the system behaviour are coupled with probabilistic models to account for uncertainties (e.g., hazard magnitude, component failure times…). A number of methodologies have been developed for IDPSA (e.g., Cell-to-Cell Mapping Technique (CCMT) (Tombuyses & Aldemir, 1997; P. Wang & Aldemir, 2004), Dynamic Event Tree

(DET) (Cohn et al., 2023; Di Maio et al., 2017), GO-FLOW methodology (Matsuoka & Kobayashi, 1988), Adaptive simulation (Turati et al., 2017a, 2017b), Monte Carlo Dynamic Event Tree (MCDET) (Kloos & Peschke, 2006), Genetic Algorithm-based Dynamic Probabilistic Risk Assessment (GA-DPRA) (Vorobyev & Kudinov, 2011), Analysis of Dynamic Accident Progression Trees (ADAPT) (Hakobyan et al., 2008) etc.). In this work, age-dependent fragility surfaces based on tailored Physics-of-Failure (PoF) fragility models (Marchetti, Di Maio, & Zio, 2024a) are embedded in a dynamic model capable of accounting for equipment sharing, coupled with a Monte Carlo simulation scheme to account for the involved uncertainties (e.g., the magnitude of the hazard, the failure time and response time of the safety features,…).

Building upon the accident simulations generated by the IDPSA dynamic model, a GSA framework is subsequently introduced for the risk-informed design of MU-SMRs. Because of the lack of operational experience and data, the risk-informed design process requires relying on complex, high-fidelity simulators to replicate as realistically as possible the physics and thermodynamics of SMRs, and obtain reliable indications of their behavior during accidents. However, the lack of data implies uncertainty in the input parameters of the simulation codes, which reverberates on their output results. One, then, needs to perform thorough uncertainty quantification to characterize the variability in the safety-related quantities of interest by propagating input uncertainties through the simulators (Gabbar & Esteves, 2022; Poudel et al., 2020). At the same time, it is important, especially for SMRs, to identify key inputs and ensure adequate safety margins, given the complexity of the physical models involved (Fang et al., 2021; Podila et al., 2021). In this respect, the literature has demonstrated that integrating uncertainty quantification with sensitivity analysis can, in fact, meet these needs (Hamel et al., 2010).

Sensitivity analysis methods are typically classified into local and global. Local sensitivity analysis evaluates the impact of variations in one or more inputs at a specific location in the input parameter space. Local methods comprise differentiation-based methods or methods based on finite differences. An early discussion in the nBorgonovo & Apostolakis, 2001; Helton, 1993bApostolakis, 2001; Helton, 1993b). As seen in the literature, local techniques are not designed to capture uncertainty. Also, they typically imply the variation of one-input-at-a-time, thus failing in capturing or respecting input dependences. This makes them possibly less suitable for inferring the importance of inputs in complex and nonlinear models, which, instead, are common in SMR simulations (Saltelli et al., 2000). Conversely, GSA methods are designed to allow the input parameters to vary across their full ranges and account for interactions and nonlinearities (Saltelli et al., 2000). GSA has already been applied across various disciplines in the nuclear sector and as well as in climate change (Butler et al., 2014), socio-cultural (Fono(Mara & Tarantola, 2008)hermal (Mara & Tarantola, 2008) and mechanical (P. Kumar et al., 2020) models. In the nuclear industry, applications involve identifying surrogate model parameters (Cervi et al., 2022), tailoring Inverse Uncertainty Quantification (IUQ) processes (Di Maio et al., 2024), analyzing source

term uncertainties in accidental scenarios (Zheng et al., 2015), and evaluating the time-dependent effects of uncertain parameters on reactor cladding temperatures during Large Break Loss Of Coolant Accidents (LBLOCAs) (Xiong et al., 2022). Additionally, sensitivity analysis, such as perturbation-theory-based approaches (Pusa, 2012), is integral to the Best Estimate Plus Uncertainty method, widely adopted for NPPs safety assessments (Martin & Petruzzi, 2021).

Applying GSA methods to SMR simulators introduces new challenges and opens new research questions. First, the analysis is challenging, because of the large computational burden of the simulation codes, which calls for an extensive uncertainty quantification that allows modelers to inspect the model behavior thoroughly, letting the inputs vary simultaneously in the parameter space. This is necessary to properly characterize engineering uncertainty in the safety-related quantities of interest (Le Duy & Vasseur, 2018; T. Zhou et al., 2018). Second, SMR models typically output a multiplicity of quantities of interest, while most GSA methods in use are constructed for univariate responses (Borgonovo et al., 2024). Third, inputs might be correlated, which is also a challenge for current GSA methods.

To solve these issues, we propose a novel framework that combines input prioritization through Optimal Transport (OT)-based sensitivity indices (Borgonovo et al., 2024), and the assessment of marginal behavior through the CUmulative SUm of NOrmalized Reordered Output (CUSUNORO) (Plischke, 2012). OT-based global sensitivity indices are defined to yield the importance of inputs for univariate or multivariate outputs and are well posed in the presence of correlated inputs. Through CUSUNORO curves, one can perform a critical parameter segmentation, i.e., identify the critical input values, that, if exceeded, may cause the system to quickly approach the CR. The novelty of the approach lies in the integrated use of a suite of SA approaches, i.e., OT-based sensitivity indices and CUSUNORO, to enable decision support regarding the design of new concepts of NPPs, such as SMRs.

Regarding the computational burden, both OT and CUSUNORO are calculated with a given-data approach using a single-loop Monte Carlo estimation, i.e., directly from the simulations used for uncertainty quantification (Plischke et al., 2013). If N_{sim} denotes the number of simulations used for uncertainty quantification, then the computational cost of the method is N_{sim}, making it independent of the input dimensionality. Conceptually, this is the minimal cost for GSA. Thus, the method post-processes the input-output dataset produced by a Monte Carlo uncertainty analysis. Consequently, as it happens in any GSA investigation, the quality of the results is associated with the uncertainty quantification thoroughness, as an insufficient exploration of the input-output space might affect the reliability of the analysis.

We present the implementation of the proposed methods on a demonstrative test case, based on a MU-SMR installation composed by $N = 4$ units of Small Modular Dual Fluid Reactor (SMDFR), a fast reactor design with liquid lead flowing through the reactor core as coolant and molten salt as fuel (C. Liu et al., 2021). The high operating

temperatures that can be reached ensure a high thermal efficiency and make the SMDFR ideal for clean hydrogen production (Huke et al., 2015). The overall design has four shared Auxiliary Cooling Systems (ACSs) to provide additional coolant mass flow rate to the SMDFR coolant circuit in case of Loss Of Coolant Accident (LOCA), and two shared Emergency Diesel Generators (EDGs) to operate in case of Loss Of Power (LOP). The peak cladding temperature (T_w) is the safety-related quantity of interest (Marchetti et al., 2025). Fragility surfaces are defined for the safety features to calculate their age-dependent failure probability. These are used as inputs to a dynamic physical model that simulates the accident scenario. Integration within a Monte Carlo simulation scheme allows estimating the failure probability of the units of the MUNPP. The comparison of the results with the estimated values of Core Damage Frequency (CDF) of MUNPPs made of either Gen-III Light Water Reactors (LWRs) or other SMRs (in line with (Prasad et al., 2017) and (Di Maio, Bani, et al., 2023), respectively) confirms that neglecting the sharing of safety features may lead to overlooking accident scenarios and to underestimating the probability of multiple units failure. Also, considering perfect and imperfect safety features maintenance shows that neglecting degradation can lead to overly optimistic risk estimates. Then, parameter prioritization by OT lists the earthquake Peak Ground Acceleration (PGA), the corrosion of CP and the failure time of ACS as the most important inputs. The results of the OT-based sensitivity provide effective indications for design improvement, e.g., improving the seismic reliability of the NPP and the resistance to corrosion of CP. The CUSUNORO analysis provides, in addition, insights on the failure-critical values of these parameters, which can be used to ensure that the SMDFR operates far from the CR.

4.2 A framework of IDPSA for MUPSA with aging safety features

Let us consider a MUNPP, composed of $i = 1,2,\dots,N$ units, and equipped with $s = 1,2,\dots,N_s$ safety features, among which ΔN_s are shared among the N units. The MUNPP is exposed to natural hazards, e.g. earthquakes. To account for aging of the shared safety features the following steps are carried out (**Fig. 40**):

1) Characterize:
    a. the natural hazard, by the magnitude-frequency curve;
    b. the system response to the hazard, in particular in terms of:
        b.i. the safety features performance, by age-dependent fragility surfaces;
        b.ii. the Common Cause Failures (CCFs) of the ΔN_s shared safety features, by CCF models;
2) Define a dynamic model of the accident scenario evolution;

3) Calculate the system failure probability at each age τ, by integrating the dynamic model into a Monte Carlo simulation scheme to account for the uncertainties therein.

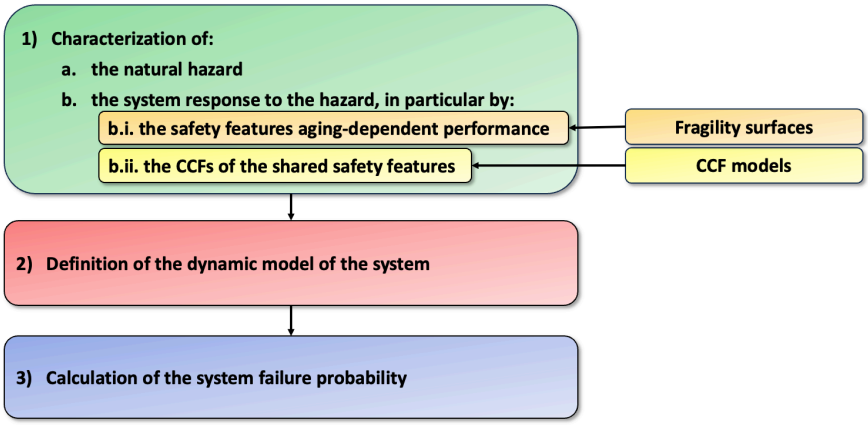


Figure 40. Flowchart of the proposed framework.

4.2.1 Hazard and system characterization

Natural hazards are typically characterized by a magnitude-frequency curve, extracted from historical data. The system response to a hazard depends on its physical properties, layout, subsystems and components, also possibly shared among different units of the system.

Each $s = 1,2,\dots,N_S$ safety feature in the system is characterized by a response time $t_{r,s}$ and a failure probability $P_{f,s}$ (see Eq. 33); the latter is composed of the probability of failure due to internal causes ($P_{f,s}^{I}$) and due to external hazards ($P_{f,s}^{E}$), both functions of the age τ and the latter also of the hazard magnitude H (Marchetti, Di Maio, & Zio, 2024a):

$$P_{f,s}(H,\tau) = P_{f,s}^{I}(\tau) + P_{f,s}^{E}(H,\tau) - P_{f,s}^{I}(\tau)\cdot P_{f,s}^{E}(H,\tau) \quad [33]$$

In particular, $P_{f,s}^{I}(\tau)$ can be computed by a degradation model (e.g., a pipe corrosion degradation model with a threshold-based failure criterion on the pipe thickness (Zhang, 2009), whereas $P_{f,s}^{E}(H,\tau)$ can be calculated using a fragility surface obtained integrating PoF-based aging models into the fragility model of the specific safety feature exposed to the specific natural hazard (Marchetti, Di Maio, & Zio, 2024a).

The probability of CCF among the shared safety features is assessed by typical CCF models, such as:

- alpha-factor model (Mosleh, 1987); for a subgroup of $N_A \in \Delta N_S$ shared safety features, CCF factors $\alpha_1, \alpha_2, \dots, \alpha_{N_A}$ are defined and the probabilities of failure of groups of $1,2,\dots,N_A$ safety features (i.e., $P_{f,s}^{1}, P_{f,s}^{2}, \dots, P_{f,s}^{N_A}$) are calculated:

$$P_{f,s}^{1} = \alpha_1 P_{f,s}$$
$$P_{f,s}^{2} = \alpha_2 P_{f,s}$$
$$\dots \quad (34)$$
$$P_{f,s}^{N_A} = \alpha_{N_A} P_{f,s}$$

- dependency evaluation tree (Jang & Jae, 2020); for a subgroup of $N_B \in \Delta N_s$ shared safety features, a dependency evaluation tree (e.g., **Fig. 41,** where ZD stands for "Zero Dependency", LD stands for "Low Dependency", MD stands for "Medium Dependency" and HD stands for "High Dependency") is used to evaluate the dependency among the features.

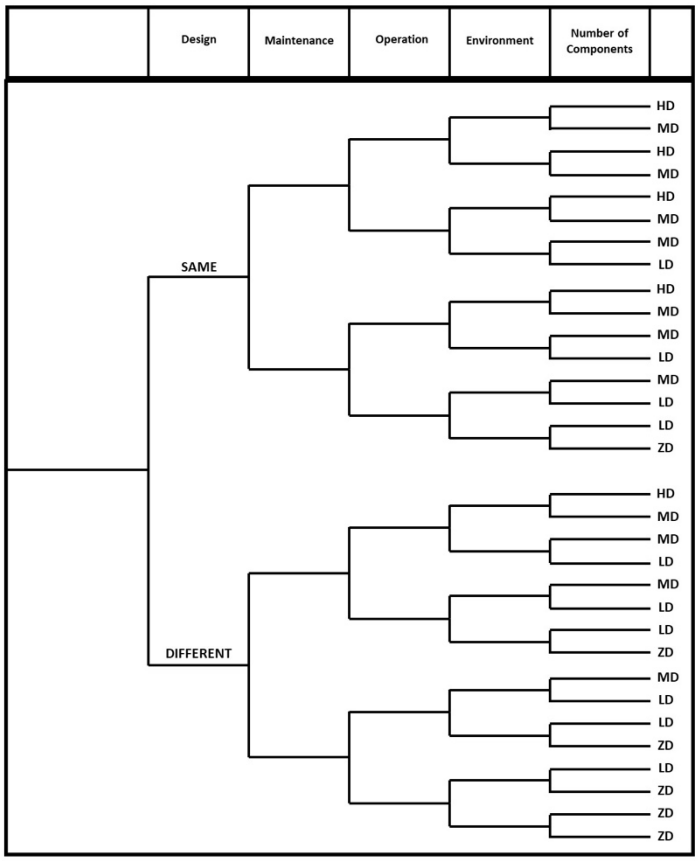


Figure 41. Dependency evaluation tree.

Then, the probability associated with each CCF combination is calculated as follows (Jang & Jae, 2020):

$$P_{s,CCF}(n_B) = \sum_{b=1}^{n_B} \left(P_{f,b} \cdot \prod_{c=1, c \neq b}^{n_B} P_{CCF,c}(b) \right) \quad (35)$$

where n_B is the number of safety features involved in the CCF combination and $P_{CCF,c}(b)$ is the probability of failure of the *c-th* safety feature conditioned to the failure of the *b-th* safety feature, defined as in **Tab. 19**.

Table 19. Conditional failure probabilities.

Dependency level	Conditional probability	Dependency level
ZD	$P_{CCF,c} = P_{f,c}$	ZD
LD	$P_{CCF,c} = \frac{1 + 19P_{f,c}}{20}$	LD
MD	$P_{CCF,c} = \frac{1 + 6P_{f,c}}{7}$	MD
HD	$P_{CCF,c} = \frac{1 + P_{f,c}}{2}$	HD

4.2.2 Dynamic model of accident evolution

The parameters values defined in Section 4.2.1 (i.e., $t_{r,s}, P_{f,s}$ and the CCF probabilities) are fed to a dynamic model to simulate the evolution of the accident scenarios in terms of relevant safety parameters.

4.2.3 System failure probability calculation

Simulations are performed to quantify the failure probability at each age τ of single units and groups of units (P_i with $i = 1,2,\dots,N$ and P_z^S with $z = 1,2,\dots,N$, respectively), conditioned to the accidental scenario occurred. To account for uncertainties (e.g., in the hazard magnitude, safety features failure times and response times,…) Monte Carlo simulation of M alternative scenario conditions is performed. A flowchart of the procedure for the simulation is provided in **Fig. 42**.

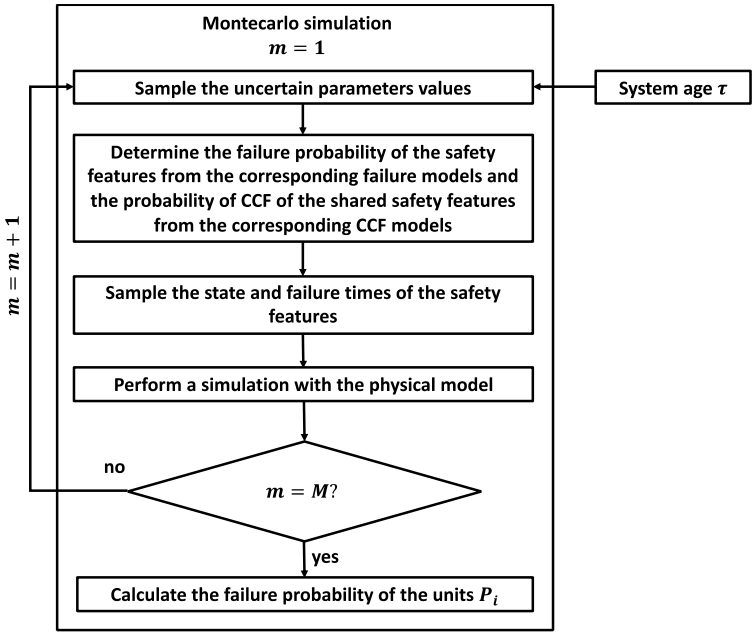


Figure 42. Flowchart of the Monte Carlo simulation scheme.

4.3 The sensitivity analysis methods

Out approach is based on the combination of global sensitivity indices based on the theory of optimal transport and CUSUNORO curves. Section 4.3.1 presents the general GSA setup. Sections 4.3.2 and 4.3.3 present OT-based global sensitivity measures and the CUSUNORO method, respectively.

4.3.1 System failure probability calculation

In the general GSA setup, one considers a simulation model that processes a set of inputs and calculates a set of quantities of interest. We denote the vector of inputs and outputs respectively by $\boldsymbol{X} = [X_1, X_2, \dots, X_I] \in D_{\boldsymbol{X}} \subset \mathbb{R}^I$, and $\boldsymbol{Y} = [Y_1, Y_2, \dots, Y_O] \in D_{\boldsymbol{Y}} \subset \mathbb{R}^O$, where I and O are the number of inputs and outputs. We also let $\boldsymbol{Y} = m(\boldsymbol{X})$ denote the input-output mapping, with $m: D_{\boldsymbol{X}} \rightarrow D_{\boldsymbol{Y}}$. Under uncertainty, the inputs and outputs are random variables on measurable space $(\Omega, B(\Omega), \mathbb{P})$, with joint probability law $\mathbb{P}_{\boldsymbol{Y},\boldsymbol{X}}$ and marginal distributions $\mathbb{P}_{\boldsymbol{X}}$ and $\mathbb{P}_{\boldsymbol{Y}}$, respectively. We also assume that the conditional laws $\mathbb{P}_{\boldsymbol{Y}|X_i}$ are well posed for all $i = 1,2, \dots, I$. Throughout the paper, we will assume that the model output has finite second order moment. This implies that the variance of Y_o is finite, an assumption that is verified by physical systems.

Under uncertainty, knowledge about the key-factors that drive the model response is gained through GSA methods. These methods have a long tradition and several of them have been developed to address problems originated by nuclear engineering applications. We recall the work of (Helton, 1993a), that describes the risk and uncertainty analysis for dose exposure from radioactive waste disposals, of (Eisenberg & Sagar, 2000), that uses importance measures for the performance

assessment of a nuclear waste repository and of (Ikonen, 2016), where GSA is applied to fuel performance codes.

Several of the GSA methods in use can be encompassed in a common rationale, where one writes the global sensitivity measure of X_i with respect to $\boldsymbol{Y}$ as (Borgonovo et al., 2016):

$$\xi(\boldsymbol{Y}, X_i) = \mathbb{E}\left[\zeta\left(\mathbb{P}_{\boldsymbol{Y}}, \mathbb{P}_{\boldsymbol{Y}|X_i}\right)\right], \tag{36}$$

where $\zeta\left(\mathbb{P}_{\boldsymbol{Y}}, \mathbb{P}_{\boldsymbol{Y}|X_i}\right)$ is a distance (or separation) between the probability distribution of $\boldsymbol{Y}$ and its conditional probability distribution after learning X_i and the expectation is carried over the distribution of X_i. To illustrate, if X_i is an absolutely continuous random variable, denoting its probability density function with $f_i(X_i)$, then Eq. (36) is equivalent to:

$$\xi(\boldsymbol{Y}, X_i) = \int_{-\infty}^{\infty} \zeta\left(\mathbb{P}_{\boldsymbol{Y}}, \mathbb{P}_{\boldsymbol{Y}|X_i}\right) f_i(X_i) dX_i \tag{37}$$

Variance-based sensitivity measures are encompassed by the common rationale. To illustrate, if the output is univariate and we select as a separation measurement the quantity

$$\zeta^{VB}\left(\mathbb{P}_Y, \mathbb{P}_{Y|X_i}\right) = \frac{(\mathbb{E}[Y|X_i] - \mathbb{E}[Y])^2}{\mathbb{V}[Y]} \tag{38}$$

we obtain $\xi^{VB}(Y, X_i)$, given by:

$$\xi^{VB}(Y, X_i) = \frac{\mathbb{V}[Y] - \mathbb{E}_{X_i}\left[\mathbb{V}_{X_{j\neq i}}[Y|X_i]\right]}{\mathbb{V}[Y]} = S(Y, X_i) \tag{39}$$

The variance-based index $\xi^{VB}(Y, X_i)$ coincides with the first-order variance-based indices, also known as Sobol indices. When inputs are dependent, Eq. (39) is equivalent to Pearson correlation ratio and coincides with the global sensitivity measure proposed by (Iman & Hora, 1990) for the probabilistic risk assessment of NPPs.

However, these methods have been developed mainly for univariate quantities of interest and are challenged by the multivariate nature of the simulation output, which, instead, characterizes the simulations of SMRs, especially when they are time or space dependent. To solve this issue, we rely on a global sensitivity measure based on the theory of optimal transport that we discuss in Section 4.3.2.

4.3.2 Optimal Transport-based GSA

The global sensitivity measure we use in this work has been defined in (Borgonovo et al., 2024), to which we refer for a complete overview. To make the present paper self-contained, we offer a concise overview. The theory of optimal transport has been widely studied across mathematics, statistics and machine learning (Y. Chen et al., 2021). A detailed theoretical description of can be found in (Peyré & Cuturi, 2019; Villani, 2007). Of relevance to us is the use of optimal transport to measure the distance between probability distributions.

In our context, we are considering two distributions of $\boldsymbol{Y}$, its marginal distribution $\mathbb{P}_{\boldsymbol{Y}}$ and conditional distribution $\mathbb{P}_{\boldsymbol{Y}|X_i}$. For notation simplicity, let us denote them with $\nu = \mathbb{P}_{\boldsymbol{Y}}$ and $\nu_i = \mathbb{P}_{\boldsymbol{Y}|X_i}$, respectively. In an optimal transport setting, we aim to find a transport plan from ν to ν_i that minimized a given cost function. We denote a generic transport plan with $\pi(\boldsymbol{y}, \boldsymbol{y}')$, where $\boldsymbol{y}$ and $\boldsymbol{y}'$ are realizations, respectively, of $\boldsymbol{Y}$ and $\boldsymbol{Y}'$. Note that $\pi(\boldsymbol{y}, \boldsymbol{y}')$ is a function mapping $k: D_{\boldsymbol{Y}} \times D_{\boldsymbol{Y}} \rightarrow [0, +\infty]$ that gives us the cost $k(\boldsymbol{y}, \boldsymbol{y}')$ we incur for moving a value of $\boldsymbol{y}$ that follows the distribution ν to a value $\boldsymbol{y}'$ that follows the conditional distribution ν_i.

The choice of the cost function can be quite general. As in (Borgonovo et al., 2024), a typical choice is for $k(\boldsymbol{y}, \boldsymbol{y}')$ to be lower semi-continuous. Then, the integral cost given plan $\pi(\boldsymbol{y}, \boldsymbol{y}')$ is:

$$K(\pi) = \iint_{Y \times Y} k(\boldsymbol{y}, \boldsymbol{y}')\, d\pi(\boldsymbol{y}, \boldsymbol{y}') \tag{40}$$

The Kantorovich OT-problem is then to find the plan $\pi(\boldsymbol{y}, \boldsymbol{y}')$ that minimizes $K(\pi)$. There is a high flexibility in choosing the cost function. A typical choice is the Euclidean distance, so that $k(\boldsymbol{y}, \boldsymbol{y}') = d^p(\boldsymbol{y}, \boldsymbol{y}') = \|\boldsymbol{y} - \boldsymbol{y}'\|^d$. In this case, the OT-problem becomes to determine

$$W_p^p(\nu, \nu_i) = \inf_{\pi \in \Pi(\nu, \nu_i)} \int d^p(\boldsymbol{y}, \boldsymbol{y}')\, d\pi(\boldsymbol{y}, \boldsymbol{y}') \tag{41}$$

where $W_p^p(\nu, \nu_i)$ is the *p-th* power of the so-called Wasserstein distance of order *p* between ν and ν_i. When $p = 2$, we find the 2-squared Wasserstein distance

$$W_2^2(\nu, \nu_i) = \inf_{\pi \in \Pi(\nu, \nu_i)} \int \|\boldsymbol{y} - \boldsymbol{y}'\|^2 d\pi(\boldsymbol{y}, \boldsymbol{y}') \tag{42}$$

which has been widely studied and applied in the literature. $W_2^2(\nu, \nu_i)$ admits a decomposition into three distinct components, which turnsGelbrich, 1990; Givens & Shortt, 2002ich, 1990; Givens & Shortt, 2002). We have:

$$\begin{aligned} W_2^2(\nu, \nu_i) = {} & \|\mathbb{E}[\boldsymbol{Y}] - \mathbb{E}[\boldsymbol{Y}|X_i]\|^2 + Tr\left(\Sigma_{\boldsymbol{Y}} + \Sigma_{\boldsymbol{Y}|X_i} - 2\Sigma_{\boldsymbol{Y}}^{1/2}\Sigma_{\boldsymbol{Y}|X_i}\Sigma_{\boldsymbol{Y}}^{1/2}\right) \\ & + \Gamma(\nu, \nu_i) \end{aligned} \tag{43}$$

where:

- $\mathbb{E}[\boldsymbol{Y}]$ and $\mathbb{E}[\boldsymbol{Y}|X_i]$ are, respectively, the expected value of $\boldsymbol{Y}$ and the conditional expected value of $\boldsymbol{Y}$ given X_i. The term $\|\mathbb{E}[\boldsymbol{Y}] - \mathbb{E}[\boldsymbol{Y}|X_i]\|^2$ quantifies the contribution due to the difference in the marginal and conditional expected values of $\boldsymbol{Y}$.
- $\Sigma_{\boldsymbol{Y}}$ and $\Sigma_{\boldsymbol{Y}|X_i}$ are the corresponding variance-covariance matrices, and the matrix trace term (i.e., $Tr\left(\Sigma_{\boldsymbol{Y}} + \Sigma_{\boldsymbol{Y}|X_i} - 2\Sigma_{\boldsymbol{Y}}^{1/2}\Sigma_{\boldsymbol{Y}|X_i}\Sigma_{\boldsymbol{Y}}^{1/2}\right)$) quantifies the difference in the second-order (covariance) structure.

- The term $\Gamma(\nu, \nu_i)$ quantifies the difference in the two distributions due to the effect of higher-order moments. $\Gamma(\nu, \nu_i)$ becomes null if ν and ν_i are two distributions belonging to the elliptical distribution family with the same characteristic generator (Gelbrich, 1990). This is the case when both the marginal and the conditional distribution of $\boldsymbol{Y}$ are Gaussian.

The work of (Borgonovo et al., 2024) defines the following global sensitivity measure based on the square 2-Wasserstain distance:

$$i(\boldsymbol{Y}, X_i) = \frac{\mathbb{E}\left[W_2^2\left(\mathbb{P}_{\boldsymbol{Y}}, \mathbb{P}_{\boldsymbol{Y}|X_i}\right)\right]}{2\mathbb{V}[\boldsymbol{Y}]}, \tag{44}$$

where $\mathbb{V}[\boldsymbol{Y}]$ is the variance of $\boldsymbol{Y}$, which, in a multivariate context, is the sum of the univariate variances of the outputs, that is, $\mathbb{V}[\boldsymbol{Y}] = \sum_{o=1}^{O} \mathbb{V}[Y_o]$. The global sensitivity index $i(\boldsymbol{Y}, X_i)$ possesses relevant properties (Borgonovo et al., 2024), whose importance is highlighted in recent statistical literature (Chatterjee, 2021):

- zero-independence: $i(\boldsymbol{Y}, X_i) = 0$ if and only if $\boldsymbol{Y}$ and X_i are statistically independent, ensuring that no important input is wrongly neglected in the analysis;
- max-functionality: $i(\boldsymbol{Y}, X_i) = 1$ if and only if $\boldsymbol{Y}$ is functionally dependent on X_i;
- monotonicity: $i(\boldsymbol{Y}, X_i)$ decreases if less refined information on X_i is received.

Zero-independence reassures us that if $i(\boldsymbol{Y}, X_i)$ is null then $\boldsymbol{Y}$ and X_i are statistically independent, that is, when fixing X_i does not change the distribution of $\boldsymbol{Y}$. Variance-based GSA methods do not satisfy this condition, because it may occur that $\boldsymbol{Y}$ and X_i are statistically dependent even if the value of the variance-based sensitivity measure is zero (see Ishlg-Ami & Homma, 1990). The max-functionality property looks at the maximum value of $\boldsymbol{Y}$ and guarantees that $i(\boldsymbol{Y}, X_i) = 1$ if and only if $\boldsymbol{Y}$ is functionally dependent only on X_i (i.e., $\boldsymbol{Y}$ is completely determined by fixing X_i). This gives the following interpretation of the values of $i(\boldsymbol{Y}, X_i)$: $0 \leq i(\boldsymbol{Y}, X_i) \leq 1$, with zero achieved when $\boldsymbol{Y}$ is not (statistically) affected by X_i and it is maximal if X_i determines $\boldsymbol{Y}$ completely. This allows a straightforward interpretation of the value of $i(\boldsymbol{Y}, X_i)$ and a transparent way to rank the inputs. Also, $i(\boldsymbol{Y}, X_i)$ is well-defined and interpretable even when the inputs are correlated. This is because it does not rely on decomposing the output variance into contributions of independent inputs, but rather it quantifies how much the distribution of $\boldsymbol{Y}$ changes given X_i.

Formally, the index in Eq. (44) is a moment-independent sensitivity measure, because it measures the separation between two distributions without any reference to its moments. However, the decomposition in Eq. (43) allows us to connect the moment independent index to contributions related to the expected impact of fixing X_i on the variance and higher order moments of $\boldsymbol{Y}$. Substituting the decomposition in Eq. (43) into Eq. (44) yields:

$$i(\boldsymbol{Y}, X_i) = i^{VB}(\boldsymbol{Y}, X_i) + i^{\Sigma}(\boldsymbol{Y}, X_i) + \frac{\mathbb{E}\left[\Gamma\left[\mathbb{P}_{\boldsymbol{Y}}, \mathbb{P}_{\boldsymbol{Y}|X_i}\right]\right]}{2\mathbb{V}[\boldsymbol{Y}]}, \tag{45}$$

where

$$i^{VB}(\boldsymbol{Y}, X_i) = \frac{\mathbb{E}[\|\mathbb{E}[\boldsymbol{Y}] - \mathbb{E}[\boldsymbol{Y}|X_i]\|^2]}{2\mathbb{V}[\boldsymbol{Y}]} = \frac{\sum_{o=1}^{O} S(Y_o, X_i)}{2}, \tag{46}$$

and

$$i^{\Sigma}(\boldsymbol{Y}, X_i) = \frac{\mathbb{E}\left[Tr\left(\left(\Sigma_{\boldsymbol{Y}} + \Sigma_{\boldsymbol{Y}|X_i} - 2\left(\Sigma_{\boldsymbol{Y}|X_i}^{\frac{1}{2}} \Sigma_{\boldsymbol{Y}} \Sigma_{\boldsymbol{Y}|X_i}^{\frac{1}{2}}\right)^{\frac{1}{2}}\right)\right)\right]}{2\mathbb{V}[\boldsymbol{Y}]} \tag{47}$$

The term $i^{VB}(\boldsymbol{Y}, X_i)$ is the sum of the variance-based indices of X_i to all outputs: thus, it accounts for the impact of X_i on the model outputs variance. The term $i^{\Sigma}(\boldsymbol{Y}, X_i)$ is the expected impact on the variance-covariance matrix of the output $\boldsymbol{Y}$, and the last term in Eq. (47) is the residual error term that contains the contribution to higher-order moments. Thus, $i(\boldsymbol{Y}, X_i)$ subsumes variance-based sensitivity indices. For this reason, summing $i(\boldsymbol{Y}, X_i)$ does not yield a value of 1, because also higher order contributions are included in its value.

A detailed description of the available given-data procedures to estimate $i(\boldsymbol{Y}, X_i)$ can be found in (Borgonovo et al., 2024). We note here that the suggested approach is based on a given-data strategy that allows one to obtain the estimates directly from the dataset provided for a Monte Carlo uncertainty quantification, performing the following steps, also shown in the flowchart of **Fig. 43**, for each input X_i:

1. sort the values of X_i in ascending order;
2. divide the sorted values of X_i into $h = 1,2, \dots, H$ intervals;
3. for each *h-th* interval, compute the optimal transport problem between the original data $\boldsymbol{Y}$ and the subset data $\boldsymbol{Y}_h$ corresponding to the selected interval, as follows:
    a. if $\boldsymbol{Y}$ is univariate, the solution is exact and computationally efficient. The corresponding algorithm is based on sorting (Borgonovo et al., 2024; Vallender, 1974);
    b. if $\boldsymbol{Y}$ is multivariate, the OT problem can be solved exactly using the simplex algorithm or anKuhn, 1956; Luenberger & Ye, 2021uhn, 1956; Luenberger & Ye, 2021);
    c. if $\boldsymbol{Y}$ is multivariate and the number of available simulations is large, the OT problem can be solved approximately with the Sinkhorn algorithm, which is used in this paper. Such algorithm notably reduces the

computational burden and makes the estimation feasible also for complex simulators (Cuturi, 2013);

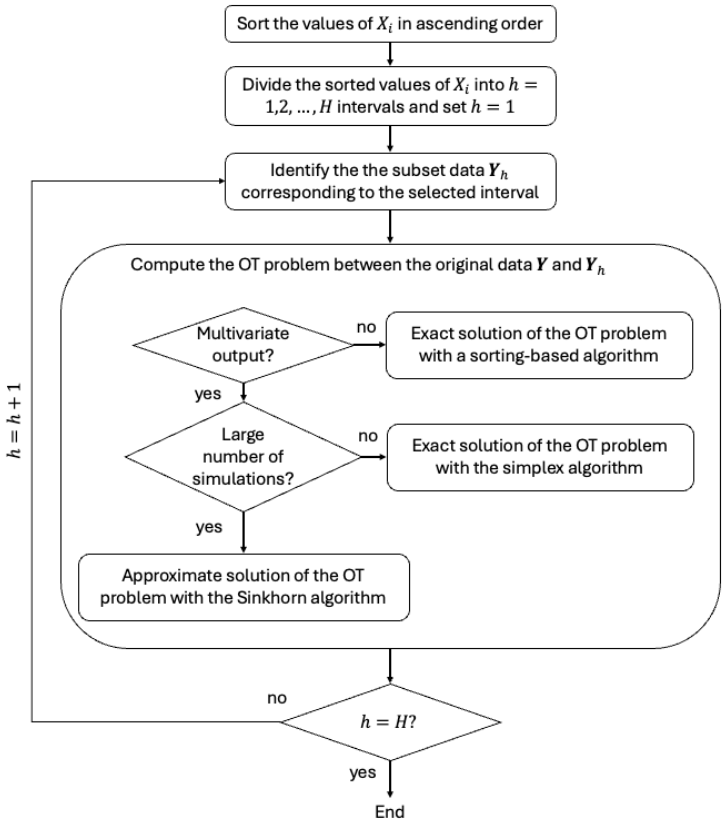


Figure 43. Flowchart of the given-data procedure to estimate $i(\boldsymbol{Y}, X_i)$.

4.3.3 CUSUNORO-based graphical visualization tool

Let π denote a permutation that sorts the observed values of the *i-th* input X_i in ascending order, so that $x_{i,\pi(k)} \leq x_{i,\pi(k+1)}$, for all $k = 1,2,\dots,K-1$, where K is the number of observations for X_i. The CUSUNORO index, which has been introduced in (Plischke, 2012), with respect to the *i-th* input and the *o-th* output is defined as follows:

$$z_o(i) = \frac{1}{\sqrt{I \cdot \sum_{k=1}^{K} \left(y_{o,k} - \overline{y_o}\right)^2}} \cdot \sum_{l=1}^{k} \left(\overline{y_o} - y_{o,\pi(l)}\right) \tag{48}$$

where $\overline{y_o}$ is the expected value of the *o-th* output. Sorting the output values $y_{o,\pi(l)}$ according to the sorted inputs and computing the cumulative sum of deviations from $\overline{y_o}$, $z_o(i)$ provides insights on the trend of the *o-th* output values due to with variations in the *i-th* input. A large cumulative sum $\sum_{l=1}^{k}\left(\overline{y_o} - y_{o,\pi(l)}\right)$ indicates a strong influence of the *i-th* input on the *o-th* output, while fluctuations around zero mean weak or no influence. The resulting CUSUNORO plot, which plots $z_o(i)$ against the reordered input $x_{i,\pi(k)}$, helps to catch the trend visually. The following insights can also be drawn from a generic *i-th* CUSUNORO curve:

- sign of input-output dependency: if $z_o(i) > 0$, Y_o is directly proportional to X_i, if $z_o(i) < 0$, Y_o is inversely proportional to X_i, and if $z_o(i)$ crosses the horizontal axis multiple times, the dependency is non-monotonic;
- type of monotonic input-output dependency: the dependency is linear if the maximum absolute value of $z_o(i)$ occurs at the median of X_i, and nonlinear the further the maximum value from the median of X_i.

In case of monotonic nonlinear dependencies, the CUSUNORO plot can provide useful insights on the regions of large output sensitivity to inputs variations by highlighting, for each *i-th* input and *o-th* output, the corresponding critical input value $x_{i,crit}^{o}$, i.e., the value providing the maximum absolute value of $z_o(i)$, above (or below) which Y_o shows a highly nonlinear growth (decrease), which may cause the system to quickly approach the CR. We use Probabilistic Safety Margins (PSMs) to evaluate, in probabilistic terms, to which extent the outputs $\boldsymbol{Y}$ are below the thresholds $\boldsymbol{y}_{thres}$ (i.e., how far the system is from the CR) (Di Maio, Scapinello, Zio, Ciarapica, et al., 2021); this is done by estimating, for each *o-th* output, the γ-percentile of its distribution (i.e., $y_{\gamma,o}$) and calculating the PSM as (Di Maio et al., 2016):

$$PSM_o = \begin{cases} \dfrac{y_{thres,o} - y_{\gamma,o}}{y_{thres,o} - y_{nom,o}} & if\ y_{\gamma,o} \leq y_{thres,o} \\ 0 & if\ y_{\gamma,o} > y_{thres,o} \\ 1 & if\ y_{\gamma,o} < y_{nom,o} \end{cases} \tag{49}$$

where $y_{nom,o}$ is the nominal value of Y_o. The design improvements should, then, aim at maximizing the PSM_o, ensuring that X_i remains below (or above) $x_{i,crit}^{o}$ to prevent the nonlinear growth of Y_o, which would lead to a rapid decrease of PSM_o.

4.3.4 The proposed GSA framework

In this Section, we discuss the workflow of the methodology proposed in the paper. Let us consider a multivariate simulation model $\boldsymbol{Y} = m(\boldsymbol{X})$ of a safety-critical system, for which a dataset of N_{sim} simulations is assumed to be available. The system design should ensure that the SMR operates away from the region of input values that lead to failure, i.e., the Critical Region $CR = \{\boldsymbol{x} \in D_{\boldsymbol{X}} \subset \mathbb{R}^I : \boldsymbol{y} = m(\boldsymbol{x}) \geq \boldsymbol{y}_{thres}\}$, where $\boldsymbol{y}_{thres} = [y_{thres,1}, y_{thres,2}, \dots, y_{thres,O}] \in D_{\boldsymbol{Y}} \subset \mathbb{R}^O$ is the vector of output thresholds that, if exceeded, lead the system into a failure state (Puppo et al., 2021), and, thus, are typically defined by regulatory requirements or engineering safety standards. The proposed GSA framework consists of the following steps, also shown in the flowchart of **Fig. 44**:

- parameter prioritization by OT-based GSA; we identify the parameters that impact the SMR safety the most (i.e., the sub-vector $\boldsymbol{X}^* = [X_1^*, X_2^*, \dots, X_{I^*}^*]$ of the I^* (with $I^* < I$) inputs with the largest values of $i(\boldsymbol{Y}, X_i)$);

- critical parameters segmentation of the most important inputs by CUSUNORO, to identify the input critical values $\boldsymbol{x}_{crit} = [x_{crit,1}, x_{crit,2}, \dots, x_{crit,I^*}]$;
- identification of suitable design improvements to keep $\boldsymbol{X}^*$ far away from $\boldsymbol{x}_{crit}$.

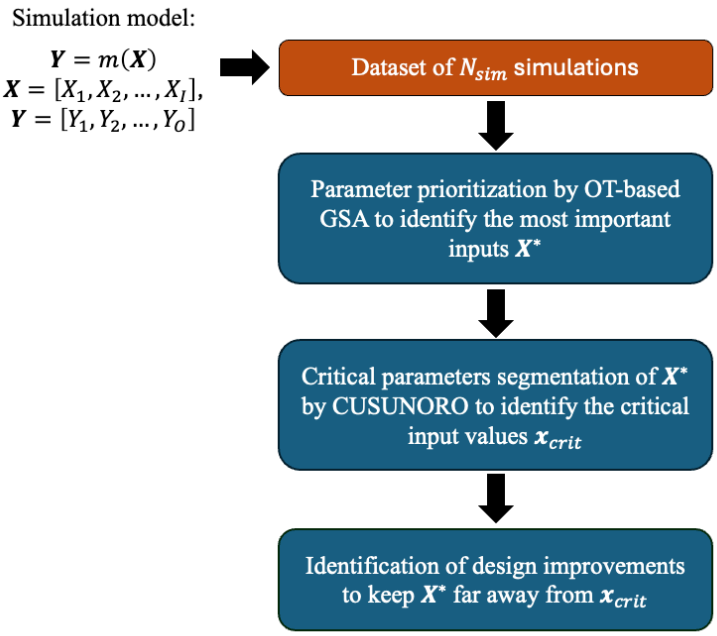


Figure 44. Flowchart of the proposed GSA framework.

To illustrate the proposed framework, we consider the following analytic model:

$$(Y_1, Y_2) = m(X_1, X_2, X_3), \text{ with}$$
$$\begin{cases} Y_1 = -1.5\sqrt[5]{X_1} + X_2^4 + 0.01X_3 \\ Y_2 = X_1^2 + 2X_2 - 0.5X_3 \end{cases} \quad (50)$$

where $X_i \sim U(0,1)$. We select this example for the ease of interpretation, although it has no direct reference to a nuclear system. We assume that the analyst has performed an uncertainty quantification and has available an input-output dataset of $N_{sim} = 10^4$ simulations. The procedure described in Section 4.3.2 is used to estimate $i(\boldsymbol{Y}, X_i)$. The results are reported in **Fig. 45**.

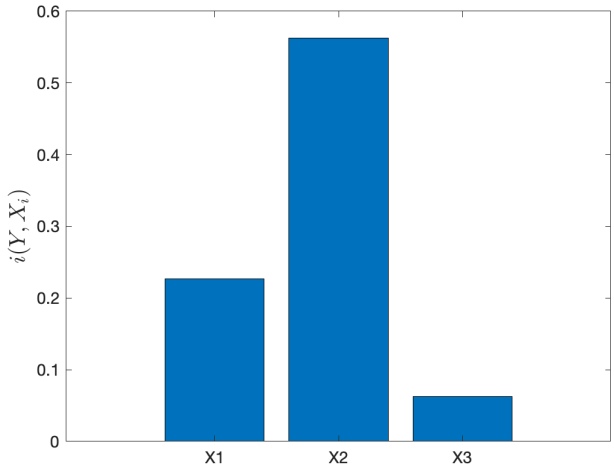


Figure 45. OT results for the analytic function in Eq. (50).

Fig. 45 shows that X_2 is the most relevant input, followed by X_1 and with X_3 playing a minor role. The design improvements of a system modelled by Eq. (50), whose parameters are X_1, X_2 and X_3, should, thus, focus on X_2 and X_1 rather than X_3.

For the sake of brevity, in what follows we only consider the first output (i.e., Y_1) with $y_{thres,1} = 0.2$, $y_{nom,1} = -1.25$ and $\gamma = 95$, leading to $PSM_Y = 0.40$. Then, following the insights provided by the OT-based parameter prioritization, $z_o(i)$ is calculated with Eq. (48) only for X_1 and X_2, and the corresponding CUSUNORO curves are plotted against their empirical Cumulative Distribution Function (CDF) (i.e., CDF_i $i = 1,2$) in **Fig. 46** and **Fig. 47**, respectively; analyzing the curves, the following considerations can be drawn:

- the dependence of Y_1 on X_1 is inverse (i.e., larger values of X_1 correspond to lower values of Y_1) and nonlinear, since its CUSUNORO curve (**Fig. 46**) is always negative and its maximum absolute value is skewed from the median of X_1 (i.e., $CDF_1 = 0.5$). The critical value for X_1 is $x_{crit,1} = 0.43$ (vertical line in **Fig. 46**);
- the dependence of Y_1 on X_2 is direct and nonlinear, since its CUSUNORO curve (**Fig. 47**) is always positive and its maximum absolute value is skewed from the median of X_2 (i.e., $CDF_2 = 0.5$). The critical value for X_2 is $x_{crit,2} = 0.68$ (vertical line in **Fig. 47**);

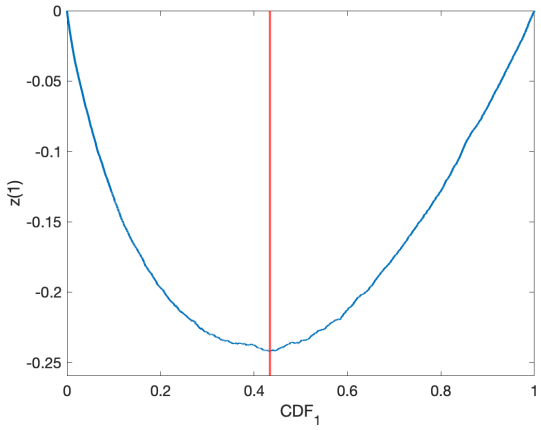


Figure 46. CUSUNORO curve and critical value for X_1.

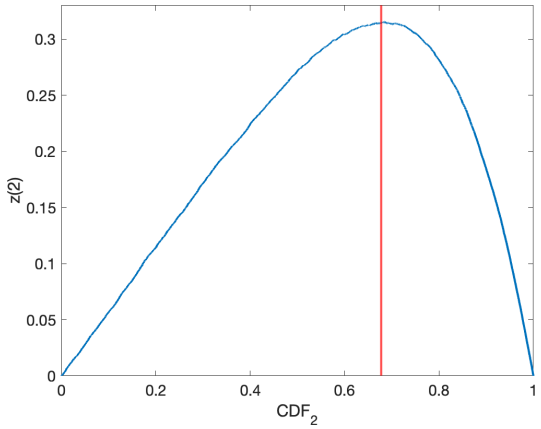


Figure 47. CUSUNORO curve and critical value for X_2.

The critical values $x_{crit,1}$ and $x_{crit,2}$ provide insights on how the most relevant inputs should be constrained. To show this, PSM_Y is calculated considering different constraints on the minimum value of X_1 (due to the inverse dependency) and on the maximum value of X_2 (due to the direct dependency). This demonstrative analysis is feasible thanks to the very low computational cost of evaluating the analytic model of Eq. (50) and to the limited number of inputs. **Fig. 48** shows PSM_Y plotted against the minimum value of X_1 and the maximum value of X_2. By limiting X_1 and X_2 to their critical values (i.e., $X_1 \sim U(x_{crit,1}, 1)$ and $X_2 \sim U(0, x_{crit,2})$), the PSM is improved to $PSM_Y^* = 0.94$, which lies outside the region of rapid decrease in the PSM (i.e., the region characterized by closely spaced contour lines, where small changes in inputs cause significant changes in the PSM). It is important to note that for dependent inputs, it is necessary to truncate the support of the joint distribution to preserve dependencies, rather than truncating marginal supports independently. These insights can enable targeted and tailored design improvements, avoiding resorting to a computationally burdensome trial-and-error procedure, which would be unfeasible for the complex long running best-estimate SMR simulation models.

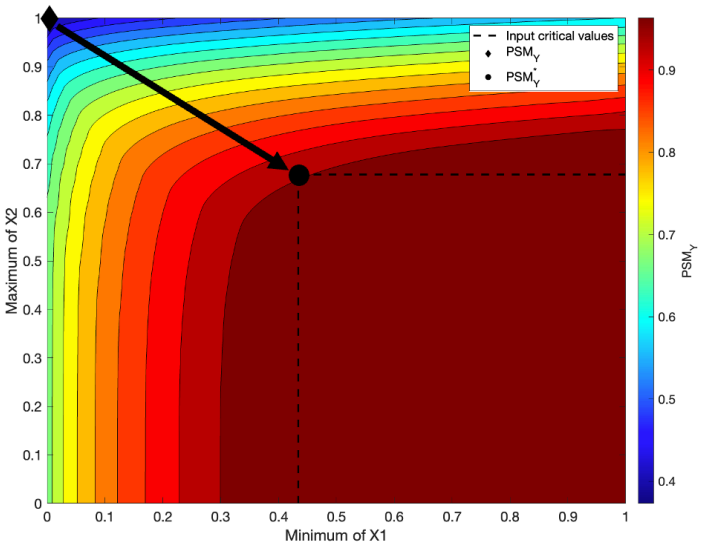


Figure 48. PSM_Y as a function of the minimum value of X_1 and maximum value of X_2.

4.4 Case study

We consider a MU-NPP composed by $N = 4$ units of SMDFRs, the same as in (Huke et al., 2015). A single unit of SMDFR is shown in **Fig. 49**. In this reactor design, the liquid fuel is a mixture of uranium tetrachloride and plutonium tetrachloride, which enters the core vessel at the bottom and spreads through a system of vertical tubes for the heat transfer before leaving the reactor from the top to enter the Pyrochemical Processing Unit (PPU). The liquid coolant is pure lead and enters the core vessel from the bottom to remove the heat from the fuel tubes by conduction before leaving the vessel from the top to enter the heat exchanger. We assume a 60-year design lifetime as in (Una et al., 2024).

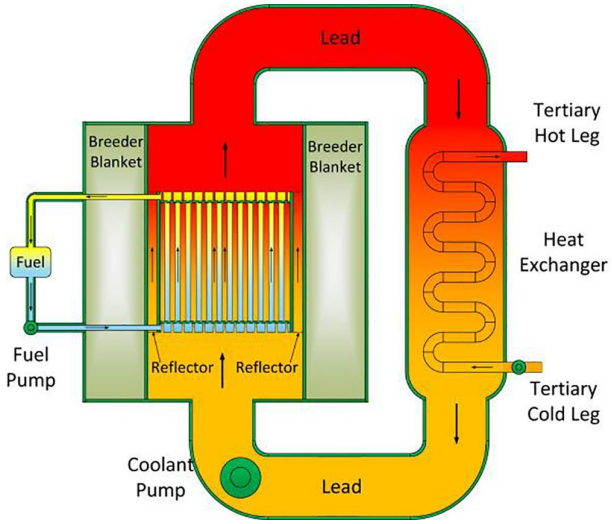


Figure 49. Sketch of the SMDFR (M. Wang et al., 2021).

The design parameters of the SMDFRs are reported in **Tab. 20**.

Table 20. Design parameters of the SMDFR (C. Liu et al., 2021).

Parameter	Value
Core zone $D\ x\ H$ [m]	$0.95\ x\ 2.0$
Distribution zone $D\ x\ H$ [m]	$0.95\ x\ 0.2$
Collection zone $D\ x\ H$ [m]	$0.95\ x\ 0.2$
Height of the core [m]	2.4
Outer reflector diameter [m]	1.25
Tank $D\ x\ H$ [m]	$1.65\ x\ 3.4$
Number of fuel tubes	1027
Fuel pin pitch [m]	0.025
Outer/interior fuel tube diameter [m]	0.008/0.007
Outer/interior coolant tube diameter [m]	0.005/0.004
Mean linear power density [W/cm]	609
Fuel inlet temperature [K]	1300
Coolant inlet temperature [K]	973
Nominal peak cladding temperature [K], $T_{w,nom}$	1150
Fuel inlet velocity [m/s]	3
Coolant inlet velocity [m/s]	5

4.4.1 Hazard and system characterization

We assume that the system can be exposed to an earthquake with $PGA \in [0, 19.62] \frac{m}{s^2}$. The magnitude-frequency curve, whose CDF is used to calculate the failure probability of the system safety features to a random PGA, is taken from (Shahraki & Shabakhty, 2015), without any specific reference to the case herein presented, and shown in **Fig. 50**. It is important to note that the the magnitude-frequency curve adopted does not refer to any site-specific seismic design basis safety assessment, but it is used, without loss of generality, for the seismic hazard characterization of a hypothetical SMDFR site.

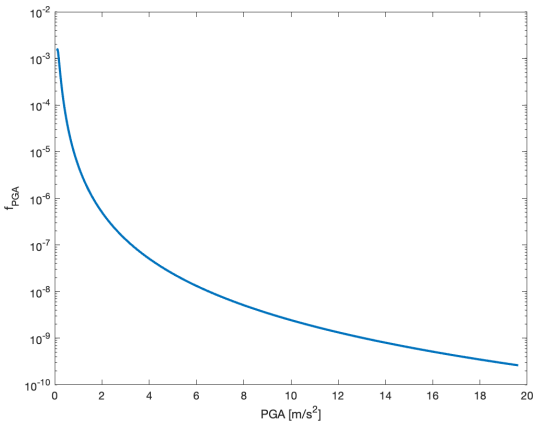


Figure 50. Earthquake magnitude-frequency curve.

For illustrative purposes, we assume that, if the earthquake occurrence leads to a LOCA, the coolant leak flow rate $\dot{m}_{leak}$ is independent of the PGA value and the LOCA

occurs at the outlet of the coolant pump. **Fig. 51** shows the leak flow rate as a function of time: the initial value is equal to the coolant flow rate in normal operating conditions, while the shape of the decrease of $\dot{m}_{leak}$ mimics the LOCA behavior in conventional Light Water Reactors (LWRs) (Park et al., 2021). This assumption is made because of the lack of specific data for LOCAs in SMDFRs.

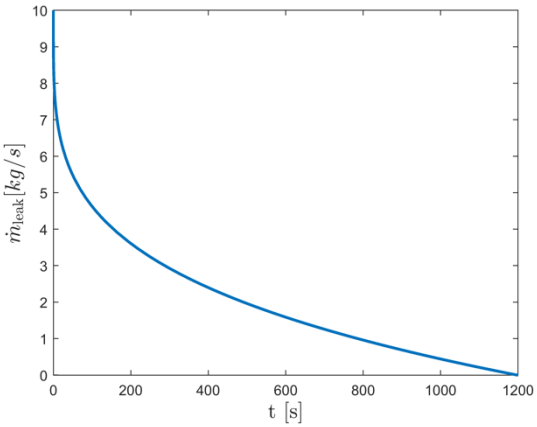


Figure 51. LOCA leak flow rate.

To prevent the occurrence of a LOCA, the NPP is equipped with stainless steel CPs. Furthermore, for mitigation of the consequences of a LOCA, the NPP is equipped with four ACSs (one for each unit, with a modular piping system that allows sharing the flow among all units, while guaranteeing that each ACS can perform its safety function independently from the others, in line with the design criteria of the Nuclear Regulatory Commission (NRC) (Nuclear Regulatory Commission (NRC), 2011), two EDGs (shared among all units, with each EDG being capable of providing power to all ACSs in case of LOP (Willis, 1993), and four Melting Fuel Plugs (MFPs) (one for each reactor), which are sections of molten salt designed to remain solid in normal operating conditions and to melt in case of a fuel temperature increase (Huke et al., 2015) (**Tab.21**).

Table 21. Safety features employed in the system.

Safety Feature	Classification	Description
Coolant Pipes (CP)	Passive, Preventive	Liquid lead containment
Auxiliary Cooling System (ACS)	Active, Mitigative	Auxiliary coolant delivery in case of LOCA
Emergency Diesel Generator (EDG)	Active, Mitigative	Independent source of power in case of LOP
Melting Fuel Plug (MFP)	Passive, Mitigative	Drains the fuel from the reactor in case of accident

The considered $s = 1,2,\dots,S$ safety features are actuated on demand with an uncertain response time t_s^r (**Tab. 22**, second column) and maintained each $\Delta t_{m,s}$ (**Tab. 22**, third column). The value of $\Delta t_{m,ACS}$ is assumed equal to that of an Auxiliary Feedwater System (AFS) of a typical LWR (Volkanovski & Cizelj, 2014); furthermore,

$\Delta t_{m,CP}$ is necessarily synchronous to the periodic drainage of coolant and fuel from the reactor. No maintenance is considered for the MFP, which is assumed to be always available. Also, the maintenance is assumed to be perfect: safety features are restored to an As Good As New (AGAN) state upon maintenance.

Table 22. Response times and maintenance schedule of the safety features.

Safety Feature	$\boldsymbol{t_s^r}$	$\boldsymbol{\Delta t_{m,s}}$
Coolant Pipes (CP)	$t_{r,CP} = 0$	$3\ y$
Auxiliary Cooling System (ACS)	$t_{r,ACS} \sim U[30,60]\ s$ (United States Nuclear Regulatory Comn	$0.5\ y$ (Volkanovski & Cizelj, 2014)
Emergency Diesel Generator (EDG)	$t_{r,EDG} \sim \mathrm{U}[60,300]$ s *(Lim et al., 2007)*	$1.5\ y$ (United States Nuclear Regulatory Commission, 2011)
Melting Fuel Plug Huke et al., 2015; Ilham & Okawa, 2023; X. Wang, 2018ham & Okawa, 2023; X. Wang, 2018)	-	

The failure probabilities $P_{f,s}$, $P_{f,s}^I$ and $P_{f,s}^E$ are assessed as follows:

1. CP:

    a. $P_{f,CP}^I$ is assessed with a load strength model (Yang, 1996):

$$P_{f,CP}^I(\tau) = P(S_{CP} \leq L_{CP}(\tau)) \quad [51]$$

    where L_{CP} is the load, i.e., the depth of the water pitting corrosion on the pipes $d_{CP}^c(\tau)$, whose initial value $d_{in,CP}^c$ is assumed to follow a normal distribution $d_{in,CP}^c \sim N(1.59\ mm, 0.619\ mm)$ (W. Zhou, 2011), and S_{CP} is the strength, i.e., 80% of the thickness of the pipe. CP is considered failed if the pipe thickness is equal or lower than 20% of its initial value. The increase in d_{CP} is calculated using a corrosion rate $d_{r,CP}^c = 1.1 \frac{mm}{year}$ (Zhang, 2009). The resulting $P_{f,CP}^I$ is shown in **Fig. 52** as a function of age.

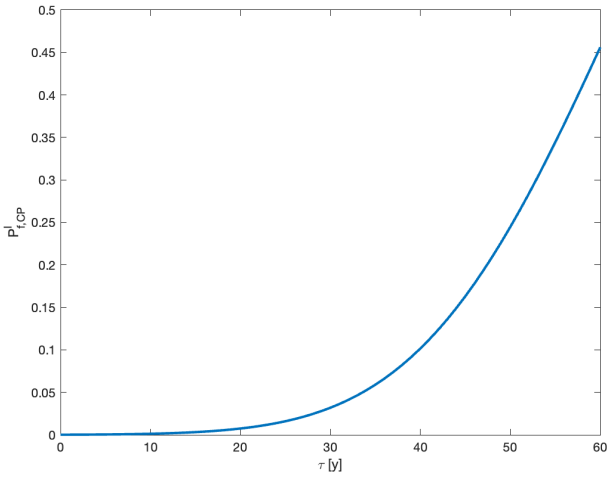


Figure 52. $P^{i}_{f,CP}$ as a function of age.

b. $P^{E}_{f,CP}$ is assessed with a fragility surface obtained integrating the fragility model from (Jeon et al., 2022) with the data from (U.S. Nuclear Regulatory Commission, 2005), which relates the seismic capacity to the thickness of the pipe, leading to the fragility surface of Eq. (52):

$$P^{E}_{f,CP}(PGA,\tau) = \phi\left[\frac{ln\left(R_{m,CP}(PGA)\right) - ln\left(C_{m,CP}(\tau)\right)}{\sqrt{\beta^{2}_{C_{CP}} + \beta^{2}_{R_{CP}}}}\right] \quad [52]$$

where $\phi[\cdot]$ is the cumulative distribution function of the standard normal distribution, $R_{m,CP}$ and $C_{m,CP}$ are the CP median structural seismic response and the age-dependent median seismic capacity, respectively, and $\beta_{R_{CP}} = 0.07$ and $\beta_{C_{CP}} = 0.14$ are the logarithmic standard deviations of R_{CP} and C_{CP}. The resulting fragility surface is shown in **Fig. 53**.

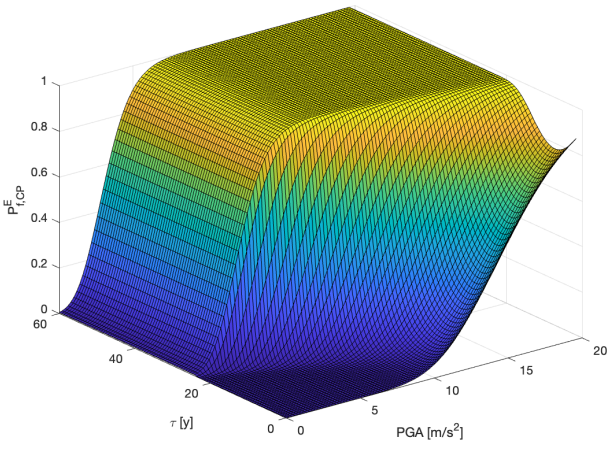


Figure 53. $P^{E}_{f,CP}$ as a function of age and PGA.

2. ACS:

a. $P^{I}_{f,ACS}$ is assessed with a load strength model:

$$P^I_{f,ACS}(\tau) = P(S_{ACS} \leq L_{ACS}(\tau)) \quad [53]$$

where L_{ACS} is the load, i.e., the depth of the water pitting corrosion on the pipes $d^c_{ACS}(\tau)$, whose initial value $d^c_{in,ACS}$ is assumed to follow the same normal distribution as $d^c_{in,CP}$, and S_{ACS} is the strength, i.e., 80% of the thickness of the pipe. The increase in d^c_{ACS} is calculated using a corrosion rate $d^c_{r,ACS} < d^c_{r,CP}$, since the liquid lead is not flowing inside the ECCS pipes. The decrease in corrosion rate due to the absence of flow is estimated following (Balbaud-Célérier & Barbier, 2001), leading to $d^c_{r,ACS} = 0.55 \frac{mm}{year}$ (Balbaud-Célérier & Barbier, 2001). $P^I_{f,ACS}$ is shown in **Fig. 54** as a function of age.

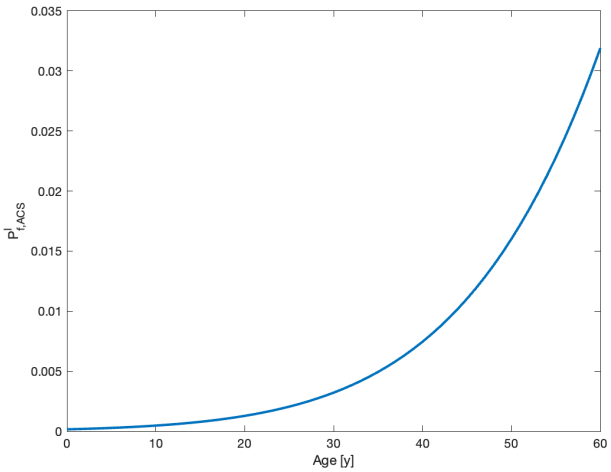


Figure 54. $P^i_{f,ACS}$ as a function of age.

b. $P^E_{f,ACS}$ is computed with Eq. (52), using the data in (U.S. Nuclear Regulatory Commission, 2005) together with $d^c_{r,ACS}$ to calculate the decrease in seismic capacity of ACS pipes, leading to the fragility surface shown in **Fig. 55**.

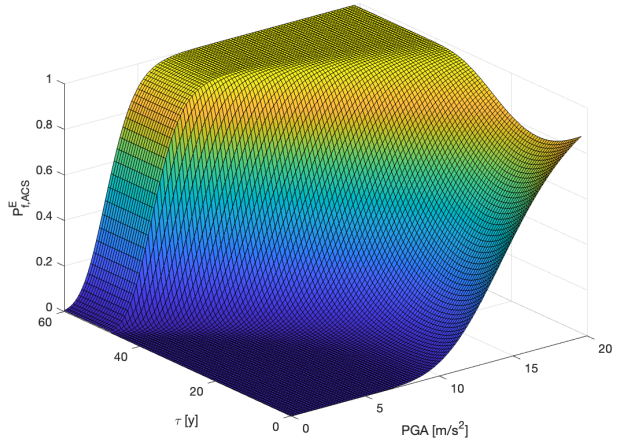


Figure 55. $P^E_{f,ACS}$ as a function of age and PGA.

3. EDG:

   a. the failure of EDG due to internal causes is assumed to be induced by its cooling pipes failure (Zhegang, 2022). $P^I_{f,EDG}$ is computed with a load-strength model:

$$P^I_{f,EDG}(\tau) = P(S_{EDG} \leq L_{EDG}(\tau)) \quad [54]$$

   where L_{EDG} is the load, i.e., the depth of the water pitting corrosion on the cooling pipes $d^c_{EDG}(\tau)$, whose initial value $d^c_{in,EDG}$ is assumed to follow the same normal distribution as $d^c_{in,CP}$, and S_{EDG} is the strength, i.e., 80% of the thickness of the pipe. The increase of $d^c_{EDG}(\tau)$ is calculated using the corrosion rates of **Tab. 23**. $P^I_{f,EDG}$ is shown in **Fig. 56** as a function of age.

Table 23. EDG corrosion rates (Van Der Schijff & Bodemann, n.d.).

Exposure time t_e $[days]$	$d^c_{r,EDG}[mm/y]$
$t_e \leq 497$	0.52
$497 < t_e \leq 759$	0.52
$759 < t_e \leq 780$	0.42
$780 < t_e \leq 1116$	0.43
$t_e \geq 1116$	0.42

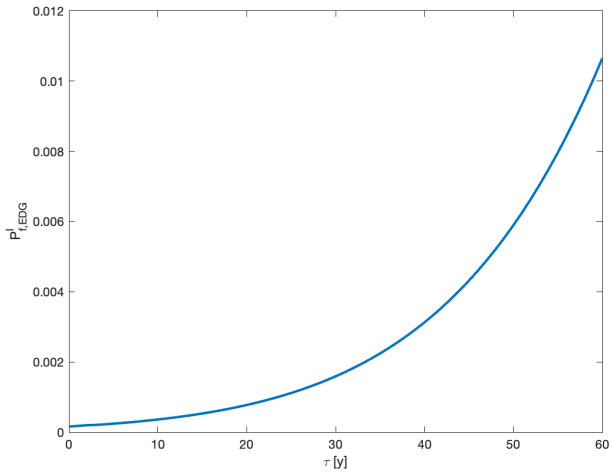


Figure 56. $P^I_{f,EDG}$ as a function of age.

b. $P^E_{f,EDG}$ is computed with a fragility surface obtained integrating the fragility model from (Y. Wang et al., 2017) with the seismic capacity degradation data from (U.S. Nuclear Regulatory Commission, 2005), leading to the fragility surface of Eq. (55):

$$P^E_{f,EDG}(PGA,\tau) = \phi\left[\frac{ln\left(\frac{PGA}{C_{m,EDG}}\right) + \beta_U \phi^{-1}(Q)}{\beta_R}\right] \quad [55]$$

where $C_{m,EDG}$ is the median seismic capacity of EDG, $Q = 0.95$ is the confidence level, $\beta_U = 0.26$ and $\beta_R = 0.24$. The resulting fragility surface is shown in **Fig. 57**.

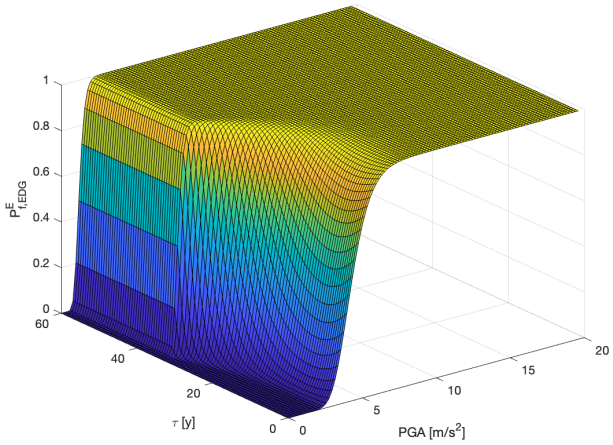


Figure 57. $P^e_{f,EDG}$ as a function of age and PGA.

Notice that a seismic event leading to the failure of CP, and therefore to a LOCA, would also likely cause the failure of the EDG, since $P^E_{f,EDG} \geq P^E_{f,CP}$ across all PGA values and system ages τ.

The inter-unit failure dependencies are accounted for by considering the possible CCFs among EDGs and ACSs as follows:

- To model the probabilities of occurrence of CCF events involving one or two EDGs, an alpha-factor model is developed, based on historical data (**Fig. 58** shows the count of CCF events for each sub-system of EDGs (Idaho National Engineering and Environmental Laboratory, 1999), an alpha-factor model is used (Mosleh, 1987):

$$P_{f,EDG}^{1} = \alpha_1 P_{f,EDG} \quad [56]$$

$$P_{f,EDG}^{2} = \alpha_2 P_{f,EDG} \quad [57]$$

where $P_{f,EDG}^{1}$ and $P_{f,EDG}^{2}$ are the probabilities that only one EDG fails and that both fail due to CCF, respectively, $\alpha_1 = 0.9881$ and $\alpha_2 = 0.0119$ (Kang et al., 2009).

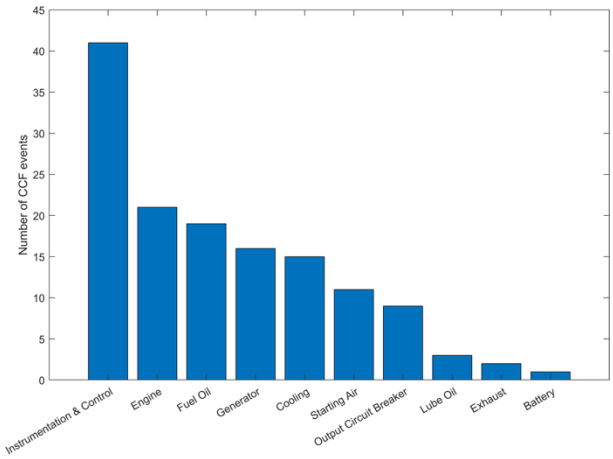


Figure 58. CCF events involving each EDG sub-system.

- Historical data on ACS are, instead, not available because of the SMDFR being a new design; the dependency evaluation tree of **Fig. 41** (Jang & Jae, 2020) is, thus, used to evaluate the dependency among the different ECCSs. We assume that the ACSs are HD among each other, since in the considered MUNPP they share the same design, maintenance team, operation mode, environment and a number of components. Therefore, the probability of the CCF combinations is calculated as (Jang & Jae, 2020):

$$P_{ACS,CCF}(n_{ACS}) = n_{ECCS} \cdot P_{f,ACS} \cdot \left(\frac{1 + P_{f,ACS}}{2}\right)^{n_{ACS}-1} \quad [58]$$

where n_{ACS} is the number of ACSs involved in the CCF group.

4.4.2 Monte Carlo-based integrated dynamic probabilistic model

The dynamic model developed (C. Liu et al., 2021) (see the brief description provided in **Appendix C**) simulates safe and accidental conditions transients that might occur

in the system. The Monte Carlo simulation takes as input the actual age of the system $\tau \in [0,60]\ y$ and proceeds as shown in **Fig. 59** to provide in output the peak cladding temperature $T_{w,i}(t)$ of each *i-th* reactor of the MUNPP over a time horizon $T_s = 1200\ s$, which is the time allowed to confirm that the drainage of the fuel from the reactor core through the melting fuel plug is successful (Huke et al., 2015; Ilham & Okawa, 2023; X. Wang, 2018), and thus the accident is successfully mitigated.

The threshold cladding temperature not to be exceeded during the accident is $T_{w,fail} = 1244\ K$, as results from the solution of Eq. (59) of the thermal stress on the fuel pipes:

$$\sigma_{th} = E\gamma(T)\Delta T \qquad [59]$$

where $E = 207\ GPa$ is the Young's Modulus of Nickel 201, which is the candidate material for Molten Salt Reactors (MSRs) (Young & Sham, 2018), $\gamma(T)$ is the temperature-dependent coefficient of thermal expansion (estimated interpolating the data in (Special Metals, n.d.) and ΔT is the resulting temperature change of the fuel pipes to the ultimate tensile strength of the pipe, $\sigma_{max} = \sigma_{UTS} = 345\ MPa$ ($\Delta T_{fail} = 94\ °C$ and $T_{w,fail} = T_{w,nom} + \Delta T_{fail} = 1244\ K$).

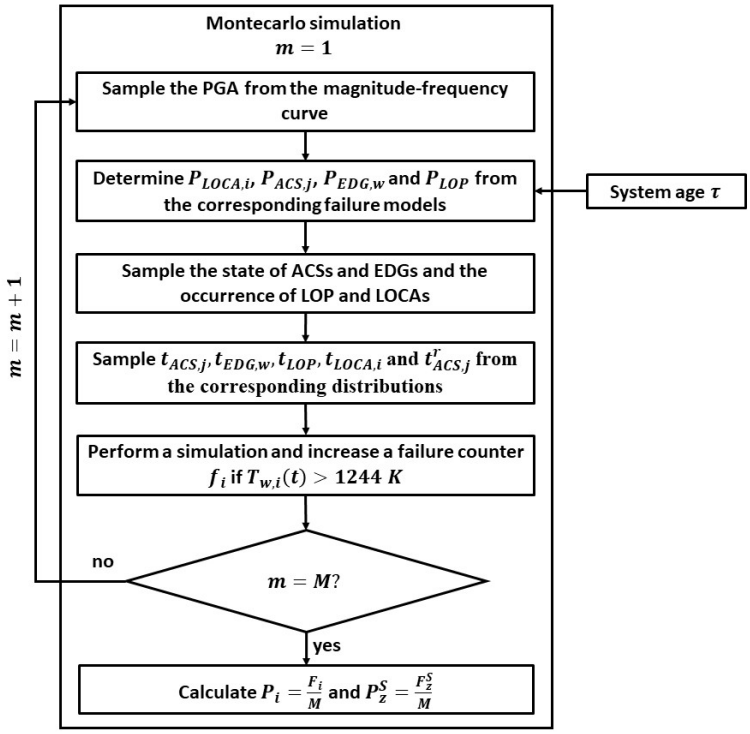


Figure 59. Monte Carlo simulation flowchart.

A Monte Carlo simulation of M trials is performed to calculate the failure probability P_i of each reactor and of group of reactors P_z^S (where $S = 1,2,3,4$ corresponds to the failure of one, two, three and four reactors, respectively), as follows:

1. the earthquake PGA is sampled from the magnitude-frequency curve (f_{PGA}) of the site;
2. τ and PGA are used to determine:

2.1. the probability of LOCA occurrence of each reactor $P_{LOCA,i} = P_{f,CP,i}$, as described in Section 4.4.1;

2.2. the failure probability of each ECCS $P_{f,ECCS,j}$, as described in Section 4.4.1;

2.3. the failure probability of each EDG $P_{f,EDG,w}$, as described in Section 4.4.1;

2.4. the probability of LOP P_{LOP}, assessed with the following fragility model (Ryu & Jae, 2021):

$$P_{LOP}(PGA) = \phi\left[\frac{ln\left(\frac{PGA}{A_{m,LOP}}\right) + \beta_{U,LOP}\phi^{-1}(Q)}{\beta_{R,LOP}}\right] \quad [60]$$

where $A_{m,LOP} = 0.2\ g$ is the time-dependent median ground acceleration capacity, Q is the confidence level, $\beta_{U,LOP} = 0.25$ and $\beta_{R,LOP} = 0.2$;

3. the probabilities determined in Step 2 and the CCF models of Section 4.4.1 are used to sample the state of ECCSs and EDGs, and the occurrence of LOP and LOCA;

4. the failure events occurrence times (i.e., $t^f_{ECCS,j}, t^f_{EDG,w}, t_{LOP}$ and $t_{LOCA,i}$) and the response times of each ECCS and each EDG (i.e., $t^r_{ECCS,j}$, $t^r_{EDG,w}$) are sampled from the corresponding distributions (**Tab. 24**);

5. the simulation of the dynamic model is performed and, for each *i-th* unit, the output values $T_{w,i}$ are obtained to determine whether the unit is failed or not. In **Fig. 60,** two examples of $T_{w,1}$ transients are shown: on the left, after the initial rise in temperature due to a LOCA at $t = 365\ s$, the activation of the ECCS around $t = 800\ s$ causes the temperature to decrease and, then, stabilize; on the right, the unmitigated rise in temperature due to a LOCA at $t = 50\ s$ leads to the reactor failure around $t = 700\ s$;

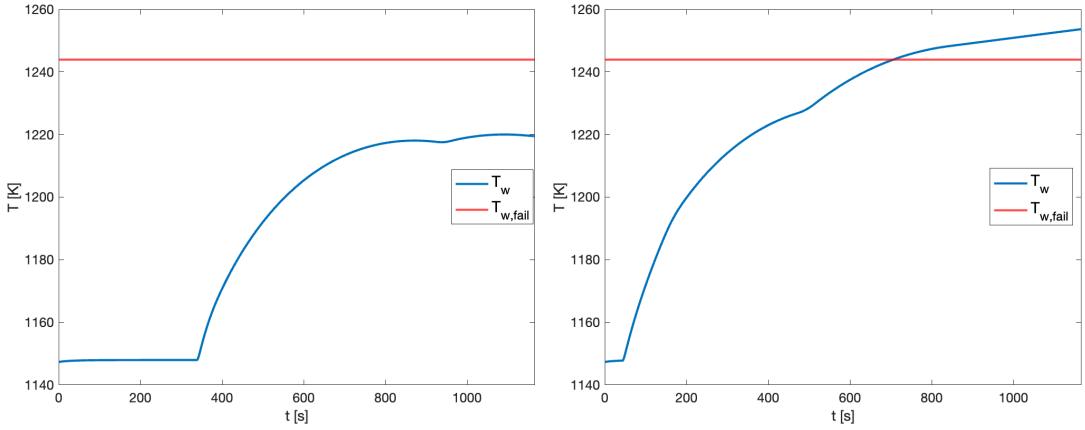


Figure 60. Example transients of $T_{w,1}$. On the left a safe transient and on the right a failed transient. The solid straight line indicates the failure threshold.

6. M trials are repeated from Step 1;

7. finally, P_i and P_z^S are calculated as follows:

$$P_i = \frac{F_i}{M} \quad [61]$$

$$P_z^S = \frac{F_z^S}{M} \quad [62]$$

where F_i is the number of simulations that lead to the failure of the *i-th* unit and F_z^S is the number of simulations that lead to the occurrence of the *z-th* scenario.

Table 24. Distributions of the uncertain model parameters.

Variable	Description	Distribution
PGA	Earthquake Peak Ground Acceleration $\left[\frac{m}{s^2}\right]$	$PGA \sim Frechet(2.31,\ 0.133)$ (Shahraki & Shabakhty, 2015)
Age	Age of the system $[y]$	$Age \sim U(0,60)$
$d_{in,CP}$	Initial depth of CP corrosion defect $[mm]$	$d_{in,C} \sim N(1.59,\ 0.619)$ (W. Zhou, 2011)
$d_{in,ACS}$	Initial depth of ACS corrosion defect $[mm]$	$d_{in,ACS} \sim N(1.59,\ 0.619)$ (W. Zhou, 2011)
$d_{in,EDG}^C$	Initial depth of EDG corrosion defect $[mm]$	$d_{in,EDG}^C \sim N(1.59,\ 0.619)$ (W. Zhou, 2011)
t_{ACS}^r	Response time of ACS $[s]$	$t_{ACS}^r \sim U(30,60)$ (United States Nuclear Regulat
t_{EDG}^r	Response time of EDG $[s]$	$t_{EDG}^r \sim U(60,300)$ *(Lim et al., 2007)*
t_{ACS}^f	Failure time of ACS $[s]$	$t_{ACS} \sim U(15, t_{sim})$, with mean value $t_{ACS}^{mean} = 607.5\ s$
t_{EDG}^f	Failure time of EDG $[s]$	$t_{EDG} \sim U(15, t_{sim})$, with mean value $t_{EDG}^{mean} = 607.5\ s$
t_{LOP}	Time of LOP [s]	$t_{LOP} \sim logN(3.30,1)\ s$
t_{LOCA}	Time of LOCA [s]	$t_{LOCA} \sim logN(3.30,1)\ s$

4.5 Results

4.5.1 Integrated Deterministic and Probabilistic Safety Assessment

The framework presented in Section 4.2 has been applied to the case study of Section 4.4. In **Fig. 61** and **Fig. 62**, we show the estimates of P_i and P_z^S, $z = 1,2,3,4$, respectively, at the end of the design life (i.e., at $\tau = 60\ y$) for the MUSMDFR, in comparison with the typical values of CDF of Gen-III LWRs (see (Ebisawa et al., 2015; Prasad et al., 2017) and of a MUNPP comprised of other SMRs (see (Di Maio, Bani, et al., 2023), when neither the degradation of safety features nor the contribution to the CDF of the sharing of safety features are considered.

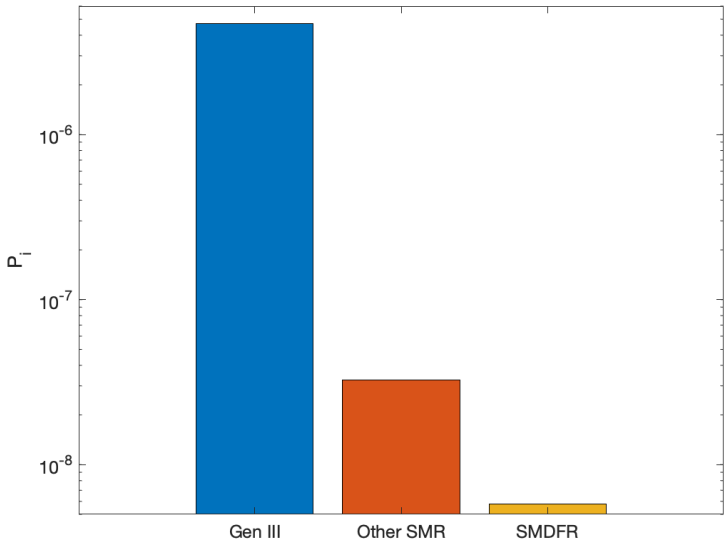


Figure 61. Comparison of P_i, neglecting safety features degradation.

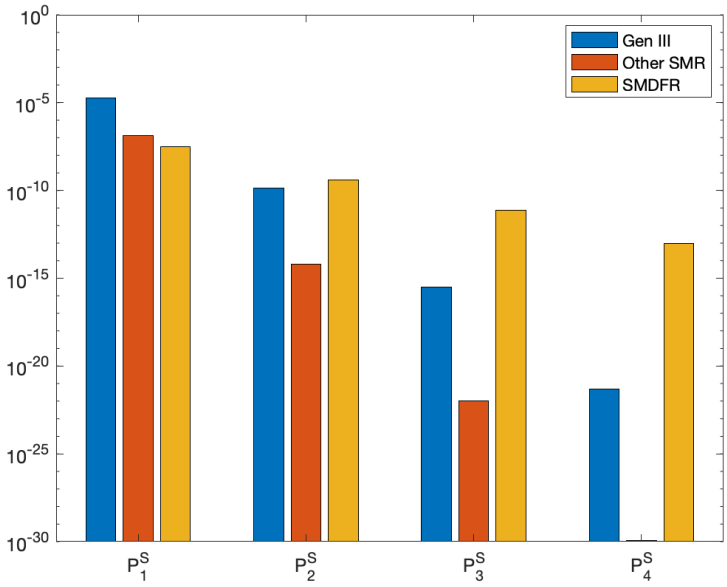


Figure 62. Comparison of P_z^S, neglecting safety features degradation.

As shown in **Fig. 61**, both MUSMRs and MUSMDFRs achieve failure probability values lower than the current threshold of acceptability (i.e., $P_{i,threshold} = 10^{-5}$ (M. Kumar et al., 2017), meaning that SMDFRs can be regarded as safe as other SMR designs (limited to LOCAs triggered by seismic events). On the other hand, **Fig. 62** highlights the importance of considering the sharing of safety features when conducting a MUPSA: whereas MUSMDFRs and MUSMRs have similar probabilities of single unit failure (i.e., P_1^S), the probabilities of multiple reactor failures (i.e., P_2^S, P_3^S and P_4^S) in MUSMDFRs are several orders of magnitude larger than those in MUSMRs; such difference is due to neglecting the effect of sharing safety features in the risk assessment of MUSMRs.

To show the impact of the safety features degradation on the MUSMDFRs risk assessment, in **Fig. 63** and **Fig. 64** we compare the values of P_i and P_z^S obtained

neglecting safety features degradation with the ones obtained considering degradation with models described in Section 4.4.1 and the maintenance schedule of **Tab. 22**, under two different assumptions:

1. Perfect maintenance (i.e., the safety features are restored As Good As New (AGAN) upon maintenance);

2. Imperfect maintenance (i.e., the degradation of the safety features is reduced but not eliminated by the maintenance intervention (Zanotelli et al., 2024). To do this, we use the imperfect maintenance model described in (Kijima, 1989; Kijima et al., 1988), which allows calculating the effective age of the maintained component as follows:

$$\tau_E^k = \tau_E^{k-1} + \beta \Delta t_m \quad [63]$$

where τ_E^k is the effective age immediately after the *k-th* maintenance intervention, $\beta \in [0,1]$ is the effectiveness of the maintenance intervention ($\beta = 0$ represents perfect maintenance, i.e. AGAN; $\beta = 1$ represents completely ineffective maintenance, i.e. As Good As Old (AGAO) and Δt_m is the time between two successive maintenance interventions. Without loss of generality, we assume $\beta = 0.1$.

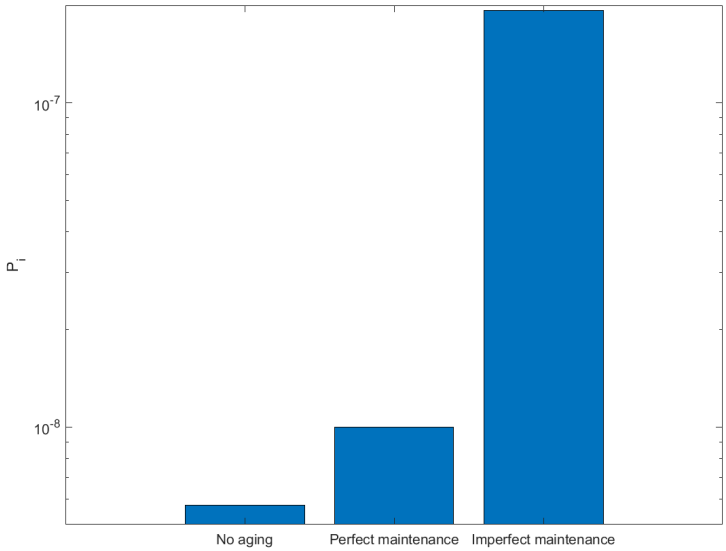


Figure 63. Results for P_i considering perfect and imperfect maintenance.

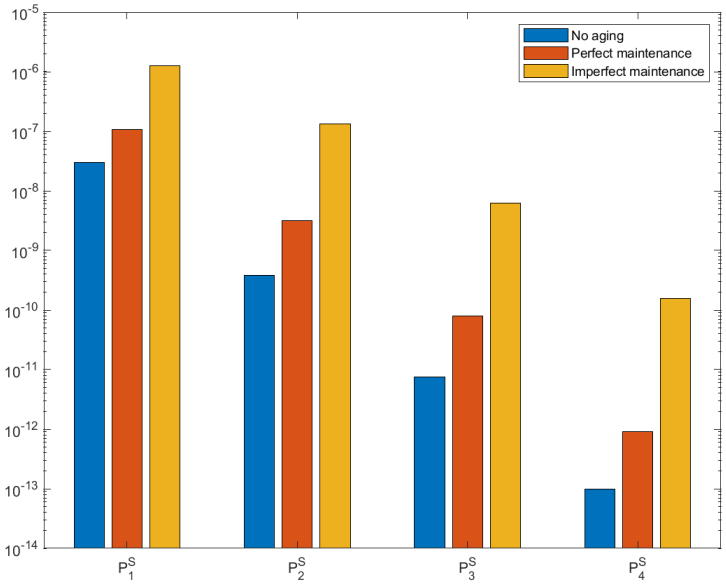


Figure 64. Results for P_z^S considering perfect and imperfect maintenance.

As expected, **Fig.63** and **Fig. 64** show that the degradation of the aging safety features leads to an increase in the failure probability of the reactors, especially in the case of imperfect maintenance. The causes of such increase are twofold: firstly, the employment of a highly corrosive coolant, and secondly the suboptimal maintenance strategy outlined in **Tab. 22**, which is based on typical maintenance schedules of existing nuclear reactors (for ECCS and EDG) and on expert-judgement (for CP). To further illustrate the impact of degradation under imperfect maintenance, **Fig. 65** shows the values of P_i at different system ages: a P_i increase is observed at 60 years of operation, emphasizing the importance of reviewing the system conditions, as customary, after the first 40 years of operation, prior to any decision regarding the extension of the system life to 60 years or beyond

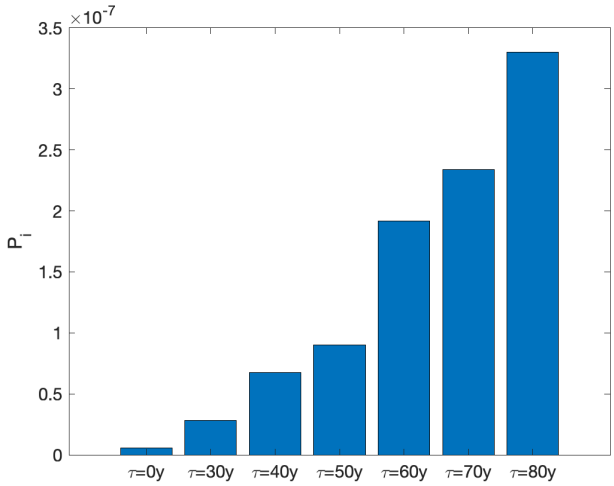


Figure 65. Values of P_i at different system ages considering imperfect maintenance.

The results presented highlight that neglecting the degradation of safety features leads to an underestimation of the risk and possibly to suboptimal decision making, especially in case of reactors employing highly corrosive coolants, such as the SMDFR.

4.5.2 Sensitivity Analysis: Results and Insights

The GSA framework presented in Section 4.3 is applied to the case study of Section 4.4. The available data consists of $N_{sim} = 10^4$ simulations of accidental scenarios (i.e., scenarios in which at least one of the reactors experiences a LOCA), generated in approximately $28h$ on a commercially available laptop with an AMD Ryzen 5 PRO 4650U processor. The total number of simulations (including those without a LOCA) is $N_{sim}^{total} = 10^7$. The median PGA for scenarios with only one LOCA is $PGA_{single}^{median} = 5.25\frac{m}{s^2}$, while for scenarios with multiple LOCAs it is $PGA_{multiple}^{median} = 14.27\frac{m}{s^2}$. The GSA is conducted considering the input parameters of **Tab. 24** and the output of interest is the maximum value of $T_{w,n}$ reached during the accidental scenario (i.e., $T_{w,max,n}$), for each *n-th* reactor unit.

4.5.2.1 Parameter prioritization

Fig. 66 shows the results of the parameter prioritization, where a dummy input (i.e., a fictitious input with no influence on the output) is added to facilitate the relative identification of uninfluential input parameters.

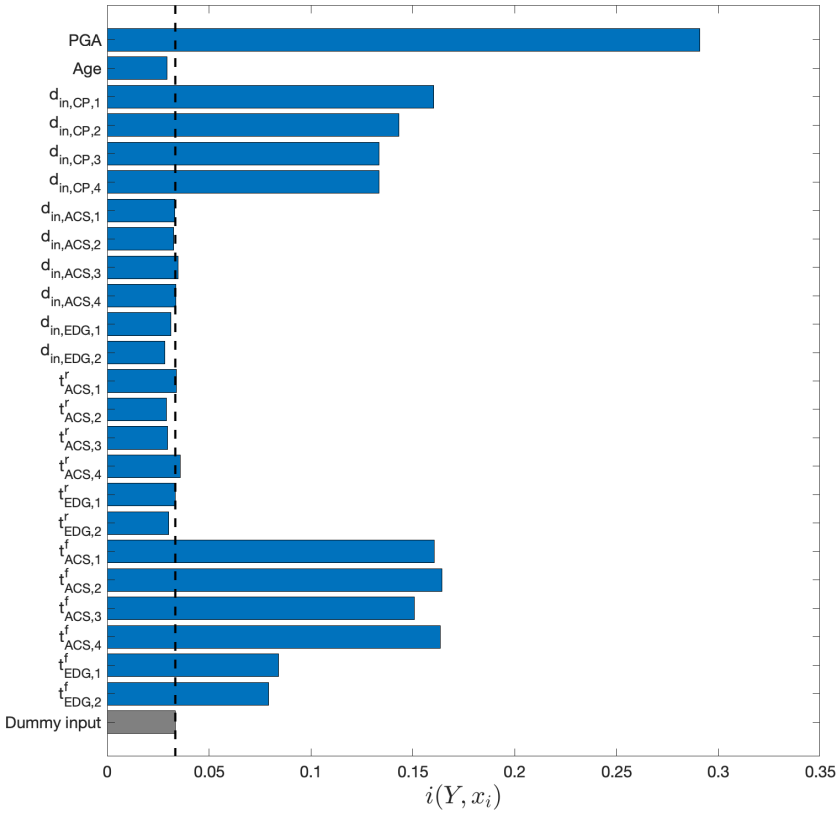


Figure 66. Parameter prioritization results.

The following considerations are made based on the parameter prioritization results:

- the PGA is the most important input; therefore, improvements should focus on anti-seismic measures;
- the failure times of the mitigative safety features (i.e., t^f_{ACS} and t^f_{EDG}) are more important that their response times (i.e., t^r_{ACS} and t^r_{EDG}); therefore, it is more beneficial to focus on improving the reliability of those safety features rather than their response speed;
- the initial depth of the corrosion defect of the CPs (i.e., $d_{in,CP}$) is among the most important inputs; therefore, an improvement to the CP resistance to corrosion can be beneficial for the system safety;
- the age of the system does not impact $T_{w,max}$ significantly; this is due to the "perfect" (AGAN) maintenance adopted for the system, which diminishes the impact of aging and degradation on the system safety.

Finally, we identify the most important inputs considering the hypothesis of perfect maintenance as the most realistic, leading to the identification of PGA, $d_{in,CP,n}$ and $t^f_{ACS,n}$ as the most important inputs.

To investigate the influence of the assumption of perfect maintenance, parameter prioritization has been reconsidered based on a set of $N_{sim,2} = 10^3$ simulated accidental scenarios with imperfect maintenance interventions (degradation of safety features only reduced and not completely eliminated) according to the same schedule of **Tab. 22**. The imperfect maintenance model adopted is the one described in (Kijima, 1989; Kijima et al., 1988), based on the calculation of the effective age of the maintained component:

$$\tau_E^q = \tau_E^{q-1} + \alpha \Delta t_m \tag{64}$$

where τ_E^q is the effective age immediately after the *q-th* maintenance intervention, α is the effectiveness of the maintenance intervention ($\alpha = 0$ represents perfect maintenance, i.e. AGAN; $\alpha = 1$ represents completely ineffective maintenance, i.e. As Good As Old (AGAO) and Δt_m is the time between two successive maintenance interventions. To show the impact of imperfect maintenance, we assume $\alpha = 0.1$.

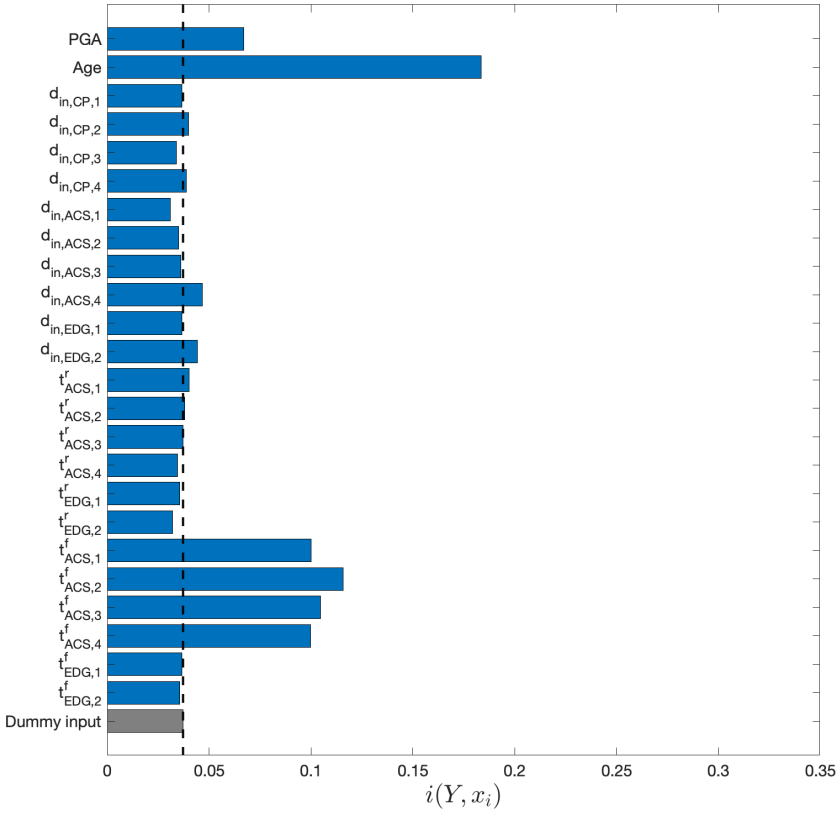


Figure 67. Parameter prioritization results considering imperfect maintenance.

As shown in **Fig. 67**, age becomes the most important input when imperfect maintenance is considered. In this case, an improvement to the maintenance strategy should be taken into account to reduce the impact of liquid lead corrosion ((Pinciroli et al., 2023)).

Lastly, a univariate parameter prioritization (i.e., considering $T_{w,max}$ of a single reactor unit at a time) has been performed based on the N_{sim} simulated accidental scenarios obtained with perfect maintenance. The prioritization is calculated using the

squared 2-Wasserstein distance (Borgonovo et al., 2024) and the results are compared with those of the multivariate parameter prioritization of **Fig. 66**.

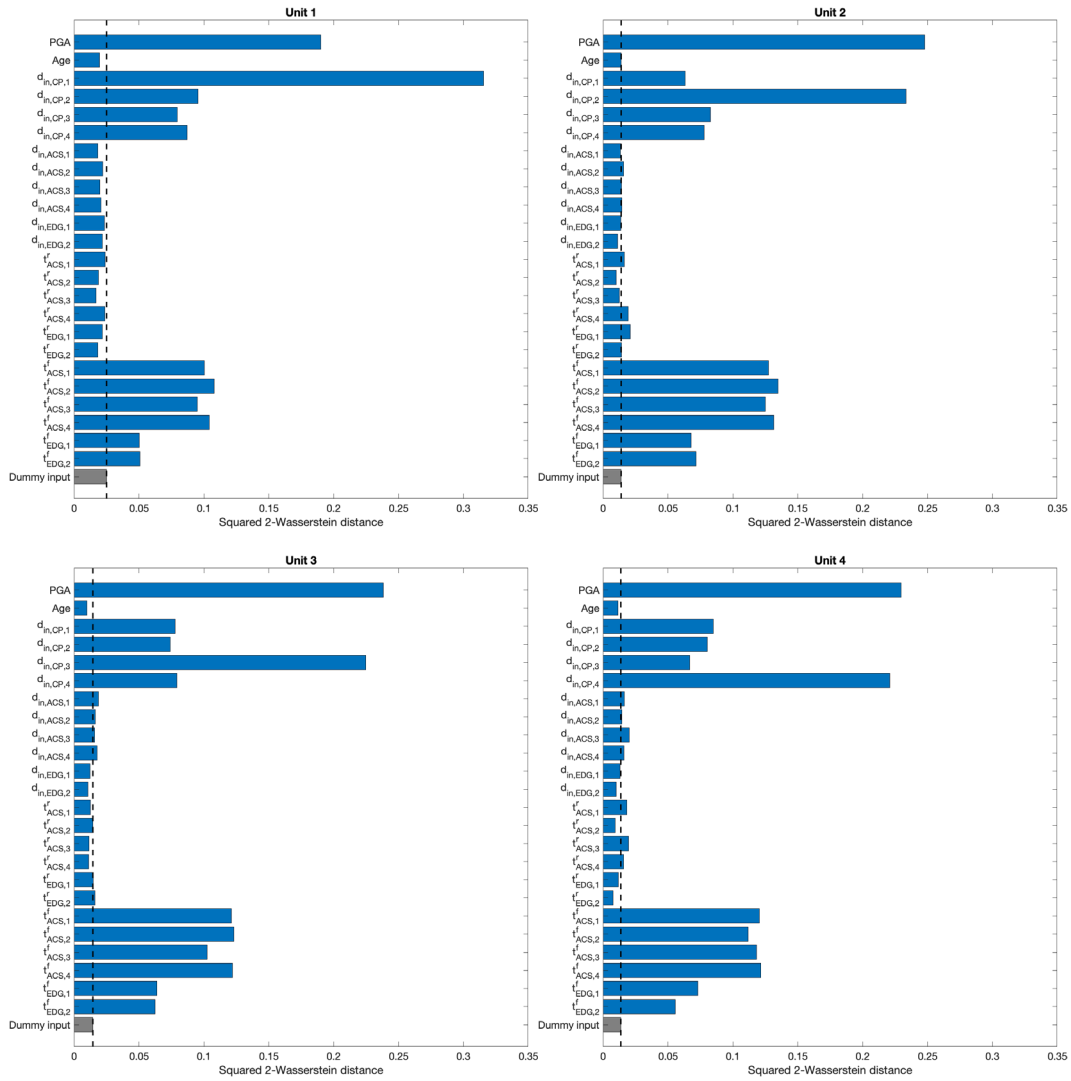


Figure 68. Univariate parameter prioritization results for unit 1 (top-left), unit 2 (top-right), unit 3 (bottom-left) and unit 4 (bottom-right).

As shown in **Fig. 68**, the results of the univariate analysis assign, for each *n-th* unit, a larger importance to $d_{in,CP,n}$, that, for unit $n = 1$, seems to be more important than PGA. This does not occur for all units because of the fluctuations of the estimates induced by the limited number of simulations available in the dataset. It is also worth noting that $d_{in,CP,n}$ has a non-negligible impact on the other SMR units. This is due to the fact that the units share the ACSs: a large initial depth of the CP corrosion defect increases the probability of a LOCA in the *n-th* unit; if LOCAs occur simultaneously in multiple units, the coolant mass flow provided by the ACSs must be shared, with a reduced mitigative effect.

4.5.2.2 *Critical input segmentation*

The critical input segmentation of PGA, $d_{in,CP,n}$ and $t^f_{ACS,n}$ is performed to identify the critical input values and provide guidelines for design improvement. For the sake of brevity, in what follows we consider only the analysis and results of the first reactor unit ($n = 1$), whose CUSUNORO curve is shown in **Fig. 69**.

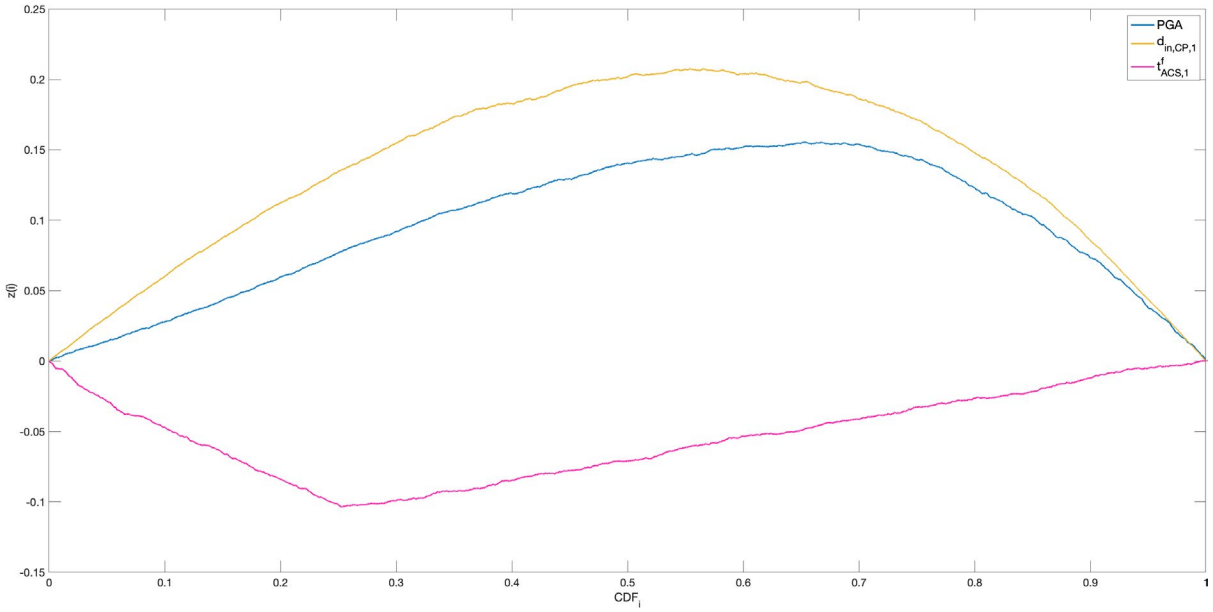


Figure 69. CUSUNORO results for PGA, $d_{in,CP,1}$ and $t^f_{ACS,1}$ considering $T_{w,max,1}$.

The following considerations about the most important inputs emerge:

- $T_{w,max,1}$ has a direct and (almost) linear dependence on $d_{in,CP,1}$, since the maximum value of the CUSUNORO curve is (almost) centered on the median of $d_{in,CP,1}$, preventing the identification of a critical value for $d_{in,CP,1}$; nevertheless, given the importance of $d_{in,CP,1}$ (**Fig. 66**), design improvements should still focus on the improvement of the CP resistance to corrosion by employing, for example, a low alloyed Fe-10Cr-4Al steel (Dömstedt et al., 2020);
- $T_{w,max,1}$ has a nonlinear dependence on the PGA (direct dependence) and the failure time of ACS (inverse dependence), since the maximum value of the corresponding CUSUNORO curves is significantly skewed from the median of the respective inputs; the critical value for the failure time of ACS is $t^f_{ACS,1,crit} = 317\ s$ (**Fig. 70**) and the critical value for the PGA is $PGA_{crit} = 11.61 \frac{m}{s^2}$ (**Fig. 71**). While not directly linked with design acceptance criteria, the critical values identify regions of large output sensitivity to input variations, which may suggest increased risk sensitivity if operating in those regions.

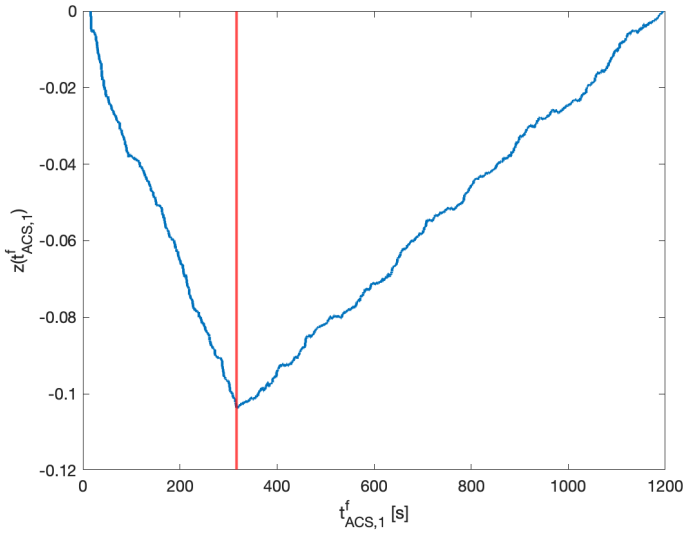


Figure 70. Critical value of ACS failure time.

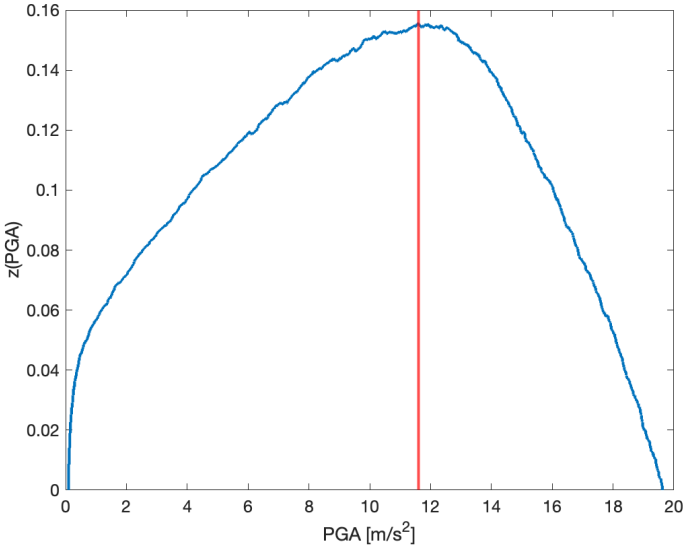


Figure 71. Critical value of PGA.

Possible design improvements could, then, be:

- reducing the probability of early failures of ACS, to avoid the region in which $t^f_{ACS,1} \leq t^f_{ACS,1,crit}$ and increase the distance from the CR; this can be achieved by increasing the ACS seismic resilience, as earthquake-induced failures tend to occur at the beginning of the accidental scenario, whereas failures due to random internal causes are uniformly distributed in time;
- reducing the earthquake impact on the NPP, effectively shifting the CR to larger PGA values.

Since it is obviously not possible to control the earthquake magnitude to avoid the region in which $PGA \geq PGA_{crit}$, in practice both objectives can be achieved by improving the NPP overall seismic resilience. As an example, let us consider the installation of viscous dampers to the NPP buildings. To evaluate the effect of damping

on the fragility of a concrete building, we first define the fragility as in (Güneyisi & Altay, 2008):

$$F(PGA) = \phi\left(\frac{1}{\beta}\ln\left(\frac{PGA}{\mu}\right)\right) \tag{65}$$

where ϕ is the standard normal cumulative distribution function, μ is the median seismic capacity and β is the standard deviation of the logarithmic median capacity. By installing a viscous damper with damping coefficient D, the median capacity of the building increases as follows (Güneyisi & Altay, 2008):

$$\mu^*(D) = \mu \cdot \frac{(73.048 \cdot \ln(D) - 112)}{100} \tag{66}$$

To find a suitable damping coefficient, we use the distribution shown in **Fig. 50** to estimate the PGA value for the design basis earthquake (SL-2 level), defined as the ground motion with an annual frequency of exceedance of 10^{-4}. To account for beyond design basis conditions, we apply a conservative amplification factor of 1.4 to this value, leading to $PGA_{BDBE} = 18\frac{m}{s^2}$ (International Atomic Energy Agency (IAEA), 2021). Finally, the damping coefficient D is found as the one that leads to $P^*_{F,S}(PGA_{BDBE}) \leq P_{F,S}(PGA_{crit})$ for all $s = 1,2,\dots,S$ safety features, where $P_{F,S}$ is the failure probability of the *s-th* safety feature considering the original SMR design and $P^*_{F,S}$ is the failure probability of the *s-th* safety feature considering the improved SMR design, leading to $D \geq 42\%$. Note that, given the lack of facility-specific models linking the seismic capacity to the damping coefficient, the model in Eq. (66), developed for concrete buildings, has been adopted to illustrate the proposed framework, and the results are not intended to serve as an actual design basis for nuclear facilities.

4.5.2.3 Implementation of the GSA-driven design improvements

To summarize, the following improvements are identified by the GSA framework:

- improvement of the CP resistance to corrosion by employing, for example, a low alloyed Fe-10Cr-4Al steel (Dömstedt et al., 2020);
- improvement of the NPP seismic reliability by installing viscous dampers with a damping coefficient $D \geq 42\%$;

While a conventional full-scope PSA would identify the need for improved seismic resilience in general terms, the proposed GSA framework provides additional, more targeted design insights. For example, the parameter prioritization results specifically highlight that improving the failure times of the ACSs is more beneficial than reducing their response times, suggesting a focus on reliability enhancements and/or specific maintenance strategies rather than responsiveness. The analysis also shows the significant role of corrosion defect depth in the CP, pointing to a different material as a targeted design improvement. Additionally, critical input segmentation provides quantitative input thresholds that define regions of increased system sensitivity, which

can guide setting design targets, such as the required damping coefficient. Overall, these insights can help the decision-maker prioritize design improvements to comply with regulations.

To show the impact of implementing the identified design improvements on the system safety, we perform $N^*_{sim} = 10^4$ simulations of accidental scenarios with the same simulation model, accounting for the above improvements in system design. The comparison between the results before (**Fig. 72**) and after (**Fig. 73**) the design improvements lead to the following considerations:

- the number of system failures (i.e., the filled red dots) is significantly reduced, and failures occur at larger PGA values;
- the number of ACS failures is significantly reduced (note that when $t^f_{ACS,1} = 1200\ s$, ACS is not failed).

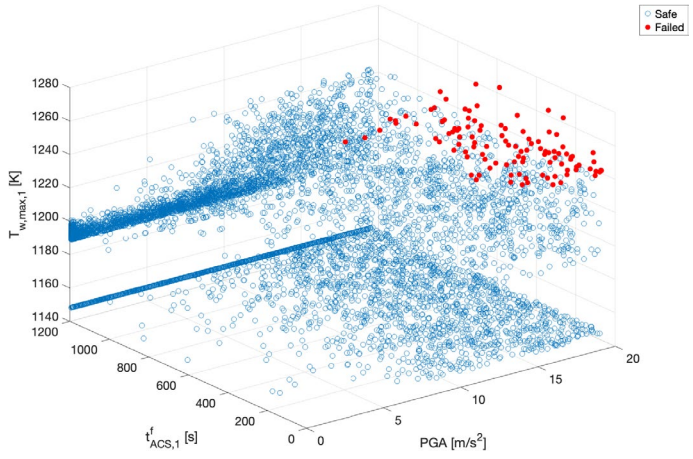


Figure 72. $T_{w,max,1}$ as a function of PGA and $t^f_{ACS,1}$ with the original design.

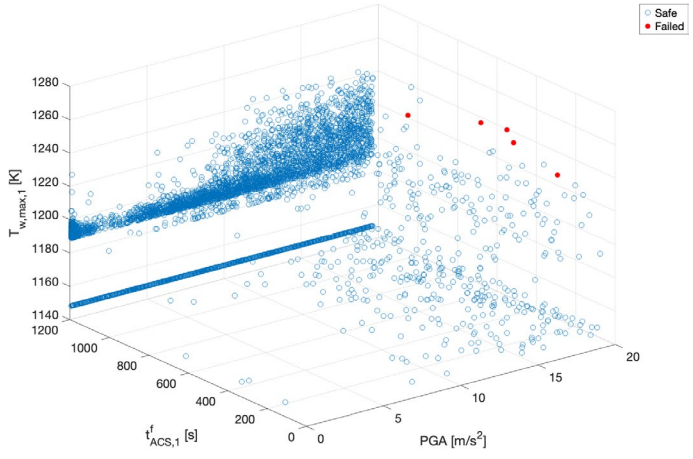


Figure 73. $T_{w,max,1}$ as a function of PGA and $t^f_{ACS,1}$ with the improved design.

Consequently, the CR obtained with the improved design is shifted to larger PGA values and is significantly smaller with respect to the CR obtained with the original design, as shown in **Fig. 74**, resulting in a safer operation of the reactor.

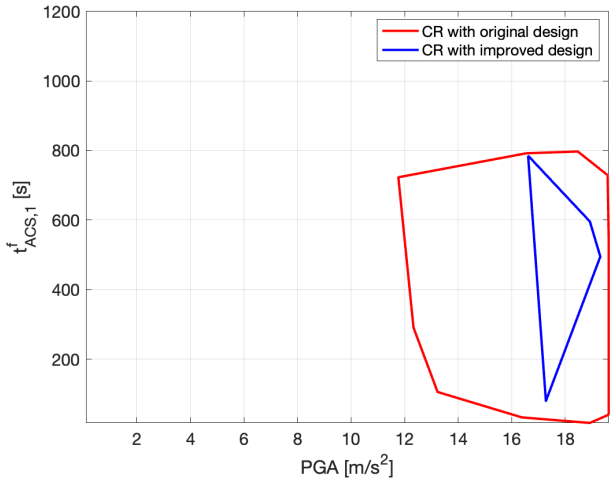


Figure 74. CR boundary with original and improved design.

Finally, the results are also compared in terms of $PSM_{T_{w,max,1}}$ (with $\gamma = 95$) and probability of failure of the first reactor (i.e., $F_{P,1}$). As shown in **Fig. 75** and **Fig. 76**, the improved design achieves a significantly larger PSM ($\sim 53\%$ increase) and a significantly lower failure probability ($\sim 95\%$ decrease), showing the benefits of implementing the identified design improvements.

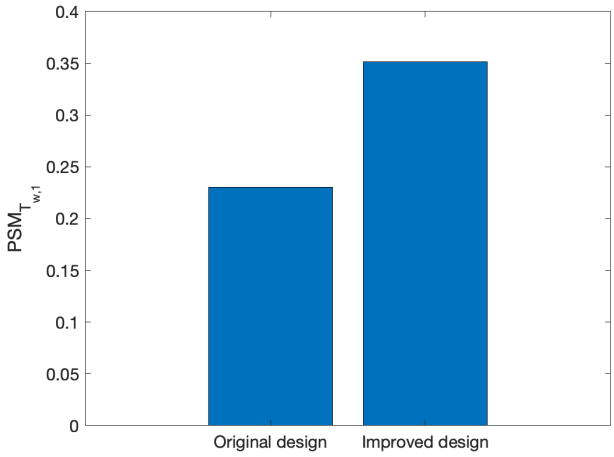


Figure 75. $PSM_{T_{w,max,1}}$ comparison between original and improved design.

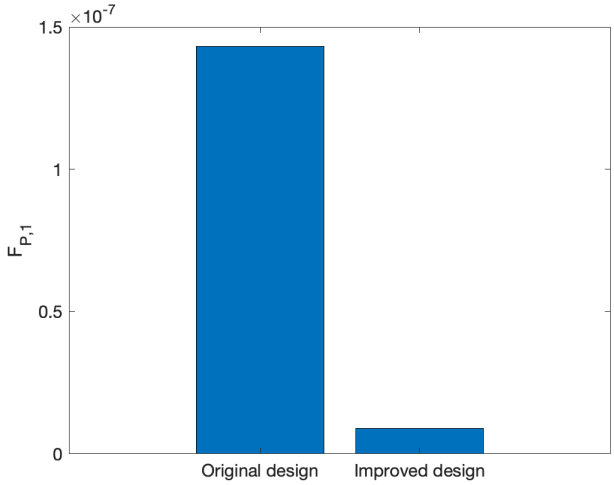


Figure 76. $F_{P,1}$ comparison between original and improved design.

4.5.2.4 Discussion

The proposed framework can provide valuable insights to assist in the modeling phase of an SMR design, under the following constraints:

- the validity of the sensitivity analysis results is inherently dependent on the fidelity of the simulation model: if the model does not satisfy the accuracy and predictiveness requirements necessary for its intended use in safety analysis and design decision-making (International Atomic Energy Agency, 2019), the sensitivity analysis results may be misleading;
- the estimation accuracy of global sensitivity measures increases with the sample size, and the natural recommendation is to use the largest size allowed by computational budget. In our case, the estimation design is given data and allows the analyst to devote the entire budget to one Monte Carlo uncertainty quantification, thus increasing the sample size as much as possible. However, as the literature widely documents, uncertainty quantification becomes problematic for models with long running times. In these cases, the literature suggests alternative approaches. On the one hand, one can reduce

computational burden by approximating time-consuming calculations in the original simulators by artificial intelligence tools or model emulators (He et al., 2025; Nasr et al., 2025). On the other hand, one can use exploration-exploitation strategies and mix high- and low-fidelity simulations (Cataldo et al., 2025). Alternatively, one can plan the experiments in two steps, with first a careful selection of the points of the input space through a space-filling design (Pronzato & Müller, 2012), and then fitting a metamodel to propagate uncertainty, also preceding the analysis with a screening exercise (Auder et al., 2012; Cervi et al., 2022). If the metamodel fit is accurate, several runs can be obtained in a short amount of time. The utilization of these strategies to reduce computational burden is a field in constant evolution in the modeling of technological systems, recently accelerated by the rapid progress in artificial intelligence techniques.

Chapter 5 Conclusions

This PhD thesis has addressed the risk assessment and management of safety-critical energy systems equipped with degrading safety barriers. In particular, a set of complementary methodological frameworks for integrating safety barriers degradation into the risk assessment and decision-making processes has been proposed.

In Chapter 2, a condition-informed multi-hazard QRA BN-based framework was developed and applied to a real onshore hydrocarbon facility. The proposed approach enables the dynamic updating of the risk profile as new information regarding the health state of safety barriers becomes available. Results showed that degradation mechanisms may significantly alter the aggregated LSIR, potentially leading to the exceedance of acceptability thresholds after only a few years of operation if not properly accounted for.

Chapter 3 introduced a PoF-based DBN framework for modeling the aging of safety barriers and its integration within a RL environment for maintenance optimization. By formulating the maintenance scheduling problem as a SDP, a DRL agent was trained to identify risk-based prescriptive maintenance policies that jointly minimize expected system risk and maintenance costs. Results show that adaptive maintenance strategies informed by degradation models outperform traditional fixed-interval policies by explicitly accounting for the time-dependent deterioration of safety barriers and the long-term consequences of maintenance actions.

Chapter 4 addressed the risk-informed design of multi-unit nuclear installations characterized by shared safety systems. An IDPSA framework was developed to simulate accident progression in a MU-NPP composed of four SMDFRs exposed to seismic hazards. Age-dependent fragility models were embedded within a dynamic simulator to account for the degradation of shared safety features. The accident scenarios generated by the IDPSA model was subsequently analyzed through an OT-based GSA framework, enabling the identification of suitable design improvements.

Taken together, the methodologies developed in this thesis allow a dynamic risk assessment that reflects the current state of the plant, and risk-informed operational and design decision-making.

The frameworks developed in this thesis also provide a foundation for several future research directions with reference to the TCs identified in **Section 1.2.1**:

1. Regarding **TC1** (dynamic risk assessment of degrading energy systems):
    - **Real-time risk assessment**. The proposed frameworks rely on periodically updated KID regarding the health state of safety barriers or on degradation models. However, modern energy systems are increasingly equipped with sensors that continuously monitor process variables and equipment conditions. A promising research direction

consists in integrating the proposed frameworks with digital twin architectures capable of processing real-time sensor data and continuously updating the system risk profile (Zio & Miqueles, 2024). Achieving such real-time capabilities also requires significant computational acceleration of the underlying risk assessment models. Surrogate modeling techniques, such as Recurrent Neural Networks (RNN) (Schuster & Paliwal, 1997), Long-Short Term Memory (LSTM) models (Van Houdt et al., 2020), Transformer models (Vaswani et al., 2017), Graph Neural Networks (GNN) (J. Zhou et al., 2020) or advanced Monte Carlo methods (Pedroni et al., 2017) could be used to efficiently estimate the risk.

- **Resilience assessment of degrading energy systems**. The methodologies developed in this thesis primarily focus on the quantification of risk. Future research could extend the proposed frameworks to assess resilience by explicitly modeling recovery processes, emergency response actions, and system restoration dynamics. This would enable evaluating how safety barrier degradation affects not only the prevention and mitigation of accidents but also the system recover capability.
- **Modeling of interacting safety systems**. The methodologies developed in this thesis assume independence among safety systems. Future research could extend the proposed frameworks to explicitly model interdependencies and interactions among safety systems. This aspect is particularly relevant for next-generation NPPs, which are equipped with multiple interacting passive safety systems (e.g., natural circulation and melting fuel plug systems in MSRs), whose reliability assessment requires the integration of complex, coupled simulation models.

2. Regarding **TC2** (maintenance optimization of degrading energy systems):
    - **DBN models for complex systems exposed to rare accident scenarios**. The proposed PoF-based DBN framework presented in Chapter 3, and more in general any BN-based framework in which the parameters are not expert-defined, rely on simulation data to learn the network parameters. However, for complex systems exposed to rare accidental scenarios, generating sufficiently large simulation datasets may become computationally unfeasible. Future work could investigate the use of Enhanced Bayesian Networks (eBN) (Straub & Der Kiureghian, 2010) which combine BNs with structural reliability methods to efficiently estimate conditional probabilities even in the presence of rare events.
    - **Causally-informed reinforcement learning**. The performance of RL-based maintenance optimization could be further improved by exploiting the causal structure encoded in the DBN model. In the current framework, the DBN is used as an environment to simulate the evolution of the system through forward inference. However, the same model can also be leveraged to extract causal information regarding the contribution of individual safety barriers to system risk. In particular, diagnostic inference could be used to identify the safety barriers and

degradation mechanisms that most significantly influence the occurrence of critical events. This information could then be incorporated into the observation space or reward structure of the RL agent, guiding the learning process toward more risk-informed and interpretable maintenance policies.

3. Regarding **TC3** (risk-informed design of degrading energy systems):
    - **Time-dependent multivariate GSA**. The proposed GSA framework currently requires collapsing time series outputs into scalar indicators (e.g., mean value, maximum value, standard deviation…) before performing the sensitivity analysis, which may not fully capture the temporal dynamics of the system response. Future work could therefore focus on developing time-dependent sensitivity analysis methods capable of directly handling multivariate and dynamic outputs, allowing the identification of parameters that influence the temporal evolution of safety-relevant variables. Such developments would provide more accurate insights for risk-informed design.

Appendix A Safety barriers performance characterization

A.1. Continuously monitored safety barriers

Let $\boldsymbol{Y}(t) = \begin{bmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \\ \dots \\ \boldsymbol{y}_K \end{bmatrix} = \begin{bmatrix} y_1(t_1), y_1(t_2), \dots, y_1(t_n) \\ y_2(t_1), y_2(t_2), \dots, y_2(t_n) \\ \dots \\ y_K(t_1), y_K(t_2), \dots, y_K(t_n) \end{bmatrix}$ be the matrix of time series of the $k = 1,2, \dots K$ process variables collected at the discrete times $t_1 < t_2 < \cdots < t_n$ from the continuous monitoring of a safety barrier. For each *k-th* process variable, a PSM can be used to measure, in probabilistic terms, to which extent the parameter y_k is below (or above) an acceptable upper threshold U_k (or lower threshold L_k) during the monitoring interval. This is done by estimating the true γ-percentile $y_{k,\gamma}$ (usually the 95th percentile) of the distribution of the parameter (Di Maio et al., 2016) with a confidence β (usually 95%), either by empirical percentile estimation methods (in case of sufficient monitoring data) or by Order Statistics (OS) (Nutt & Wallis, 2004) (in case of scarcity of monitoring data). Then, the estimated percentile $\hat{y}_{k,\gamma}$ is used to calculate the upper and lower PSM (i.e., $PSM_{k,up}$ and $PSM_{k,low}$) as follows:

$$PSM_{k,up} = \begin{cases} \dfrac{U_k - \hat{y}_{k,\gamma}}{U_k - y_{k,ref}} & if\ \hat{y}_{k,\gamma} \le U_k \\ 0 & if\ \hat{y}_{k,\gamma} > U_k \\ 1 & if\ \hat{y}_{k,\gamma} < y_{k,ref} \end{cases} \tag{67}$$

$$PSM_{k,low} = \begin{cases} \dfrac{\hat{y}_{k,\gamma} - L_k}{y_{k,ref} - L_k} & if\ \hat{y}_{k,\gamma} \ge U_k \\ 0 & if \hat{y}_{k,\gamma} < U_k \\ 1 & if\ \hat{y}_{k,\gamma} > y_{k,ref} \end{cases} \tag{68}$$

where $y_{k,ref}$ is a reference value for y_k, typically the nominal value. Once $PSM_{k,up}$ and $PSM_{k,low}$ are estimated for all the K process variables, they are aggregated as follows:

$$PSM_{up} = \frac{1}{K}\sum_{k=1}^{K} PSM_{k,up} \tag{69}$$

$$PSM_{low} = \frac{1}{K}\sum_{k=1}^{K} PSM_{k,low} \tag{70}$$

$$PSM = \min\left(PSM_{up}, PSM_{low}\right) \tag{71}$$

where $\min(\cdot)$ is the minimum operator. The PSM is then taken as x_{KPI} and used to estimate P_H, P_M and P_L from the probability distributions shown in **Fig. 77**.

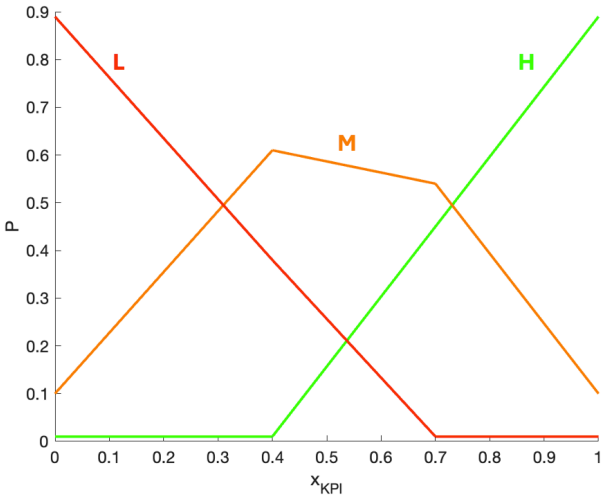


Figure 77. Probability distributions for the HSs.

A.2. Event-based safety barriers

The performance of event-based safety barriers is characterized by tailored KPIs. To estimate the probabilities of the HS, each KPI value is converted into a KPI% as follows:

- for normally distributed KPIs, a normal distribution $N(\mu, \sigma)$ is defined by calculating its parameters with the following system of equations (Di Maio, Scapinello, Zio, Ciarapica, et al., 2021):

$$\begin{cases} \mu = \dfrac{\phi^{-1}(0.7)Z_L - \phi^{-1}(0.4)Z_U}{\phi^{-1}(0.7) - \phi^{-1}(0.4)} \\ \sigma = \dfrac{Z_U - Z_L}{\phi^{-1}(0.7) - \phi^{-1}(0.4)} \end{cases} \quad (72)$$

  where ϕ^{-1} is the inverse Cumulative Distribution Function (CDF) of the standard normal distribution, Z_L is the KPI value below which the performance is considered low and Z_U is the KPI value above which the performance is considered good. Once the normal distribution is characterized, the KPI% is the percentile of the distribution corresponding to the KPI value;

- for binary KPIs, the performance is considered good if the KPI is equal to the associated optimal value (KPI_{opt}), and low for any other value, leading to:

$$KPI\% = \delta_{KPI,KPI_{opt}} \quad (73)$$

- for KPIs evaluated through questionnaires, qualitative indicators (i.e., H, M, L, which correspond to $KPI\% = 1$, $KPI\% = 0.5$ and $KPI\% = 0$, respectively) are associated with each possible combinations of answers.

The KPI% is then taken as x_{KPI} and used to estimate P_H, P_M and P_L from the probability distributions shown in **Fig. 77**. In case of safety barriers whose performance is characterized by multiple KPIs, the aggregation is performed as follows:

$$\begin{cases} P_H = \dfrac{\sum_{i=1}^{N_{KPI}} P_{H|KPI_i} W_{KPI_i}^e W_{KPI_i}^h}{\sum_{i=1}^{N_{KPI}} W_{KPI_i}^e W_{KPI_i}^h} \\ P_M = \dfrac{\sum_{i=1}^{N_{KPI}} P_{M|KPI_i} W_{KPI_i}^e W_{KPI_i}^h}{\sum_{i=1}^{N_{KPI}} W_{KPI_i}^e W_{KPI_i}^h} \\ P_L = \dfrac{\sum_{i=1}^{N_{KPI}} P_{L|KPI_i} W_{KPI_i}^e W_{KPI_i}^h}{\sum_{i=1}^{N_{KPI}} W_{KPI_i}^e W_{KPI_i}^h} \end{cases} \quad (74)$$

where N_{KPI} is the number of KPIs associated with the safety barriers performance, $W_{KPI_i}^e$ is an expert-based weight and $W_{KPI_i}^h$ is an inertia weight, calculated as follows:

- KPIs whose low values correspond to low barrier performance:

$$W_{KPI_i}^h = e^{\frac{\tau_{KPI_i} - KPI_i}{\tau_{KPI_i}}} \quad (75)$$

- KPIs whose low values correspond to high barrier performance:

$$W_{KPI_i}^h = e^{\frac{KPI_i - \tau_{KPI_i}}{\tau_{KPI_i}}} \quad (76)$$

where τ_{KPI_i} is the value of the KPI at the previous monitoring/inspection interval.

Appendix B Dynamic Bayesian Networks

A Bayesian Network (BN) is a probabilistic model, in which random variables characterized by a finite set of mutually exclusive states are represented by nodes (Jordan et al., 2007). The conditional dependencies between the nodes are denoted by directed arcs to form an acyclic graph, and their strength is defined by CPTs. For a set of random variables $U = \{X_1, \dots, X_Z\}$ the joint probability $P(U)$ is defined as the product of marginal and local conditional probabilities $P\left(X_z \middle| \pi(X_z)\right)$:

$$P(U) = \prod_{z=1}^{Z} P\left(X_z \middle| \pi(X_z)\right) \tag{77}$$

where $\pi(X_z)$ is the set of parent nodes of X_z.

DBN is an extension of BNs (Jordan et al., 2007; Neapolitan, 2004) that allow for explicitly modelling the temporal evolution of a set of random variables over a discretized timeline with N_τ time steps. Each ***z-th*** node X_z at the τ***-th*** time step can be conditionally dependent not only on its parents at the same time step, but also on its parents (and its own states) at the previous time step, so that the joint probability of a set of random variables at time step $\tau + \Delta\tau$ is equal to (Khakzad, 2015):

$$P\left(U^{\tau+\Delta\tau}\right) = \prod_{z=1}^{Z} P\left(X_z^{\tau+\Delta\tau} \middle| X_z^{\tau}, \pi(X_z), \pi\left(X_z^{\tau+\Delta\tau}\right)\right) \tag{78}$$

where $X_z^{\tau+\Delta\tau}$ and X_z^{τ} are the copies of X_z in two consecutive time steps and $\pi(X_z^{\tau+\Delta\tau})$ and $\pi(X_z)$ are the parent sets of X_z at the time steps $\tau + \Delta\tau$and τ, respectively.

Fig. 78 shows an example of DBN for $N_\tau = 2$ time steps, where the dashed lines represent the temporal arcs (i.e., conditional dependencies among nodes at different time steps) and the continuous lines represent static arcs (i.e., conditional dependencies among nodes at the same time step). According to the DBN of **Fig 78**, the conditional probability of X_3, for example, would be $P\left(X_3^{\tau+\Delta\tau} \middle| X_3^{\tau}, X_1^{\tau}, X_2^{\tau+\Delta\tau}\right)$. It is also important to notice that DBNs, with respect to BNs, can handle closed cycles of links among variables, provided that at least one of them belongs to a different time step, allowing for a more flexible modelling.

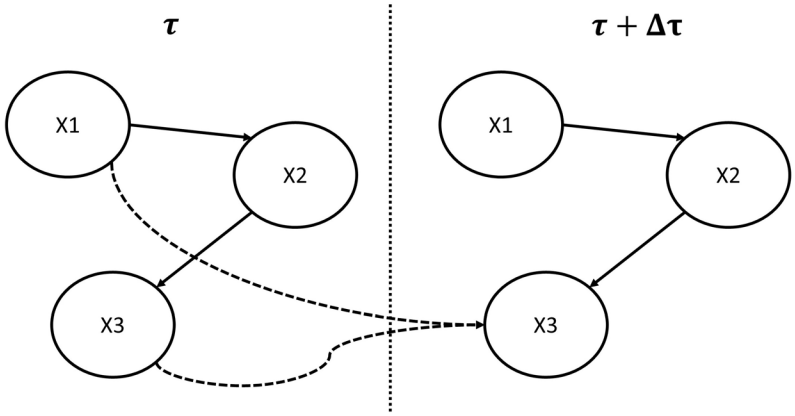


Figure 78. Example of DBN.

Appendix C Proximal Policy Optimization algorithm

PPO is a state-of-the-art policy gradient method for RL which aims at maximizing a surrogate objective function using stochastic gradient ascent. PPO retains some of the advantages of Trust Region Policy Optimization (TRPO) (Schulman et al., 2015) but is much simpler to implement and is more general (Schulman et al., 2017).

Let $r_t(\boldsymbol{\theta})$ denote the probability ratio $r_t(\boldsymbol{\theta}) = \frac{\pi_{\boldsymbol{\theta}}(\boldsymbol{a}_t|\boldsymbol{s}_t)}{\pi_{\boldsymbol{\theta}_{old}}(\boldsymbol{a}_t|\boldsymbol{s}_t)}$, where $\boldsymbol{\theta}$ is the vector of the policy parameters , $\pi_{\boldsymbol{\theta}}(\boldsymbol{a}_t|\boldsymbol{s}_t)$ is the updated policy and $\pi_{\boldsymbol{\theta}_{old}}(\boldsymbol{a}_t|\boldsymbol{s}_t)$ is the policy before the last update. The surrogate objective of PPO is the following:

$$L^{CLIP}(\boldsymbol{\theta}) = \widehat{\mathbb{E}}_t[\min[r_t(\boldsymbol{\theta})\widehat{A}_t, clip(r_t(\boldsymbol{\theta}), 1-\epsilon, 1+\epsilon)\widehat{A}_t]] \tag{79}$$

where ϵ is a hyperparameter that indicates the clipping of the probability ratio $r_t(\boldsymbol{\theta})$. The clipping removes the incentive for moving $r_t(\boldsymbol{\theta})$ outside of the interval $[1-\epsilon, 1+\epsilon]$. The surrogate objective is the minimum between the clipped and unclipped objective.

Appendix D The MU-SMDFR simulation model

The developed model simulates four units of SMDFR, each consisting of a core described by two models: a neutronic model and a thermal-hydraulic model, linked by the reactivity feedback. To capture the neutronic behaviour of the SMDFR, a modified point kinetic model with 6 delayed neutron groups is adopted to account for the flowing of the fuel: even if the fuel outside the core is kept subcritical, the decay process of delayed neutron precursors has to be considered to evaluate its impact on the neutron distribution in the core. This is done considering two additional terms: the precursor loss when the fuel leaves the core, and the precursor gain when the fuel re-enters the core (C. Liu et al., 2021). Then, a thermal-hydraulic model is built based on the assumption that the fuel, piping wall and coolant in the core are divided into 3 parts and each part has lumped propertied (C. Liu et al., 2021).

To model the occurrence of a LOCA, the following assumptions are made:

- the LOCA flow rate $\dot{m}_{leak}$ mimics the one that might occur in conventional reactors (Park et al., 2021), leading to:

$$\dot{m}_{leak} = \dot{m}_{leak,0} + a \cdot t^b \tag{80}$$

where $\dot{m}_{leak,0} = 18\frac{kg}{s}$ is the initial value of the leak flow rate and a and b are parameters. We assume that, without loss of generality, $a = 3$ and $b = \frac{1}{4}$.

- the velocity imposed by the pump on the coolant is constant. Therefore, the flow rate of the coolant $\dot{m}_c$ decreases as the total coolant mass decreases due to air entering the pipes. This change is due to the reduced density of the fluid in the pipe cross-section, since the mass flow rate of a pump $\dot{m}$ can be expressed as:

$$\dot{m} = \rho v A \tag{81}$$

where ρ is the density of the fluid, v is the constant velocity of the fluid and A is the cross-sectional area. Therefore, we can calculate $\dot{m}_c$ as follows:

$$\dot{m}_c = \dot{m}_{c,0} \cdot \frac{\rho_{lead} \cdot a + \rho_{air} \cdot (1 - a)}{\rho_{lead}} \tag{82}$$

where $\dot{m}_{c,0}$ is the nominal coolant mass flow rate, ρ_{lead} is the density of liquid lead, ρ_{air} is the density of air and a is the fraction of the total coolant mass that has been leaked. Finally, to mitigate the accidental scenario that follows the LOCA, the mitigative action of ECCS is modelled as a constant flow rate of liquid lead, leading to:

$$\dot{m}_{c,tot} = \dot{m}_c + \dot{m}_{c,ACS} \tag{83}$$

References

Ab Rahim, M. S., Reniers, G., Yang, M., & Bajpai, S. (2024). Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review. *Journal of Loss Prevention in the Process Industries*, *88*. https://doi.org/10.1016/j.jlp.2024.105274

Abdolhamidzadeh, B., Abbasi, T., Rashtchian, D., & Abbasi, S. A. (2010). A new method for assessing domino effect in chemical process industry. *Journal of Hazardous Materials*, *182*(1–3), 416–426. https://doi.org/10.1016/j.jhazmat.2010.06.049

Abdolhamidzadeh, B., Abbasi, T., Rashtchian, D., & Abbasi, S. A. (2011). Domino effect in process-industry accidents – An inventory of past events and identification of some patterns. *Journal of Loss Prevention in the Process Industries*, *24*(5), 575–593. https://doi.org/10.1016/J.JLP.2010.06.013

Andonov, S. (2017). Bowtie Methodology: A Guide for Practitioners. In *Bowtie Methodology: a Guide for Practitioners*. https://doi.org/10.1201/9781315158853

Aneziris, O. N., Nivolianitou, Z., Konstandinidou, M., Mavridis, G., & Plot, E. (2017). A Total Safety Management framework in case of a major hazards plant producing pesticides. *Safety Science*, *100*. https://doi.org/10.1016/j.ssci.2017.03.021

Arulkumaran, K., Deisenroth, M. P., Brundage, M., & Bharath, A. A. (2017). Deep reinforcement learning: A brief survey. In *IEEE Signal Processing Magazine* (Vol. 34, Number 6, pp. 26–38). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/MSP.2017.2743240

Atwood, C. L. (1996). Constrained noninformative priors in risk assessment. *Reliability Engineering and System Safety*, *53*(1). https://doi.org/10.1016/0951-8320(96)00026-9

Auder, B., De Crecy, A., Iooss, B., & Marquès, M. (2012). Screening and metamodeling of computer experiments with functional outputs. Application to thermal-hydraulic computations. *Reliability Engineering and System Safety*, *107*. https://doi.org/10.1016/j.ress.2011.10.017

Aumeier, S. E., Alpay, B., Lee, J. C., & Akcasu, A. Z. (2006). Probabilistic techniques for diagnosis of multiple component degradations. *Nuclear Science and Engineering*, *153*(2). https://doi.org/10.13182/NSE06-A2599

Balbaud-Célérier, F., & Barbier, F. (2001). Investigation of models to predict the corrosion of steels in flowing liquid lead alloys. *Journal of Nuclear Materials*, *289*(3), 227–242. https://doi.org/10.1016/S0022-3115(01)00431-7

Barrelas, J., Ren, Q., & Pereira, C. (2021). Implications of climate change in the implementation of maintenance planning and use of building inspection systems. *Journal of Building Engineering*, *40*, 102777. https://doi.org/10.1016/J.JOBE.2021.102777

Bellman, R. (1952). On the Theory of Dynamic Programming. *Proc Natl Acad Sci U S A*.

Benayoun, R., Tergny, J., & Laritchev, O. (1971). Linear Programming with Multiple Objective Functions: Step Method (STEM). *Mathematical Programming*.

Bjørnsen, K., & Aven, T. (2019). Risk aggregation: What does it really mean? *Reliability Engineering and System Safety*, *191*. https://doi.org/10.1016/j.ress.2019.106524

Borgonovo, E., & Apostolakis, G. E. (2001). A new importance measure for risk-informed decision making. *Reliability Engineering and System Safety*, *72*(2). https://doi.org/10.1016/S0951-8320(00)00108-3

Borgonovo, E., Figalli, A., Plischke, E., & Savaré, G. (2024). Global Sensitivity Analysis via Optimal Transport. *Management Science*. https://doi.org/10.1287/mnsc.2023.01796

Borgonovo, E., Hazen, G. B., & Plischke, E. (2016). A Common Rationale for Global Sensitivity Measures and Their Estimation. *Risk Analysis*, *36*(10). https://doi.org/10.1111/risa.12555

Butler, M. P., Reed, P. M., Fisher-Vanden, K., Keller, K., & Wagener, T. (2014). Identifying parametric controls and dependencies in integrated assessment models using global sensitivity analysis. *Environmental Modelling and Software*, *59*. https://doi.org/10.1016/j.envsoft.2014.05.001

Calvo-Fullana, M., Paternain, S., Chamon, L. F. O., & Ribeiro, A. (2021, February 23). State Augmented Constrained Reinforcement Learning: Overcoming the Limitations of Learning with Rewards. *International Conference on Machine LEarning*. http://arxiv.org/abs/2102.11941

Cataldo, G., Borgonovo, E., Siddens, A., Carpenter, K., Nado, M., & Plischke, E. (2025). Global sensitivity analyses for test planning with black-box models for Mars Sample Return. *Risk Analysis*, *n/a*(n/a). https://doi.org/https://doi.org/10.1111/risa.70010

Center for Chemical Process Safety. (2009). *Guidelines for Developing Quantitative Safety Risk Criteria*. American Institute of Chemical Engineers. https://doi.org/10.1002/9780470552940

Cervi, E., Lu, X., Cammi, A., Di Maio, F., & Zio, E. (2022). Sensitivity-Analysis-Driven Surrogate Model for Molten Salt Reactors Control. *Journal of Nuclear Engineering*, *3*(4). https://doi.org/10.3390/jne3040016

Chatterjee, S. (2021). A New Coefficient of Correlation. *Journal of the American Statistical Association*, *116*(536). https://doi.org/10.1080/01621459.2020.1758115

Chen, C., Reniers, G., & Khakzad, N. (2021). A dynamic multi-agent approach for modeling the evolution of multi-hazard accident scenarios in chemical plants. *Reliability Engineering and System Safety*, *207*. https://doi.org/10.1016/j.ress.2020.107349

Chen, H., Chen, G., Men, J., Zheng, C., Huang, Y., Gao, X., & Zhao, Y. (2026). An advanced alternative technique for add-on safety barrier optimal allocation for prevention and mitigation of domino effects based on the multi-objective optimization model. *Reliability Engineering and System Safety*, *269*. https://doi.org/10.1016/j.ress.2025.112108

Chen, Y. (2020). Consequence Simulation and Risk Assessment Model of Liquid Ammonia Leakage Accident Based on PHAST Software. *2020 International Conference on Advance in Ambient Computing and Intelligence (ICAACI)*, 125–129. https://doi.org/10.1109/ICAACI50733.2020.00032

Chen, Y., Georgiou, T. T., & Pavon, M. (2021). Stochastic control liaisons: Richard Sinkhorn meets gaspard monge on a schrödinger bridge. In *SIAM Review* (Vol. 63, Number 2). https://doi.org/10.1137/20M1339982

Cherubin, P., Pellino, S., & Petrone, A. (2011). Baseline risk assessment tool: A comprehensive risk management tool for process safety. *Process Safety Progress*, *30*(3), 251–260. https://doi.org/10.1002/prs.10464

Cohn, B., Noel, T., Cardoni, J., Haskin, T., Osborn, D., & Aldemir, T. (2023). Integrated Safety and Security Analysis of Nuclear Power Plants Using Dynamic Event Trees. *Nuclear Science and Engineering*, *197*(sup1). https://doi.org/10.1080/00295639.2023.2177076

Compare, M., Bellani, L., Cobelli, E., Zio, E., Annunziata, F., Carlevaro, F., & Sepe, M. (2020). A reinforcement learning approach to optimal part flow management for gas turbine maintenance. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *234*(1), 52–62. https://doi.org/10.1177/1748006X19869750

Cozzani, V., Antonioni, G., Landucci, G., Tugnoli, A., Bonvicini, S., & Spadoni, G. (2014). Quantitative assessment of domino and NaTech scenarios in complex industrial areas. *Journal of Loss Prevention in the Process Industries*, *28*, 10–22. https://doi.org/10.1016/J.JLP.2013.07.009

Cozzani, V., & Salzano, E. (2004). The quantitative assessment of domino effects caused by overpressure: Part I. Probit models. *Journal of Hazardous Materials*, *107*(3), 67–80. https://doi.org/10.1016/J.JHAZMAT.2003.09.013

Cozzani, V., Tugnoli, A., & Salzano, E. (2009). The development of an inherent safety approach to the prevention of domino accidents. *Accident Analysis and Prevention*, *41*(6), 1216–1227. https://doi.org/10.1016/j.aap.2008.06.002

Cuturi, M. (2013). Sinkhorn distances: Lightspeed computation of optimal transport. *Advances in Neural Information Processing Systems*.

De Farias, D. P., & Van Roy, B. (2003). The linear programming approach to approximate dynamic programming. *Operations Research*, *51*(6), 850–865. https://doi.org/10.1287/opre.51.6.850.24925

Decarli, L., Crivellari, A., La Rosa, L., Zio, E., Di Maio, F., Scapinello, O., & Martinoia, L. (2021). Multihazard Risk Aggregation Approach for Quantitative Risk Assessment of Upstream Oil and Gas Facilities. *Society of Petroleum Engineers - Abu Dhabi International Petroleum Exhibition and Conference, ADIP 2021*. https://doi.org/10.2118/207276-MS

Dempster, A. P., Laird, N. M., & Rubin, D. B. (1977). Maximum Likelihood from Incomplete Data via the EM Algorithm. *Journal of the Royal Statistical Society. Series B (Methodological)*, *39*(1), 1–38.

Di Maio, F., Bani, L., & Zio, E. (2023). Seismic resilience assessment of Small Modular Reactors by a Three-loop Monte Carlo Simulation. *Nuclear Engineering and Design*, *410*, 112385. https://doi.org/10.1016/J.NUCENGDES.2023.112385

Di Maio, F., Marchetti, S., & Zio, E. (2023a). A framework of sensitivity analysis for the performance assessment of safety barriers impacted by NaTech accidents. *Process Safety and Environmental Protection*, *171*, 1022–1030. https://doi.org/10.1016/j.psep.2022.08.072

Di Maio, F., Marchetti, S., & Zio, E. (2023b). Robust multi-objective optimization of safety barriers performance parameters for NaTech scenarios risk assessment and management. *Reliability Engineering & System Safety*, 109245. https://doi.org/10.1016/j.ress.2023.109245

Di Maio, F., Matteo Coscia, T., Pedroni, N., Bersano, A., Mascari, F., & Zio, E. (2024). Global Sensitivity Analysis for Segmented Inverse Uncertainty Quantification in the Safety Analysis of Nuclear Power Plants. *Annals of Nuclear Energy*, *208*, 110791. https://doi.org/10.1016/J.ANUCENE.2024.110791

Di Maio, F., Picoco, C., & Zio, E. (2017). A repairable dynamic event tree framework for the safety assessment of a steam generator of a nuclear power plant. *PSAM 2016 - 13th International Conference on Probabilistic Safety Assessment and Management*.

Di Maio, F., Rai, A., & Zio, E. (2016). A dynamic probabilistic safety margin characterization approach in support of Integrated Deterministic and Probabilistic Safety Analysis. *Reliability Engineering and System Safety*, *145*. https://doi.org/10.1016/j.ress.2015.08.016

Di Maio, F., Scapinello, O., Zio, E., Ciarapica, C., Cincotta, S., Crivellari, A., Decarli, L., & La Rosa, L. (2021). Accounting for Safety Barriers Degradation in the Risk Assessment of Oil and Gas Systems by Multistate Bayesian Networks. *Reliability Engineering & System Safety*, *216*, 107943. https://doi.org/10.1016/J.RESS.2021.107943

Di Maio, F., Scapinello, O., Zio, E., Cincotta, S., Crivellari, A., Decarli, L., & Rosa, L. (2021). A Bayesian Regularized Artificial Neural Network for the Estimation of the Ignition Probability in Accidents in Oil & Gas Plants. *Proceedings of the 31st European Safety and Reliability Conference*, 2310–2314. https://doi.org/10.3850/978-981-18-2016-8_703-cd

Dömstedt, P., Lundberg, M., & Szakálos, P. (2020). Corrosion studies of a low alloyed Fe–10Cr–4Al steel exposed in liquid Pb at very high temperatures. *Journal of Nuclear Materials*, *531*. https://doi.org/10.1016/j.jnucmat.2020.152022

Dong, G., Han, W., & Wang, Y. (2021). Dynamic Bayesian Network-Based Lithium-Ion Battery Health Prognosis for Electric Vehicles. *IEEE Transactions on Industrial Electronics*, *68*(11), 10949–10958. https://doi.org/10.1109/TIE.2020.3034855

Driessens, K., & Matwin, S. (2004). Integrating Guidance into Relational Reinforcement Learning. *Machine Learning*, *57*, 271–304.

Ebisawa, K., Teragaki, T., Nomura, S., Abe, H., Shigemori, M., & Shimomoto, M. (2015). Concept and methodology for evaluating core damage frequency considering failure correlation at multi units and sites and its application. *Nuclear Engineering and Design*, *288*, 82–97. https://doi.org/10.1016/J.NUCENGDES.2015.01.002

Eisenberg, N. A., & Sagar, B. (2000). Importance measures for nuclear waste repositories. *Reliability Engineering and System Safety*, *70*(3). https://doi.org/10.1016/S0951-8320(00)00050-8

Energy Institute. (2006). *Ignition Probability Review, Model Development and Look-up Correlations. IP Research Report. London: Energy Institute*.

Fang, J., Shaver, D. R., Tomboulides, A., Min, M., Fischer, P., Lan, Y. H., Rahaman, R., Romano, P., Benhamadouche, S., Hassan, Y. A., Kraus, A., & Merzari, E. (2021). Feasibility of full-core pin resolved CFD simulations of small modular reactor with momentum sources. *Nuclear Engineering and Design*, *378*. https://doi.org/10.1016/j.nucengdes.2021.111143

Flage, R., Baraldi, P., Zio, E., & Aven, T. (2013). Probability and Possibility-Based Representations of Uncertainty in Fault Tree Analysis. *Risk Analysis*, *33*(1), 121–133. https://doi.org/10.1111/j.1539-6924.2012.01873.x

Floudas, C. A., & Lin, X. (2005). Mixed Integer Linear Programming in Process Scheduling: Modeling, Algorithms, and Applications. *Annals of Operations Research*, *139*, 131–162.

Fonoberova, M., Fonoberov, V. A., & Mezić, I. (2013). Global sensitivity/uncertainty analysis for agent-based models. *Reliability Engineering and System Safety*, *118*. https://doi.org/10.1016/j.ress.2013.04.004

Francis, R. A., Guikema, S. D., & Henneman, L. (2014). Bayesian Belief Networks for predicting drinking water distribution system pipe breaks. *Reliability Engineering and System Safety*, *130*, 1–11. https://doi.org/10.1016/j.ress.2014.04.024

Friedrichs, F., & Igel, C. (2005). Evolutionary tuning of multiple SVM parameters. *Neurocomputing*, *64*(1-4 SPEC. ISS.), 107–117. https://doi.org/10.1016/j.neucom.2004.11.022

Gabbar, H. A., & Esteves, O. L. A. (2022). Real-Time Simulation of a Small Modular Reactor in-the-Loop within Nuclear-Renewable Hybrid Energy Systems. *Energies*, *15*(18). https://doi.org/10.3390/en15186588

Gelbrich, M. (1990). On a Formula for the L2 Wasserstein Metric between Measures on Euclidean and Hilbert Spaces. *Mathematische Nachrichten*, *147*(1). https://doi.org/10.1002/mana.19901470121

GeNie. (n.d.). Decision Systems Laboratory, University of Pittsburg. Available at: http://www.genie.sis.pitt.edu.

Gershman, S. J., & Daw, N. D. (2017). Reinforcement Learning and Episodic Memory in Humans and Animals: An Integrative Framework. *Annual Review of Psychology*, *68*(1), 101–128. https://doi.org/10.1146/annurev-psych-122414-033625

Givens, C. R., & Shortt, R. M. (2002). A class of Wasserstein metrics for probability distributions. *Michigan Mathematical Journal*, *31*(2). https://doi.org/10.1307/mmj/1029003026

Goble, R., & Bier, V. M. (2013). Risk Assessment Can Be a Game-Changing Information Technology-But Too Often It Isn't. *Risk Analysis*, *33*(11). https://doi.org/10.1111/risa.12055

Grondman, I., Busoniu, L., Lopes, G. A. D., & Babuška, R. (2012). A survey of actor-critic reinforcement learning: Standard and natural policy gradients. In *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews* (Vol. 42, Number 6, pp. 1291–1307). https://doi.org/10.1109/TSMCC.2012.2218595

Guidelines for Risk Based Process Safety. (2010). In *Guidelines for Risk Based Process Safety*. https://doi.org/10.1002/9780470925119

Güneyisi, E. M., & Altay, G. (2008). Seismic fragility assessment of effectiveness of viscous dampers in R/C buildings under scenario earthquakes. *Structural Safety*, *30*(5). https://doi.org/10.1016/j.strusafe.2007.06.001

Guojin, Z., Yonghang, C., Wenjing, Z., & Min, D. (2021). Research on evaluation and inspection of pressure relief valve. *IOP Conference Series: Materials Science and Engineering*, *1043*(4). https://doi.org/10.1088/1757-899X/1043/4/042017

Hakobyan, A., Aldemir, T., Denning, R., Dunagan, S., Kunsman, D., Rutt, B., & Catalyurek, U. (2008). Dynamic generation of accident progression event trees. *Nuclear Engineering and Design*, *238*(12). https://doi.org/10.1016/j.nucengdes.2008.08.005

Hamel, J., Li, M., & Azarm, S. (2010). Design improvement by sensitivity analysis under interval uncertainty using multi-objective optimization. *Journal of Mechanical Design*, *132*(8). https://doi.org/10.1115/1.4002139

Han, Y., Zhen, X., & Huang, Y. (2022). Multi-objective optimization for preventive maintenance of offshore safety critical equipment integrating dynamic risk and maintenance cost. *Ocean Engineering*, *245*, 110557. https://doi.org/10.1016/J.OCEANENG.2022.110557

Hao, Z., Di Maio, F., & Zio, E. (2023). A sequential decision problem formulation and deep reinforcement learning solution of the optimization of O&M of cyber-physical energy systems (CPESs) for reliable and safe power production and supply. *Reliability Engineering and System Safety*, *235*. https://doi.org/10.1016/j.ress.2023.109231

Hassija, V., Senthil Kumar, C., & Velusamy, K. (2014). Probabilistic safety assessment of multi-unit nuclear power plant sites - An integrated approach. *Journal of Loss Prevention in the Process Industries*, *32*(1), 52–62. https://doi.org/10.1016/j.jlp.2014.07.013

He, S., Ye, Y., Wang, M., Zhang, J., Tian, W., Qiu, S., & Su, G. H. (2025). A machine learning and CFD based approach for fouling rapid prediction in shell-and-tube heat exchanger. *Nuclear Engineering and Design*, *432*, 113759. https://doi.org/10.1016/J.NUCENGDES.2024.113759

Health and Safety Executive (HSE). (2013). *Methods of Approximation and Determination of Human Vulnerability for Offshore Major Accident Hazard Assessment. Health and Safety Executive, Bootle*.

Helton, J. C. (1993a). Risk, uncertainty in risk, and the EPA release limits for radioactive waste disposal. *Nuclear Technology*, *101*(1). https://doi.org/10.13182/NT93-A34765

Helton, J. C. (1993b). Uncertainty and sensitivity analysis techniques for use in performance assessment for radioactive waste disposal. *Reliability Engineering and System Safety*, *42*(2–3). https://doi.org/10.1016/0951-8320(93)90097-I

Hosseini, S. A., Roma, G., Maio, F. Di, & Zio, E. (2026). Dynamic Bayesian Networks for Modelling Chemical Degradation in Concrete Structures of Nuclear Waste Repositories Exposed to Climate Change. *Reliability Engineering & System Safety*. https://doi.org/10.1016/j.ress.2026.112250

Howard, R. A. (1966). Dynamic Programming. *Management Science*, *12*(5).

Hu, Y., Miao, X., Zhang, J., Liu, J., & Pan, E. (2021). Reinforcement learning-driven maintenance strategy: A novel solution for long-term aircraft maintenance decision optimization.

Computers & Industrial Engineering, *153*, 107056. https://doi.org/10.1016/J.CIE.2020.107056

Huang, D., Chen, T., & Wang, M. J. J. (2001). A fuzzy set approach for event tree analysis. *Fuzzy Sets and Systems*, *118*(1), 153–165. https://doi.org/10.1016/S0165-0114(98)00288-7

Huke, A., Ruprecht, G., Weißbach, D., Gottlieb, S., Hussein, A., & Czerski, K. (2015). The Dual Fluid Reactor - A novel concept for a fast nuclear reactor of high efficiency. *Annals of Nuclear Energy*, *80*, 225–235. https://doi.org/10.1016/j.anucene.2015.02.016

Hussein, A., Gaber, M. M., Elyan, E., & Jayne, C. (2017). Imitation learning: A survey of learning methods. In *ACM Computing Surveys* (Vol. 50, Number 2). Association for Computing Machinery. https://doi.org/10.1145/3054912

Idaho National Engineering and Environmental Laboratory. (1999). *NUREG/CR-68 19, Vol. 1, Common-Cause Failure Event Insights - Emergency Diesel Generators*.

Iervolino, I., Giorgio, M., & Chioccarelli, E. (2013). Gamma degradation models for earthquake-resistant structures. *Structural Safety*, *45*, 48–58. https://doi.org/10.1016/J.STRUSAFE.2013.09.001

Ikonen, T. (2016). Comparison of global sensitivity analysis methods - Application to fuel behavior modeling. *Nuclear Engineering and Design*, *297*. https://doi.org/10.1016/j.nucengdes.2015.11.025

Ilham, M., & Okawa, T. (2023). A Simple Analytical Model to Predict the Freeze Plug Opening Time in Molten Salt Reactors. *Journal of Nuclear Engineering and Radiation Science*, *9*(4). https://doi.org/10.1115/1.4062879

Iman, R. L., & Hora, S. C. (1990). A Robust Measure of Uncertainty Importance for Use in Fault Tree System Analysis. *Risk Analysis*, *10*(3). https://doi.org/10.1111/j.1539-6924.1990.tb00523.x

International Atomic Energy Agency. (1996). *Defence in Depth in Nuclear Safety* (Number 10).

International Atomic Energy Agency. (2019). *IAEA Safety Standards Series No. SSG-2 (Rev. 1), Deterministic Safety Analysis for Nuclear Power Plants*.

International Atomic Energy Agency (IAEA). (2016). *SSR-2/1 (Rev. 1): Safety of Nuclear Power Plants: Design*.

International Atomic Energy Agency (IAEA). (2021). *SSG-67 - Seismic Design for Nuclear Installations*.

Ishlg-Ami, T., & Homma, T. (1990). An importance quantification technique in uncertainty analysis for computer models. *Proceedings of ISUMA 1990 - 1st International Symposium on Uncertainty Modeling and Analysis*. https://doi.org/10.1109/ISUMA.1990.151285

ISO 17776. (2016). *Petroleum and natural gas industries - Offshore production installations – Major accident hazard management during the design of new installations*.

Jaakkola, T., Singh, S. P., Jordan, M. I., & Jordan, M. (1994). Reinforcement Learning Algorithm for Partially Observable Markov Decision Problems. *Advances in Neural Information Processing Systems 7 (NIPS 1994)*, 345–352.

Jang, S., & Jae, M. (2020). A development of methodology for assessing the inter-unit common cause failure in multi-unit PSA model. *Reliability Engineering & System Safety*, *203*, 107012. https://doi.org/10.1016/J.RESS.2020.107012

Janssens, J., Talarico, L., Reniers, G., & Sörensen, K. (2015). A decision model to allocate protective safety barriers and mitigate domino effects. *Reliability Engineering and System Safety*, *143*. https://doi.org/10.1016/j.ress.2015.05.022

Jeon, B. G., Kim, S. W., Yun, D. W., Hahm, D., & Eem, S. (2022). Seismic Fragility Evaluation of Main Steam Piping of Isolated APR1400 NPP Considering the Actual Failure Mode. *Sustainability (Switzerland)*, *14*(14). https://doi.org/10.3390/su14148315

Jordan, M., Kleinberg, J., & Schölkopf, B. (2007). *Bayesian networks and decision graphs* (2n ed.). New York NY: Springer.

Kalantarnia, M., Khan, F., & Hawboldt, K. (2009). Dynamic risk assessment using failure assessment and Bayesian theory. *Journal of Loss Prevention in the Process Industries*, *22*(5). https://doi.org/10.1016/j.jlp.2009.04.006

Kang, D. Il, Hwang, M. J., Han, S. H., & Yang, J. E. (2009). Approximate formulas for treating asymmetrical common cause failure events. *Nuclear Engineering and Design*, *239*(2), 346–352. https://doi.org/10.1016/J.NUCENGDES.2008.10.004

Kanj, H., Aly, W. H. F., & Kanj, S. (2022). A Novel Dynamic Approach for Risk Analysis and Simulation Using Multi-Agents Model. *Applied Sciences (Switzerland)*, *12*(10). https://doi.org/10.3390/app12105062

Karayalcin, I. I. (1982). The analytic hierarchy process: Planning, priority setting, resource allocation. *European Journal of Operational Research*, *9*(1). https://doi.org/10.1016/0377-2217(82)90022-4

Kenneth Kitson, N., Constantinou, A. C., Guo, Z., Liu, Y., & Chobtham, K. (2022). *A survey of Bayesian Network structure learning*. https://doi.org/https://doi.org/10.48550/arXiv.2109.11415

Kerkkamp., D., Bukhsh., Z. A., Zhang., Y., & Jansen., N. (2022). Grouping of Maintenance Actions with Deep Reinforcement Learning and Graph Convolutional Networks. *Proceedings of the 14th International Conference on Agents and Artificial Intelligence - Volume 2: ICAART*, 574–585. https://doi.org/10.5220/0010907500003116

Khakzad, N. (2015). Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures. *Reliability Engineering and System Safety*, *138*, 263–272. https://doi.org/10.1016/j.ress.2015.02.007

Khakzad, N., Khan, F., & Amyotte, P. (2013). Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection*, *91*(1–2). https://doi.org/10.1016/j.psep.2012.01.005

Kijima, M. (1989). Some Results for Repairable Systems with General Repair. *Journal of Applied Probability*, *26*(1), 89–102. https://doi.org/10.2307/3214319

Kijima, M., Morimura, H., & Suzuki, Y. (1988). Periodical replacement problem without assuming minimal repair. *European Journal of Operational Research*, *37*(2), 194–203. https://doi.org/10.1016/0377-2217(88)90329-3

Kloos, M., & Peschke, J. (2006). MCDET: A probabilistic dynamics method combining Monte Carlo simulation with the discrete dynamic event tree approach. *Nuclear Science and Engineering*, *153*(2). https://doi.org/10.13182/NSE06-A2601

Knowles, M., Baglee, D., & Wermter, S. (2011). Reinforcement learning for scheduling of maintenance. *Res. and Dev. in Intelligent Syst. XXVII: Incorporating Applications and Innovations in Intel. Sys. XVIII - AI 2010, 30th SGAI Int. Conf. on Innovative Techniques and Applications of Artificial Intel.*, 409–422. https://doi.org/10.1007/978-0-85729-130-1_31

Konda, V. R., & Tsitsiklis, J. N. (1999). Actor-Critic Algorithms. *13th Annual Neural Information Processing Systems Conference, NIPS 1999*, 1008–1014.

Kuhn, H. W. (1956). Variants of the hungarian method for assignment problems. *Naval Research Logistics Quarterly*, *3*(4). https://doi.org/10.1002/nav.3800030404

Kuhnle, A., Jakubik, J., & Lanza, G. (2019). Reinforcement learning for opportunistic maintenance optimization. *Production Engineering*, *13*(1), 33–41. https://doi.org/10.1007/s11740-018-0855-7

Kumar, M., Whittaker, A. S., Kennedy, R. P., Johnson, J. J., & Kammerer, A. (2017). Seismic probabilistic risk assessment for seismically isolated safety-related nuclear facilities. *Nuclear Engineering and Design*, *313*. https://doi.org/10.1016/j.nucengdes.2016.12.031

Kumar, P., Sanderse, B., Boorsma, K., & Caboni, M. (2020). Global sensitivity analysis of model uncertainty in aeroelastic wind turbine models. *Journal of Physics: Conference Series*, *1618*(4). https://doi.org/10.1088/1742-6596/1618/4/042034

Lamarsh, J. (1981). SAFETY CONSIDERATIONS IN THE DESIGN AND OPERATION OF LIGHT WATER NUCLEAR POWER PLANTS. *Annals of the New York Academy of Sciences*, *365*.

Landucci, G., Argenti, F., Spadoni, G., & Cozzani, V. (2016). Domino effect frequency assessment: The role of safety barriers. *Journal of Loss Prevention in the Process Industries*, *44*, 706–717. https://doi.org/10.1016/J.JLP.2016.03.006

Landucci, G., Argenti, F., Tugnoli, A., & Cozzani, V. (2015). Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. *Reliability Engineering & System Safety*, *143*, 30–43. https://doi.org/10.1016/J.RESS.2015.03.023

Laskowska, E., & Vatn, J. (2019). State modelling and prognostics of safety valves used in the oil and gas industry. *Proceedings of the 29th European Safety and Reliability Conference (ESREL 2019), 22-26 September, Hannover, DE*.

Le Duy, T. D., & Vasseur, D. (2018). A practical methodology for modeling and estimation of common cause failure parameters in multi-unit nuclear PSA model. *Reliability Engineering & System Safety*, *170*, 159–174. https://doi.org/10.1016/J.RESS.2017.10.018

Lee, D., & Kwon, K. (2023). Dynamic Bayesian network model for comprehensive risk analysis of fatigue-critical structural details. *Reliability Engineering and System Safety*, *229*. https://doi.org/10.1016/j.ress.2022.108834

Lee, J. H., Yilmaz, A., Denning, R., & Aldemir, T. (2020). An online operator support tool for severe accident management in nuclear power plants using dynamic event trees and deep learning. *Annals of Nuclear Energy*, *146*. https://doi.org/10.1016/j.anucene.2020.107626

Lemoine, A. J., & Wenocur, M. L. (1985). On Failure Modeling. *Nav Res Logist*.

Lim, H. G., Yang, J. E., & Hwang, M. J. (2007). A quantitative analysis of a risk impact due to a starting time extension of the emergency diesel generator in optimized power reactor-1000. *Reliability Engineering & System Safety*, *92*(7), 961–970. https://doi.org/10.1016/J.RESS.2006.07.004

Lincoln, B., & Rantzer, A. (2006). Relaxing dynamic programming. *IEEE Transactions on Automatic Control*, *51*(8), 1249–1260. https://doi.org/10.1109/TAC.2006.878720

Linder, K. W., Adams, C. J., Andress, G. S., Bosma, M. J., Bouchard, J. K., Cable, E. A., Damon, W. A., Feld, J. M., Fisher, P. J., & Gagnon, G. (2002). *NFPA 25 Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems*.

Liu, C., Luo, R., & Macián-Juan, R. (2021). A new uncertainty-based control scheme of the small modular dual fluid reactor and its optimization. *Energies*, *14*(20). https://doi.org/10.3390/en14206708

Liu, X., Zheng, S., Wu, X., & Zheng, Y. (2021). Time-dependent Seismic Fragility Analysis of Buried Steel Pipes in Alkaline and Near-Neutral Soil Environments. *IOP Conference Series: Earth and Environmental Science*, *643*(1). https://doi.org/10.1088/1755-1315/643/1/012076

Liu, Y. (2020). Safety barriers: Research advances and new thoughts on theory, engineering and management. *Journal of Loss Prevention in the Process Industries*, *67*, 104260. https://doi.org/10.1016/J.JLP.2020.104260

Liu, Z., & Fan, J. (2014). Technology readiness assessment of Small Modular Reactor (SMR) designs. *Progress in Nuclear Energy*, *70*, 20–28. https://doi.org/10.1016/J.PNUCENE.2013.07.005

Luenberger, D. G., & Ye, Y. (2021). *Linear and nonlinear programming (4th ed.)*. Springer.

Maciulaitis, R., Grigonis, M., & Malaiskiene, J. (2018). The impact of the aging of intumescent fire protective coatings on fire resistance. *Fire Safety Journal*, *98*, 15–23. https://doi.org/10.1016/J.FIRESAF.2018.03.007

Mara, T. A., & Tarantola, S. (2008). Application of global sensitivity analysis of model output to building thermal simulations. *Building Simulation*, *1*(4). https://doi.org/10.1007/s12273-008-8129-5

Marchetti, S., Di Maio, F., & Zio, E. (2024a). A Physics-of-Failure (PoF) model-based Dynamic Bayesian Network for considering the aging of safety barriers in the risk assessment of industrial facilities. *Journal of Loss Prevention in the Process Industries*, *91*, 105402. https://doi.org/10.1016/J.JLP.2024.105402

Marchetti, S., Di Maio, F., & Zio, E. (2024b). A Physics-of-Failure (PoF) Model-based Dynamic Bayesian Network for Considering the Aging of Safety Barriers in the Risk Assessment of Industrial Facilities. *Submitted to Journal of Loss Prevention in the Process Industries*, *91*, 105402. https://doi.org/doi.org/10.1016/j.jlp.2024.105402

Marchetti, S., Di Maio, F., & Zio, E. (2025). An Integrated Deterministic and Probabilistic Safety Assessment of Multi-Unit Small Modular Reactors considering the degradation of shared safety barriers. *Nuclear Science and Engineering*. https://doi.org/https://doi.org/10.1080/00295639.2025.2515349

Marchetti, S., Di Maio, F., Zio, E., Decarli, L., La Rosa, L., & Nicotra, G. (2023). Key performance indicators for aging safety barriers in oil and gas facilities. *European Conference On Safety And Reliability (ESREL)*, 2230–2235. https://doi.org/10.3850/978-981-18-8071-1_P708-cd

Marchetti, S., Di Maio, F., Zio, E., Decarli, L., La Rosa, L., Nicotra, G., Tortora, A., Crivellari, A., & Cincotta, S. (2024). A Bayesian Regularized Artificial Neural Network For Estimating The Ignition Probability In Oil And Gas Plants. *European Safety and Reliability Conference (ESREL)*.

Martin, R. P., & Petruzzi, A. (2021). Progress in international best estimate plus uncertainty analysis methodologies. *Nuclear Engineering and Design*, *374*. https://doi.org/10.1016/j.nucengdes.2020.111033

Matsuoka, T., & Kobayashi, M. (1988). GO-FLOW: A New Reliability Analysis Methodology. *Nuclear Science and Engineering*, *98*(1), 64–78. https://doi.org/10.13182/NSE88-A23526

Matyas, K., Nemeth, T., Kovacs, K., & Glawar, R. (2017). A procedural approach for realizing prescriptive maintenance planning in manufacturing industries. *CIRP Annals*, *66*(1), 461–464. https://doi.org/10.1016/J.CIRP.2017.04.007

Meier, S. W. (2020). APPENDIX E-SEISMIC DESIGN OF STORAGE TANKS. In *API Standard 650*.

MISOF. (2018). *Modelling of ignition sources on offshore oil and gas facilities – MISOF, Report for Norwegian Oil and Gas Association, Report no: 107566/R2*. https://offshorenorge.no/contentassets/067198d80b9c4b039b879bd0c8ae42bf/107566_r2_final_.pdf

Misuri, A., & Cozzani, V. (2021). A paradigm shift in the assessment of Natech scenarios in chemical and process facilities. *Process Safety and Environmental Protection*, *152*, 338–351. https://doi.org/10.1016/J.PSEP.2021.06.018

Misuri, A., Landucci, G., & Cozzani, V. (2020). Assessment of safety barrier performance in Natech scenarios. *Reliability Engineering and System Safety*, *193*. https://doi.org/10.1016/j.ress.2019.106597

Misuri, A., Landucci, G., & Cozzani, V. (2021a). Assessment of risk modification due to safety barrier performance degradation in Natech events. *Reliability Engineering and System Safety*, *212*. https://doi.org/10.1016/j.ress.2021.107634

Misuri, A., Landucci, G., & Cozzani, V. (2021b). Assessment of safety barrier performance in the mitigation of domino scenarios caused by Natech events. *Reliability Engineering and System Safety*, *205*. https://doi.org/10.1016/j.ress.2020.107278

Mosleh, A. (1987). A multi-parameter, event-based common-cause failure model. *SMiRT9 Paper No. M7/3*.

Nasr, M. A., Loi, L., Riva, S., Zolfaghari, A., Wang, X., & Cammi, A. (2025). Enhancing multi-physics modeling in new-generation nuclear reactors using machine learning: Implementing Gaussian Process Regression for updating cross sections. *Annals of Nuclear Energy*, *224*, 111720. https://doi.org/10.1016/J.ANUCENE.2025.111720

National Research Council (US). (1999). *Impact of Advances in Computing and Communications Technologies on Chemical Science and Technology: Report of a Workshop. Washington (DC): National Academies Press (US);. 5, Needs and New Directions in Computing for the Chemical Process Industries.* https://www.ncbi.nlm.nih.gov/books/NBK44989/

Neapolitan, R. E. (2004). *Learning Bayesian Networks*. Northeastern Illinois University.

Nie, J., Braverman, J., Hofmayer, C., Choun, Y.-S., Kim, M. K., & Choi, I.-K. (2011). *Seismic Fragility Analysis of a Condensate Storage Tank with Age-Related Degradations*. Brookhaven National Laboratory.

Nuclear Regulatory Commission (NRC). (2011). *Westinghouse AP1000 Design Control Document* .

Nutt, W. T., & Wallis, G. B. (2004). Evaluation of nuclear safety from the outputs of computer codes in the presence of uncertainties. *Reliability Engineering and System Safety*, *83*(1), 57–77. https://doi.org/10.1016/j.ress.2003.08.008

Okumura, R., Okada, M., & Taniguchi, T. (2020). Domain-Adversarial and -Conditional State Space Model for Imitation Learning. *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 5179–5186. https://doi.org/10.1109/IROS45743.2020.9341705

Palenske, G. A., & Ornelas, G. N. (2023). Obstructions and Early Suppression Fast Response Sprinklers. *Fire Technology*, *59*(6), 3157–3184. https://doi.org/10.1007/s10694-021-01205-y

Parhizkar, T., Utne, I. B., & Vinnem, J. E. (2021). *Online Probabilistic Risk Assessment of Complex Marine Systems: Principles, Modelling and Applications*. Springer International Publishing. https://books.google.it/books?id=C2xREAAAQBAJ

Park, J. H., An, Y. J., Yoo, K. H., & Na, M. G. (2021). Leak flow prediction during loss of coolant accidents using deep fuzzy neural networks. *Nuclear Engineering and Technology*, *53*(8), 2547–2555. https://doi.org/10.1016/j.net.2021.01.040

Pedroni, N., Zio, E., & Cadini, F. (2017). Advanced Monte Carlo Methods and Applications. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, *3*(4). https://doi.org/10.1061/ajrua6.0000921

Peyré, G., & Cuturi, M. (2019). Computational optimal transport. *Foundations and Trends in Machine Learning*, *11*(5–6). https://doi.org/10.1561/2200000073

Pinciroli, L., Baraldi, P., Ballabio, G., Compare, M., & Zio, E. (2022). Optimization of the Operation and Maintenance of renewable energy systems by Deep Reinforcement Learning. *Renewable Energy*, *183*, 752–763. https://doi.org/10.1016/j.renene.2021.11.052

Pinciroli, L., Baraldi, P., & Zio, E. (2023). Maintenance optimization in industry 4.0. *Reliability Engineering and System Safety*, *234*. https://doi.org/10.1016/j.ress.2023.109204

Pitblado, R., Fisher, M., Nelson, B., Fløtaker, H., Molazemi, K., & Stokke, A. (2016). Concepts for dynamic barrier management. *Journal of Loss Prevention in the Process Industries*, *43*, 741–746. https://doi.org/10.1016/J.JLP.2016.07.005

Plischke, E. (2012). An adaptive correlation ratio method using the cumulative sum of the reordered output. *Reliability Engineering and System Safety*, *107*. https://doi.org/10.1016/j.ress.2011.12.007

Plischke, E., Borgonovo, E., & Smith, C. L. (2013). Global sensitivity measures from given data. *European Journal of Operational Research*, *226*(3), 536–550. https://doi.org/10.1016/J.EJOR.2012.11.047

Podila, K., Colton, A., Trottier, A., Pfeiffer, P., Chen, Q., Rao, Y., Sun, L., Huang, X., & Waddington, G. (2021). Demonstration of a coupled computational fluid dynamics approach for modelling non-water cooled small modular reactors. *Annals of Nuclear Energy*, *159*. https://doi.org/10.1016/j.anucene.2021.108346

Podofillini, L., Reer, B., & Dang, V. N. (2023). A traceable process to develop Bayesian networks from scarce data and expert judgment: A human reliability analysis application. *Reliability Engineering and System Safety*, *230*. https://doi.org/10.1016/j.ress.2022.108903

Poropudas, J., & Virtanen, K. (2011). Simulation metamodeling with dynamic Bayesian networks. *European Journal of Operational Research*, *214*(3), 644–655. https://doi.org/10.1016/j.ejor.2011.05.007

Poudel, B., Joshi, K., & Gokaraju, R. (2020). A Dynamic Model of Small Modular Reactor Based Nuclear Plant for Power System Studies. *IEEE Transactions on Energy Conversion*, *35*(2). https://doi.org/10.1109/TEC.2019.2956707

Prasad, M., Vinod, G., Gaikwad, A. J., & Ramarao, A. (2017). Site core damage frequency for multi-unit Nuclear Power Plants site. *Progress in Nuclear Energy*, *96*, 56–61. https://doi.org/10.1016/J.PNUCENE.2016.12.007

Pronzato, L., & Müller, W. G. (2012). Design of computer experiments: Space filling and beyond. *Statistics and Computing*, *22*(3). https://doi.org/10.1007/s11222-011-9242-3

Puppo, L., Pedroni, N., Maio, F. Di, Bersano, A., Bertani, C., & Zio, E. (2021). A Framework based on Finite Mixture Models and Adaptive Kriging for Characterizing Non-Smooth and Multimodal Failure Regions in a Nuclear Passive Safety System. *Reliability Engineering & System Safety*, *216*, 107963. https://doi.org/10.1016/J.RESS.2021.107963

Pusa, M. (2012). Perturbation-theory-based sensitivity and uncertainty analysis with CASMO-4. *Science and Technology of Nuclear Installations*, *2012*. https://doi.org/10.1155/2012/157029

Rocchetta, R., Bellani, L., Compare, M., Zio, E., & Patelli, E. (2019). A reinforcement learning framework for optimal operation and maintenance of power grids. *Applied Energy*, *241*, 291–301. https://doi.org/10.1016/J.APENERGY.2019.03.027

Romaric, S., Mouafo, T., Vaton, S., Courant, J.-L., Gosselin, S., Gosselin, S. A., Tembo, S. R., & Gosselin, S. (2016). A tutorial on the EM algorithm for Bayesian networks: application to

self-diagnosis of GPON-FTTH networks. *IWCMC 2016 : 12th International Wireless Communications & Mobile Computing Conference*, 369–376. https://doi.org/10.1109/IWCMC.2016.7577086ï

Ryu, J., & Jae, M. (2021). A quantification methodology of Seismic Probabilistic Safety Assessment for nuclear power plant. *Annals of Nuclear Energy*, *159*. https://doi.org/10.1016/j.anucene.2021.108296

Saaty, R. W. (1987). The analytic hierarchy process—what it is and how it is used. *Mathematical Modelling*, *9*(3–5), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8

Saaty, T. L. (2002). Decision making with the Analytic Hierarchy Process. *Scientia Iranica*, *9*(3). https://doi.org/10.1504/ijssci.2008.017590

Saltelli, A., Chan, K., & Scott, E. (2000). *Sensitivity Analysis*. Chichester: John Wiley & Sons.

Schulman, J., Levine, S., Moritz, P., Jordan, M. I., & Abbeel, P. (2015). Trust Region Policy Optimization. *International Conference on Machine Learning*. http://arxiv.org/abs/1502.05477

Schulman, J., Wolski, F., Dhariwal, P., Radford, A., & Klimov, O. (2017). Proximal Policy Optimization Algorithms. *ArXiv Preprint ArXiv:1707.06347*. http://arxiv.org/abs/1707.06347

Schuster, M., & Paliwal, K. K. (1997). Bidirectional recurrent neural networks. *IEEE Transactions on Signal Processing*, *45*(11). https://doi.org/10.1109/78.650093

Shahraki, H., & Shabakhty, N. (2015). Seismic Performance Reliability of RC Structures: Application of Response Surface Method and Systemic Approach. *Civil Engineering Infrastructures Journal*, *48*(1), 47–68.

Shi, H., Dong, Z., Xiao, N., & Huang, Q. (2021). Wind Speed Distributions Used in Wind Energy Assessment: A Review. In *Frontiers in Energy Research* (Vol. 9). Frontiers Media S.A. https://doi.org/10.3389/fenrg.2021.769920

Shi, J., Khan, F., Zhu, Y., Li, J., & Chen, G. (2018). Robust data-driven model to study dispersion of vapor cloud in offshore facility. *Ocean Engineering*, *161*, 98–110. https://doi.org/10.1016/J.OCEANENG.2018.04.098

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*, *19*(5), 494–506. https://doi.org/10.1016/J.JLP.2005.12.004

Sobral, J., & Guedes Soares, C. (2019). Assessment of the adequacy of safety barriers to hazards. *Safety Science*, *114*. https://doi.org/10.1016/j.ssci.2018.12.021

Special Metals. (n.d.). *Datasheet of Nickel 201 thermo mechanical properties*. Retrieved May 21, 2024, from https://www.specialmetals.com/documents/technical-bulletins/nickel-200.pdf

Stoffen, P. G. (n.d.). *Methods for the calculation of Physical Effects Due to releases of hazardous materials (liquids and gases)*.

Straub, D., & Der Kiureghian, A. (2010). Bayesian Network Enhanced with Structural Reliability Methods: Methodology. *Journal of Engineering Mechanics*, *136*(10). https://doi.org/10.1061/(asce)em.1943-7889.0000173

Sudheer, S., Kumar, L., Manjunath, B. S., Pasi, A., Meenakshi, G., & Prabhu, S. V. (2013). Fire safety distances for open pool fires. *Infrared Physics and Technology*, *61*, 265–273. https://doi.org/10.1016/j.infrared.2013.09.006

Sutton, R. S., & Barto, A. G. (2018). *Reinforcement Learning: An Introduction* (2nd edition). MIT Press, Cambridge.

Sutton, R. S., Mcallester, D., Singh, S., & Mansour, Y. (1999). Policy Gradient Methods for Reinforcement Learning with Function Approximation. *Advances in Neural Information Processing Systems*.

Syversveen, A. R. (1998). Noninformative Bayesian Priors. Interpretation and Problems with Construction and Applications. *Preprint Statistics*, *3*.

The Swedish National Board of Housing. (2011). *Building and Planning's general recommendations on the analytical design of a building's fire protection, BBRAD*. https://www.boverket.se/en/start/publications/publications/2013/the-swedish-national-board-of-housing-building-and-plannings-general-recommendations-on-the-analytical-design-of-a-buildings-fire-protection-bbrad/

Tombuyses, B., & Aldemir, T. (1997). CONTINUOUS CELL-TO-CELL MAPPING. *Journal of Sound and Vibration*, *202*(3), 395–415. https://doi.org/10.1006/JSVI.1996.0835

Tripathi, M., Singh, L. K., & Singh, S. (2020). Dynamic reliability framework for a Nuclear Power Plant using dynamic flowgraph methodology. *Annals of Nuclear Energy*, *143*. https://doi.org/10.1016/j.anucene.2020.107467

Turati, P., Pedroni, N., & Zio, E. (2017a). An Adaptive Simulation Framework for the Exploration of Extreme and Unexpected Events in Dynamic Engineered Systems. *Risk Analysis*, *37*(1), 147–159. https://doi.org/10.1111/risa.12593

Turati, P., Pedroni, N., & Zio, E. (2017b). Simulation-based exploration of high-dimensional system models for identifying unexpected events. *Reliability Engineering & System Safety*, *165*, 317–330. https://doi.org/10.1016/J.RESS.2017.04.004

Una, B., Marisol, G., Sooyoung, C., G. J, S., Ross, S., Brendan, K., & Lindley, B. (2024). Simulation of the NuScale SMR and Investigation of the Effect of Load-Following on Component Lifetimes. *Nuclear Technology*, *210*(1), 1–22. https://doi.org/10.1080/00295450.2023.2216973

United States Nuclear Regulatory Commission. (2002). *Auxiliary Feedwater System*. https://www.nrc.gov/docs/ML0307/ML030760397.pdf

United States Nuclear Regulatory Commission. (2011). *Emergency Diesel Generators*. https://www.nrc.gov/docs/ML1122/ML11229A061.html

Unwin, S. D., Lowry, P. P., & Toyooka, M. Y. (2012). Reliability models of aging passive components informed by materials degradation metrics to support long-term reactor operations. *Nuclear Science and Engineering*, *171*(1). https://doi.org/10.13182/NSE11-18

U.S. Nuclear Regulatory Commission. (2005). *Risk-Informed Assessment of Degraded Buried Piping Systems in Nuclear Power Plants*. https://www.nrc.gov/docs/ML0516/ML051650146.pdf

Vallender, S. S. (1974). Calculation of the Wasserstein Distance Between Probability Distributions on the Line. *Theory of Probability & Its Applications*, *18*(4). https://doi.org/10.1137/1118101

Van Der Schijff, O. J., & Bodemann, S. C. (n.d.). Corrosion of Piping in Dry and Preaction Fire Sprinkler Systems: Interim Results of Long Term Corrosion Testing Under Compressed Air and Nitrogen Supervision. *Corrosion 2013*. Retrieved http://southteksystems.com/

Van Houdt, G., Mosquera, C., & Nápoles, G. (2020). A review on the long short-term memory model. *Artificial Intelligence Review*, *53*(8). https://doi.org/10.1007/s10462-020-09838-1

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, *2017-December*. https://doi.org/10.1201/9781003561460-19

Villa, V., Paltrinieri, N., Khan, F., & Cozzani, V. (2016). Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. *Safety Science*, *89*. https://doi.org/10.1016/j.ssci.2016.06.002

Villani, C. (2007). Optimal Transport Old and New. *Media*, *338*.

Volkanovski, A., & Cizelj, L. (2014). Nuclear Power Plant Maintenance Optimization with Heuristic Algorithm. *Science and Technology of Nuclear Installations*, *2014*, 458016. https://doi.org/10.1155/2014/458016

Vorobyev, Y., & Kudinov, P. (2011). Development and application of a genetic algorithm based dynamic pra methodology to plant vulnerability search. *International Topical Meeting on Probabilistic Safety Assessment and Analysis 2011, PSA 2011*, *1*.

Vujić, J., Bergmann, R. M., Škoda, R., & Miletić, M. (2012). Small modular reactors: Simpler, safer, cheaper? *Energy*, *45*(1). https://doi.org/10.1016/j.energy.2012.01.078

Wang, D., Wang, X., Xu, J., Feng, D. C., & Xu, S. (2021). Framework for calculating seismic fragility function of urban road networks: A case study on Tangshan City, China. *Structure and Infrastructure Engineering*, *17*(11), 1508–1522. https://doi.org/10.1080/15732479.2020.1815804

Wang, J. P., Brant, L., Wu, Y. M., & Taheri, H. (2012). Probability-based PGA estimations using the double-lognormal distribution: Including site-specific seismic hazard analysis for four sites in Taiwan. *Soil Dynamics and Earthquake Engineering*, *42*, 177–183. https://doi.org/10.1016/j.soildyn.2012.06.015

Wang, J., & Zhao, M. (2020). Study on the effects of aging by accelerated weathering on the intumescent fire retardant coating for steel elements. *Engineering Failure Analysis*, *118*. https://doi.org/10.1016/j.engfailanal.2020.104920

Wang, M., He, X., Macian-Juan, R., & Wang, X. (2021). One-dimensional transient analysis of the dual-fluid reactor system. *Annals of Nuclear Energy*, *162*. https://doi.org/10.1016/j.anucene.2021.108481

Wang, P., & Aldemir, T. (2004). Some improvements in state/parameter estimation using the cell-to-cell mapping technique. *Nuclear Science and Engineering*, *147*(1). https://doi.org/10.13182/NSE04-A2415

Wang, X. (2018). Draining Time of the Dual Fluid Reactor. *12th International Topical Meeting on Nuclear Reactor Thermal-Hydraulics, Operation and Safety (NUTHOS-12)*. https://www.researchgate.net/publication/325846731

Wang, Y., Li, L., & Wang, D. (2017). A study of seismic probability safety assessment for a typical three-loop pressurized water reactor nuclear power plant. *25th International Conference on Nuclear Engineering*.

Willis, J. R. (1993). Modeling of emergency diesel generators in an 800 megawatt nuclear power plant. *IEEE Transactions on Energy Conversion*, *8*(3). https://doi.org/10.1109/60.257056

Xie, M. (2013). Thermodynamic and Gasdynamic Aspects of a Boiling Liquid Expanding Vapour Explosion. *Uitgeverij BOXPress, s-Hertogenbosch, The Netherlands*.

Xing, J., Zeng, Z., & Zio, E. (2019a). A framework for dynamic risk assessment with condition monitoring data and inspection data. *Reliability Engineering & System Safety*.

Xing, J., Zeng, Z., & Zio, E. (2019b). Dynamic business continuity assessment using condition monitoring data. *International Journal of Disaster Risk Reduction*, *41*. https://doi.org/10.1016/j.ijdrr.2019.101334

Xing, J., Zeng, Z., & Zio, E. (2020). Joint optimization of safety barriers for enhancing business continuity of nuclear power plants against steam generator tube ruptures accidents. *Reliability Engineering and System Safety*, *202*. https://doi.org/10.1016/j.ress.2020.107067

Xiong, Q., Du, P., Deng, J., Huang, D., Song, G., Qian, L., Wu, Z., & Luo, Y. (2022). Global sensitivity analysis for nuclear reactor LBLOCA with time-dependent outputs. *Reliability Engineering and System Safety*, *221*. https://doi.org/10.1016/j.ress.2022.108337

Yang, K. (1996). Failure probability evaluation for normally distributed load-strength model with unknown parameters. *Reliability Engineering & System Safety*, *51*(1), 115–118. https://doi.org/10.1016/0951-8320(95)00103-4

Young, G. A., & Sham, T.-L. (2018). *Initial assessment of metallurgical interaction of clad/base metal systems*. https://doi.org/10.2172/1506992

Yu, J., Song, Y., Tang, D., & Dai, J. (2021). A Digital Twin approach based on nonparametric Bayesian network for complex system health monitoring. *Journal of Manufacturing Systems*, *58*, 293–304. https://doi.org/10.1016/j.jmsy.2020.07.005

Yuan, S., Cai, J., Reniers, G., Yang, M., Chen, C., & Wu, J. (2022). Safety barrier performance assessment by integrating computational fluid dynamics and evacuation modeling for toxic gas leakage scenarios. *Reliability Engineering and System Safety*, *226*. https://doi.org/10.1016/j.ress.2022.108719

Yuan, S., Reniers, G., Yang, M., & Bai, Y. (2023). Cost-effective maintenance of safety and security barriers in the chemical process industries via genetic algorithm. *Process Safety and Environmental Protection*, *170*, 356–371. https://doi.org/10.1016/j.psep.2022.12.008

Zanotelli, M., Hines, J. W., & Coble, J. B. (2024). Combining Similarity Measures and Left-Right Hidden Markov Models for Prognostics of Items Subjected to Perfect and Imperfect Maintenance. *Nuclear Science and Engineering*. https://doi.org/10.1080/00295639.2024.2303165

Zeng, T., Chen, G., Reniers, G., & Men, J. (2022). Developing a barrier management framework for dealing with Natech domino effects and increasing chemical cluster resilience. *Process Safety and Environmental Protection*, *168*. https://doi.org/10.1016/j.psep.2022.10.024

Zeng, Z., & Zio, E. (2018). Joint Optimization of Business Continuity by Designing Safety Barriers for Accident Prevention, Mitigation and Emergency Responses. *2018 3rd*

International Conference on System Reliability and Safety (ICSRS), Barcelona, Spain, 316–320.

Zhang, J. (2009). A review of steel corrosion by liquid lead and lead–bismuth. *Corrosion Science*, *51*(6), 1207–1227. https://doi.org/10.1016/J.CORSCI.2009.03.013

Zhegang, M. (2022). *INL/RPT-22-66601, Enhanced Component Performance Study: Emergency Diesel Generators 1998–2020*.

Zhen, X., Han, Y., & Huang, Y. (2021). Optimization of preventive maintenance intervals integrating risk and cost for safety critical barriers on offshore petroleum installations. *Process Safety and Environmental Protection*, *152*, 230–239. https://doi.org/10.1016/J.PSEP.2021.06.011

Zheng, X., Itoh, H., Kawaguchi, K., Tamaki, H., & Maruyama, Y. (2015). Application of Bayesian nonparametric models to the uncertainty and sensitivity analysis of source term in a BWR severe accident. *Reliability Engineering & System Safety*, *138*, 253–262. https://doi.org/10.1016/J.RESS.2015.02.004

Zhou, T., Modarres, M., & Droguett, E. L. (2018). A review of multi-unit nuclear power plant probabilistic risk assessment research. *International Conference on Nuclear Engineering, Proceedings, ICONE*, *2*. https://doi.org/10.1115/ICONE26-81130

Zhou, W. (2011). Reliability Evaluation of Corroding Pipelines Considering Multiple Failure Modes and Time-Dependent Internal Pressure. *Journal of Infrastructure Systems*. https://doi.org/10.1061/(ASCE)

Zhu, Q., Qin, Y., Zhou, C., & Gao, W. (2018). Extended multilevel flow model-based dynamic risk assessment for cybersecurity protection in industrial production systems. *International Journal of Distributed Sensor Networks*, *14*(6), 1550147718779564. https://doi.org/10.1177/1550147718779564

Zio, E. (2014). Integrated deterministic and probabilistic safety assessment: Concepts, challenges, research directions. *Nuclear Engineering and Design*, *280*, 413–419. https://doi.org/10.1016/j.nucengdes.2014.09.004

Zio, E. (2016). Some challenges and opportunities in reliability engineering. *IEEE Transactions on Reliability*, *65*(4). https://doi.org/10.1109/TR.2016.2591504

Zio, E., Di Maio, F., & Tong, J. (2010). Safety margins confidence estimation for a passive residual heat removal system. *Reliability Engineering and System Safety*, *95*(8). https://doi.org/10.1016/j.ress.2010.03.006

Zio, E., & Miqueles, L. (2024). Digital twins in safety analysis, risk assessment and emergency management. In *Reliability Engineering and System Safety* (Vol. 246). https://doi.org/10.1016/j.ress.2024.110040