DISS. ETH NO.: 28043

FOR A SAFER NUCLEAR OUTLOOK: LEARNING FROM EXPERIENCE WITHIN AN ADAPTIVE & GENERIC PROBABILISTIC SAFETY ASSESSMENT FRAMEWORK

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH

(Dr. sc. ETH Zurich)

presented by

ALI AYOUB

MSc in NUCLEAR ENGINEERING

ETH ZURICH – EPF LAUSANNE

born on June 10, 1994

citizen of Lebanon

accepted on the recommendation of

Prof. Dr. Didier Sornette (ETH Zurich)

Prof. Dr. Wolfgang Kröger (ETH Zurich)

Prof. Dr. Haruko Wainwright (UC Berkeley)

2021

Abstract

With the goal of more intensively learning from experience to verify and improve the level of nuclear safety, and supporting the continued safe operation of critical infrastructures, with civil nuclear power plants in the core, we have carried out a project with the following inter-woven parts: 1) The continued development and establishment of a novel open comprehensive nuclear events database; 2) subsequent event and statistical analysis to more intensively learn from the past, and 3) extracting lessons for Probabilistic Safety Assessment (PSA) methods, in particular; 4) the development of harmonized and simplified PSA models, with a main motivation of enabling large-scale generic precursor analysis, being applied to relevant events within the database; and 5) exploiting the simplified PSA models and the performed large scale precursor analyses to offer a comprehensive statistical study of the operational risk in the civil nuclear sector, and develop an innovative methodology to learn from near misses and minor glitches, with the goal of constructing useful forecasts of extreme events. Furthermore, while looking into past disasters in different critical industries, we have realized that a deficiency in risk information transmission can be identified in most of the accidents' chains. This motivated us to carry out a parallel project to study the problem of risk information concealment by debunking its causes, importance, and suggesting practical solutions.

This dissertation is a compilation of four self-contained journal papers, in addition to a chapter presenting our two books in brief, all contributing to the literature of nuclear and critical infrastructures safety. The first chapter serves as an introduction of the dissertation, putting things in context, motivating the work, and presenting the topics to be dealt with throughout the thesis.

In chapter two, we present our ETH Zurich curated nuclear events database, along with its construction criteria, layout, accessibility, and detailed features. Analyzing the database, we find that the majority of the events/precursors worldwide have originated outside the nuclear island. Design residuals are the major contributor to systems' unreliability, with an occurrence frequency of more than 20%. Finally, the contribution of human/organizational factors is found to be similar to that of technical factors, highlighting the importance of vigilance by the plant staff and regulators.

In chapter three, we further utilize the ETH Zurich database to extract important safety and modeling lessons. We find that major accidents always trigger a wave of "reactive" reporting as well as changes in regulatory or corporate management that last 5 to 6 years, mostly due to increased alertness, improved transparency, uncovering latent design errors, and heightened public pressure. Furthermore, we suggest some steps that should be taken in order to limit future occurrences of common-cause failures (CCFs) based on the lessons learned from exploiting the database. Finally, we identify mild quantitative signs of aging for plants after 25 years.

In chapter four, we present our developed in-house generic PSA models for pressurized and boiling water reactors along with their interesting properties of being computationally light, transparent, user-friendly, and easily adaptable to account for major plant-specific differences. The models cover the common internal initiating events, frontline and support systems reliability and dependencies, human-factors, CCFs, and account for new factors typically overlooked in many developed PSAs. For quantification, the models use generic US reliability data, precursor analysis reports and studies, the ETHZ Curated Nuclear Events Database, and experts' opinions, while taking uncertainties into account. The models results are in good agreement with the results of detailed PSAs. The models are finally used for large-scale precursor analyses of relevant precursors in our database.

In chapter five, we utilize the results of the large-scale precursor analysis to perform a comprehensive statistical study of the operational risks in the civil nuclear sector. We show that the distribution of precursors' frequency vs severity follow the universal shape of a Pareto distribution, and identify a runaway Dragon Kings domain. Moreover, we reveal an interesting regime shift following the Three

Mile Island (TMI) accident. With respect to risk assessment, our main finding is that risk is dominated by exogenous factors (95%). We calculate that, by focusing on these factors, the frequency of accidents of the Fukushima scale can be brought down to about $6\ 10^{-6}$ per reactor-year.

In the sixth and last chapter, we present our work on the problem of risk information transmission within critical infrastructure companies. For brevity purposes and thesis formatting, the chapter will only introduce the problem and the research methodology; for the comprehensive study, details, and results, the reader is referred to our two Springer book-sequel presented in chapter 6, and should be published in early 2022. The first book presents case studies of 20 major disasters caused by intra-organizational silence and failure in upward feedback about observed risks before and during these disasters. The second book proposes practical solutions to the problem of risk information concealment mainly based on the professional opinions of 100 practitioners managing critical infrastructures around the world.

Kurzfassung

Mit dem Ziel, intensiver aus Erfahrungen zu lernen, um das Niveau der nuklearen Sicherheit zu überprüfen und zu verbessern, und den fortgesetzten sicheren Betrieb kritischer Infrastrukturen zu unterstützen, wobei zivile Kernkraftwerke im Mittelpunkt stehen, haben wir ein Projekt mit den folgenden miteinander verwobenen Teilen durchgeführt: 1) die Weiterentwicklung und Einrichtung einer neuartigen, offenen und umfassenden Datenbank für nukleare Ereignisse; 2) die anschließende Ereignis- und statistische Analyse, um intensiver aus der Vergangenheit zu lernen, und 3) die Gewinnung von Erkenntnissen insbesondere für probabilistische Sicherheitsbewertungsmethoden (PSA); 4) die Entwicklung harmonisierter und vereinfachter PSA-Modelle, deren Hauptmotivation darin besteht, eine groß angelegte generische Vorläuferanalyse zu ermöglichen, die auf relevante Ereignisse in der Datenbank angewandt wird; und 5) die Nutzung der vereinfachten PSA-Modelle und der durchgeführten groß angelegten Precursor-Analysen, um eine umfassende statistische Studie des Betriebsrisikos im zivilen Nuklearsektor zu erstellen und eine innovative Methode zu entwickeln, um aus near misses und kleineren Pannen zu lernen, mit dem Ziel, nützliche Prognosen für Extremereignisse zu erstellen. Darüber hinaus haben wir bei der Untersuchung vergangener Katastrophen in verschiedenen kritischen Industriezweigen festgestellt, dass bei den meisten Unfallketten ein Mangel bei der Übermittlung von Risikoinformationen festzustellen ist. Dies hat uns dazu veranlasst, ein paralleles Projekt zur Untersuchung des Problems der Verheimlichung von Risikoinformationen durchzuführen, indem wir die Ursachen und die Bedeutung dieses Problems entlarven und praktische Lösungen vorschlagen.

Diese Dissertation ist eine Zusammenstellung von vier in sich abgeschlossenen Journalbeiträgen sowie einem Kapitel, in dem unsere beiden Bücher kurz vorgestellt werden, die alle einen Beitrag zur Literatur über die Sicherheit von Kernkraftwerken und kritischen Infrastrukturen leisten. Das erste Kapitel dient als Einführung in die Dissertation, indem es die Dinge in einen Kontext stellt, die Arbeit motiviert und die Themen vorstellt, die in der gesamten Arbeit behandelt werden.

Im zweiten Kapitel stellen wir unsere von der ETH Zürich kuratierte Datenbank für nukleare Ereignisse vor, zusammen mit ihren Aufbaukriterien, ihrem Layout, ihrer Zugänglichkeit und ihren detaillierten Funktionen. Bei der Analyse der Datenbank stellen wir fest, dass die meisten Ereignisse/Vorläufer weltweit ihren Ursprung außerhalb der Nuklearinsel haben. Mit einer Häufigkeit von mehr als 20 % tragen Konstruktionsfehler am meisten zur Unzuverlässigkeit der Systeme bei. Schließlich wird festgestellt, dass der Beitrag menschlicher/organisatorischer Faktoren ähnlich groß ist wie der der technischen Faktoren, was die Bedeutung der Wachsamkeit des Anlagenpersonals und der Aufsichtsbehörden hervorhebt.

In Kapitel drei nutzen wir die Datenbank der ETH Zürich, um wichtige Erkenntnisse über Sicherheit und Modellierung zu gewinnen. Wir stellen fest, dass schwere Unfälle immer eine Welle "reaktiver" Berichterstattung sowie Änderungen in der Aufsichtsbehörde oder im Unternehmensmanagement auslösen, die 5 bis 6 Jahre andauern, meist aufgrund erhöhter Wachsamkeit, verbesserter Transparenz, der Aufdeckung latenter Konstruktionsfehler und erhöhtem öffentlichen Druck. Darüber hinaus schlagen wir einige Maßnahmen vor, die ergriffen werden sollten, um das Auftreten von common-cause failures (CCFs) in Zukunft zu begrenzen, und zwar auf der Grundlage der aus der Auswertung der Datenbank gewonnenen Erkenntnisse. Schließlich ermitteln wir leichte quantitative Anzeichen für die Alterung von Anlagen nach 25 Jahren.

In Kapitel vier stellen wir die von uns entwickelten generischen PSA-Modelle für Druck- und Siedewasserreaktoren vor, die sich dadurch auszeichnen, dass sie rechnerisch leicht, transparent,

benutzerfreundlich und leicht anpassbar sind, um die wichtigsten anlagenspezifischen Unterschiede zu berücksichtigen. Die Modelle decken die üblichen internen auslösenden Ereignisse, die Zuverlässigkeit der Front- und Unterstützungssysteme und deren Abhängigkeiten, menschliche Faktoren und CCFs ab und berücksichtigen neue Faktoren, die in vielen entwickelten PSAs typischerweise übersehen werden. Für die Quantifizierung verwenden die Modelle generische US-Zuverlässigkeitsdaten, Berichte und Studien über Vorläuferanalysen, die ETHZ-Datenbank für nukleare Ereignisse und Expertenmeinungen, wobei auch Unsicherheiten berücksichtigt werden. Die Ergebnisse der Modelle stimmen gut mit den Resultaten der detaillierten PSAs überein. Die Modelle werden schliesslich für gross angelegte Precursor-Analysen relevanter Vorläufer in unserer Datenbank verwendet.

In Kapitel fünf nutzen wir die Ergebnisse der großmaßstäblichen Precursor-Analysen, um eine umfassende statistische Untersuchung der Betriebsrisiken im zivilen Nuklearsektor durchzuführen. Wir zeigen, dass die Verteilung der Häufigkeit und des Schweregrads von Vorläufern der universellen Form einer Pareto-Verteilung folgt, und identifizieren einen Runaway Dragon-Kings Bereich. Darüber hinaus zeigen wir einen interessanten Regimewechsel nach dem Three Mile Island (TMI)-Unfall. In Bezug auf die Risikobewertung ist unsere wichtigste Erkenntnis, dass das Risiko von exogenen Faktoren dominiert wird (95 %). Wir berechnen, dass die Häufigkeit von Unfällen der Größenordnung von Fukushima auf etwa $6\ 10^{-6}$ pro Reaktorjahr gesenkt werden kann, wenn man sich auf diese Faktoren konzentriert.

Im sechsten und letzten Kapitel stellen wir unsere Arbeit zum Problem der Übertragung von Risikoinformationen innerhalb von Unternehmen mit kritischer Infrastruktur vor. Aus Gründen der Kürze und der Formatierung der Dissertation werden in diesem Kapitel nur das Problem und die Forschungsmethodik vorgestellt; für die umfassende Studie, Details und Ergebnisse wird der Leser auf unsere beiden Springer-Bücher verwiesen, die in Kapitel 6 vorgestellt werden und Anfang 2022 veröffentlicht werden sollen. Das erste Buch enthält Fallstudien zu 20 großen Katastrophen, die durch das Schweigen innerhalb der Organisation und das Versagen bei der Aufwärtsrückmeldung über beobachtete Risiken vor und während dieser Katastrophen verursacht wurden. Im zweiten Buch werden praktische Lösungen für das Problem der Verheimlichung von Risikoinformationen vorgeschlagen, die sich hauptsächlich auf die Meinungen von 100 Fachleuten stützen, die kritische Infrastrukturen in der ganzen Welt verwalten.

Acknowledgments

First and foremost, a genuine thank you goes to my Doktorvater, Professor Didier Sornette for all the interesting discussions and positive interactions throughout my PhD. I've learnt a lot from his non-mainstream and critical views on many scientific, political, and social dogmas. Didier was not just an academic mentor, he was a life mentor, and even beyond, a serious mentor during our weekend's wakeboarding and wake-surfing sessions. Also equally, I send my sincere gratitude to my second Doktorvater, and ultimately my wise friend, Professor Wolfgang Kröger, who was always available for any kind of a formal or informal chat or discussion. With his long experience, he has always had the big picture view, and with whom I enjoyed every collaboration on topics starting from nuclear safety, and not ending with autonomous driving systems safety. I would also like to thank Professor Haruko Wainwright for giving the time to review the work and serve on my examination committee. Many thanks to Dr. Spencer Wheatley for our early-days discussions, and to our industrial collaborators and funders, namely, the Gösgen and Leibstadt Nuclear Power Plants (KKG and KKL). I would also like to recognize my previous Master's students, Andrej Stankovski, Keyi Ma, and Xi Chen for the fruitful collaborations and interactions. A particular acknowledgment goes to Adriana Schellenbaum-Lenner for all the smooth and efficient administrative help.

A shout out to all my friends in Lebanon and abroad, with special regards going to Mohamad&Ghofran, Reda, Nour, Zeinab, Ali&Maud, Kevin F.C, Rajai, Rebecca, Mike, Amir, Richard, Blazhe, Ali Berjawi, Nawss, Ahmad, Dmitry, Hamza&Walaa, OBD, Marc, Abbass, Dongshuai, and many others including present and former lab members, who formed the social backbone during my Swiss times, and without whom things would have been much more complicated. An exceptional thank you goes to my second family and all-time buddies, the group of *Shabeb l Awedim.*

Finally and most importantly, all gratitude is to God, then my family and parents for their unconditional love, thoughts, and prayers, to my dearest grandparents whom I lost while abroad and will not be able to share my doctorate news with; thank you all.

Zurich, October 2021
Ali Ayoub

For a safer world…

Table of Contents

Chapter 1

Introduction

Understanding and improving safety are crucial issues for the nuclear sector, requiring continuous improvements and leveraging all potential knowledge, including empirical evidence and operational experience. With about 19'000 reactor-years of operation worldwide, the civil nuclear industry is considered a data-dense field with very rich and mature experience. Although well documented, much of this knowledge is maintained by utilities, regulators, and international organizations in different largely unsynchronized efforts that usually lack openness, comprehensiveness, scope, homogeneity, practical annotations, searchability, and technical risk metrics. The majority of the work is done at a country and sector-specific level, with limited efforts towards building an open comprehensive international database, with complications due to confidentiality in the field. Furthermore, through rigorous statistical analysis of comprehensive data, and precursor events in particular, many lessons can be learned including basic trends, causalities, importance of factors, origins, severity, the evolution of human versus non-human causes.

When it comes to models and methods that can support in data and events analyses, the Probabilistic Safety Assessment (PSA) method takes the major share, being the nuclear industry's standard tool for precursor analysis, risk estimation, and the means to understand safety and support risk-informed decision-making. Over the time, and through its extensive use, PSA witnessed rapid developments and reached high levels of details and sophistication. It evolved as a very plant-specific and site-specific method, capturing the very details of each plant, however, remains difficult to use or understand outside the circle of their developers or super-experts. The resulting complexities, in addition to the absence of a standardized PSA methodology and scope, made it difficult to compare results of different PSAs, and hindered possibilities for design-to-design and plant-to-plant safety comparisons. Therefore, PSAs became less suitable to understand industry-wide performance and big picture safety insights and trends. In this regard, simplified and generic PSAs, along with other potential benefits, can serve as a powerful tool for efficient and large-scale rough precursor analysis, where relaxed requirements may permit the inclusion of events and factors that are highly important, yet difficult to handle within "restrictive" standard PSA. Such a generic framework will allow for pooling experience across sites and plants, and will help to understand big picture safety issues and provide better risk estimates and statistics (pooled samples).

The main goal of this thesis is to fill the literature gap by 1) developing and presenting a comprehensive nuclear events database, focused on worldwide safety-relevant events and precursors; 2) exploiting the database to extract major safety lessons and statistics; 3) developing an in-house generic and adaptive PSA models (for light water reactors) and utilize them in the analysis of hundreds of precursors from the database; and 4) offer a comprehensive statistical study of the operational risk in the civil nuclear sector.

On a separate line, studying major nuclear catastrophes (Chernobyl and Fukushima) with a managerial and less technical eye, we have realized that the deficiency in risk information transmission before, during, and after the disasters have aggravated the situation. In fact, the summer 2012 report of the National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission exposed numerous examples of the widespread distortion of risk information within the Japanese nuclear industry, and of failure to pass on warnings from different specialists that the Fukushima-Daiichi plant was unprepared for a high-wave tsunami. Moreover, many of the organizational failures of internal

risk transmission which led to the Fukushima disaster resembled the failures which led to the 1986 Chernobyl catastrophe. The developers of the RBMK (high-power channel-type) reactors used at Chernobyl kept defects in the reactor design secret from the Soviet Politburo and concealed minor accidents at some Soviet nuclear power plants from operators at other nuclear plants. This concealment led to a situation where the management of Chernobyl NPP and its operators put reactor #4 of the plant into an extreme experimental/testing regime, in which the minor design defects of the RBMK reactor became significant; this ultimately led to a power surge causing the reactor to burn uncontrollably. To make matters worse, the management of the plant lied to the Soviet Politburo, playing down the actual condition of the reactor in the first few hours after the disaster. This postponed the crisis management response to the disaster and led to delay and inaccuracy in informing direct victims of the disaster, the Soviet public and the international community. This was an eye-opener to go and dig more into traces of this same problem of risk information concealment in other industries and critical infrastructures. For that, we have carried out a project to study this problem by debunking its causes, importance, and suggesting practical solutions, through analyzing past critical infrastructures disasters and leveraging the professional experience of practitioners.

Detailed overview of the thesis

This is a cumulative thesis, based on a series of four published and submitted papers, in addition to a chapter summarizing two books. Chapters 2 and 3 are based on two published journals jointly first-authored with Andrej Stankovski, and co-authored with Wolfgang Kröger and Didier Sornette. Chapter 4 is based on a submitted first-authored journal, co-authored with Wolfgang Kröger and Didier Sornette. Chapter 5 is based on a submitted first-authored journal, co-authored with Didier Sornette. Chapter 6 is based on two working co-authored Springer books, with Dmitry Chernov as first author, and Didier Sornette and Giovanni Sansavini as coauthors. My contribution in the four journal papers include the joint formulation of the research questions, the major implementation of the work, models, methods, analyses, and results, in addition to drafting the manuscripts. For the books, my contribution includes the analysis and the case study of some of the presented disasters (in nuclear, oil and gas, mining, dams), in addition to the preparation, conduction, and results' analysis of a major share of the interviews (55%). Below is a summary of each of the five thesis chapters.

The ETH Zurich curated nuclear events database: Layout, event classification, and analysis of contributing factors

In this chapter, we present an open database of nuclear events focused on worldwide safety significance with potentials for precursors. Explaining our events collection method and classification approach, each of the 1250 events in the database has been subjugated to coherent breakdown of features such as significance, origin, operating conditions, failure chains, contributing factors, severity of failures, and others. The events have been analyzed by experts and researchers in nuclear technology and safety, and are accessible using a custom-made user interface, making the database the largest open, comprehensive, curated, and user-friendly database in the world. We find that the majority of events (52%) have originated outside the nuclear island compared to within (48%). The most commonly affected components are related to the emergency power and emergency core cooling systems (ECCS). Design residuals are the major contributor to systems' unreliability, with an occurrence frequency of more than 20%. Finally, the importance of vigilance by the plant staff and regulators is highlighted, as the contribution of human/organizational factors is found to be similar to that of technical factors.

Precursors and startling lessons: Statistical analysis of 1250 events with safety significance from the civil nuclear sector

In this chapter, we analyze the ETH Zurich open curated database of 1250 worldwide nuclear events focused on safety significance with potentials for precursors, presented in the companion paper. We find that major accidents always trigger a wave of "reactive" reporting as well as changes in regulatory or corporate management that last 5 to 6 years, mostly due to increased alertness, improved transparency, uncovering latent design errors, and heightened public pressure. The leading causes for multi-unit events are found to be external triggers and design issues, confirming the need to adapt PSAs to cover multi-unit events accordingly. Common-cause failures (CCF) are found to occur fairly frequently, at different levels, and can significantly erode the safety of the plant. From the lessons learned from this analysis, we suggest that frequent review of components design and operating procedures, employing different teams for testing and maintenance activities on redundant trains, and sharing operational experience between plants of similar designs, are some of the steps that should be taken in order to limit future occurrences of CCFs and beyond that further improve plant safety. We identify some quantitative signs of aging for plants after the age of 25. Our findings stress the need for larger recording, reliance, and sharing of operational data to support learning from experience and avoid reoccurrence of accidents and events.

Generic and adaptive probabilistic safety assessment models: Precursor analysis and multi-purpose utilization

Motivated by learning from experience and exploiting existing knowledge in civil nuclear operations, in this chapter, we have developed in-house generic Probabilistic Safety Assessment (PSA) models for pressurized and boiling water reactors. The models are computationally light, handy, transparent, user-friendly, and easily adaptable to account for major plant-specific differences. They cover the common internal initiating events, frontline and support systems reliability and dependencies, human-factors, common-cause failures, and account for new factors typically overlooked in many developed PSAs. For quantification, the models use generic US reliability data, precursor analysis reports and studies, the ETHZ Curated Nuclear Events Database, and experts' opinions. Moreover, uncertainties in the most influential basic events are addressed. The generated results show good agreement with assessments available in the literature with detailed PSAs. We envision the models as an unbiased framework to measure nuclear operational risk with the same "ruler", and hence support inter-plant risk comparisons that are usually not possible due to differences in plant-specific PSA assumptions and scopes. The models can be used for initial risk screening, order-of-magnitude precursor analysis, and other research and pedagogic applications especially when no plant-specific PSAs are available. Finally, we are using the generic models for large-scale precursor analysis that will generate big picture trends, lessons, and insights.

Comprehensive quantitative large-scale assessment of nuclear power risks

How much should nuclear contribute to the energy portfolio needed to ensure a sustainable Earth environment for mankind? With the threats of global climate change and the emphasis on clean energy, nuclear opponents prominently raise the spectre of nuclear catastrophes. However, the dread of nuclear, often associated with singular catastrophic events such as Chernobyl or Fukushima and amplified by nuclear weapons terror, has limited quantitative scientific foundation, given the paucity

of data. In this chapter, we fill this gap by offering the first comprehensive statistical study of the operational risks in the civil nuclear sector. Using what is by far the largest recently constructed open database on accident precursors, and using our in-house generic probabilistic safety analysis (PSA) models for precursor analyses, we provide the first quantification of the severity of precursors to nuclear plant core damage, which takes the universal shape of a Pareto distribution. We also identify a special runaway Dragon Kings regime beyond the Pareto domain for the largest events. With respect to risk assessment, our main finding is that risk is dominated by exogenous factors (95%). We calculate that, by focusing on these factors, the frequency of accidents of the Fukushima scale can be brought down to about $6\ 10^{-6}$ per reactor-year (less than one severe radioactive release per 300 years of operation of the whole nuclear fleet). Our results also demonstrate the need for a global international cooperation focused on the construction of full blockchains of the cascades of accident precursors in order to create an even safer civil nuclear industry.

Risk Information transmission: Obstacles and practical solutions

When investigating past disasters, it soon becomes clear that before the disaster, some employees of the affected organization were aware of dangerous conditions that had the potential to escalate to a critical level. But for a variety of reasons, information about these risky conditions were not delivered to decision-makers. Consequently, the organization continued to move towards catastrophe, unaware of the possible threat - despite the fact that some of its employees clearly understood the likelihood of an impending disaster. In this chapter, we present our work on risk information transmission within critical infrastructure companies. Here, we only introduce the problem and the research methodology; the comprehensive study, details, and results can be found in our two Springer books cited in this chapter, which will be published by early 2022. The first book is focused on case studies of major disasters caused by intra-organizational silence and failure in upward feedback about observed risks before and during these disasters. The second book proposes practical solutions to the problem of risk information concealment mainly based on the professional opinions of 100 practitioners managing critical infrastructures around the world.

Chapter 2

The ETH Zurich curated nuclear events database: Layout, event classification, and analysis of contributing factors

We present an open database of nuclear events focused on worldwide safety significance with potentials for precursors. Explaining our events collection method and classification approach, each of the 1250 events in the database has been subjugated to coherent breakdown of features such as significance, origin, operating conditions, failure chains, contributing factors, severity of failures, and others. The events have been analyzed by experts and researchers in nuclear technology and safety, and are accessible using a custom-made user interface, making the database the largest open, comprehensive, curated, and user-friendly database in the world. We find that the majority of events (52%) have originated outside the nuclear island compared to within (48%). The most commonly affected components are related to the emergency power and emergency core cooling systems (ECCS). Design residuals are the major contributor to systems' unreliability, with an occurrence frequency of more than 20%. Finally, the importance of vigilance by the plant staff and regulators is highlighted, as the contribution of human/organizational factors is found to be similar to that of technical factors.

Based on **Ayoub, A.,** Stankovski, A., Kröger, W., & Sornette, D. (2021). The ETH Zurich curated nuclear events database: Layout, event classification, and analysis of contributing factors. *Reliability Engineering & System Safety*, *213*, 107781.

1. Introduction

Despite their dreadfulness, accidents in heavy industries can provide a unique opportunity for learning from mistakes and realizing existing weaknesses. This is usually well characterized with the direct technical back-fits that are implemented in the aftermath of major accidents. In addition to technical aspects, many human, organizational, and safety cultural principles are inferred from major accidents such as Chernobyl, Fukushima, Deepwater Horizon, Piper Alpha [1-3]. Therefore, a lot of work has been done to collect and manage historical precursory events, especially in critical infrastructures, as a way to reduce unsafe conditions, and support the safe operation in these industries. Gnoni and Saleh [4] discussed the importance and the challenges of building good near-miss collection and management systems in hazardous industries. They reason about cost savings that can be enjoyed when learning from near-misses rather than actual accidents. Zou et al. [5] developed a novel framework that can help to support inspections and reduce the occurrence frequency of operational events. The model integrates both qualitative root causes identification and statistical root cause analysis of operational events in nuclear power plants. Moura et al. [6] prepared a dataset of 238 major accidents covering many critical industries such as oil and gas, mining, chemicals, aviation, construction, and others. By analyzing the events in their dataset, they studied the interplay between human, organizational and technical factors that have contributed to historical major accidents. Moreover, they utilized the dataset to highlight important safety lessons, common patterns, and provide better risk

communication schemes with stakeholders to improve learning from experienced accidents [7]. Hauge et al. [8] analyzed 12000 events in different oil and gas facilities to study and quantify common cause failures (CCFs) in the oil and gas industry. Preischl et al. [9, 10] used operational experience from German nuclear power plants to study human operational errors and come up with statistical estimates of the corresponding human error probabilities (HEP). Park et al. [11] used a similar approach in studying HEP using a subset of 193 reports published by the Nuclear Event Evaluation Database (NEED), managed by the Korean Institute of Nuclear Safety (KINS). Kröger [12] analyzed a set of major power grid-related accidents and blackouts along with their causes, and realized the importance of the contextual and non-technical aspects in the safety of critical infrastructures.

In the nuclear industry, the accumulation of a vast knowledge stemming from more than 60 years of operating experience of a large fleet of nuclear power plants has continuously increased reactor safety by learning from mishaps, identifying strengths and weaknesses, and improving regulatory compliance. The utilities have done an excellent job in recording and keeping track of the operational experience over time, mandated by specific regulatory and IAEA requirements. With more than 18'000 reactor-years of operation worldwide [13], the civil nuclear industry is considered a data-dense field with a very rich and mature experience. Although well documented, much of this knowledge is maintained by utilities, regulators, and international organizations in different largely unsynchronized efforts that usually lack openness, comprehensiveness, and searchability. The majority of the work is done at a country and sector-specific level, with limited efforts towards building an open comprehensive international database, with complications due to confidentiality in the field.

In the following, we give a brief summary of major works done by different organizations around the world to collect nuclear operational experience and precursor data and state some of their limitations:

- The International Atomic Energy Agency (IAEA) and the OECD Nuclear Energy Agency (NEA) jointly manage an international database for nuclear operational experience, called the International Reporting System for Operating Experience (IRS) [14]. Participating countries report their events to the program – voluntarily – to foster information and knowledge exchange within the industry. The IRS database covers events starting 1981 onwards and focuses on safety-relevant events with detailed information intended for specialists. Unfortunately, the IRS database is not publicly accessible.
- The IAEA also maintains a website, the Nuclear Events Web-based System (NEWS) that is meant for the public [15]. The website contains INES rated events (International Nuclear and Radiological Event Scale) spanning a one-year time horizon. The majority of the NEWS events come from non-reactor facilities and are of minor safety significance or related to workplace radiation exposure.
- The World Association of Nuclear Operators (WANO) has the Performance Analysis program that collects and analyzes operating experience events from member utilities and provide reports on lessons learnt and performance indicators [16]. The WANO events are quite technically detailed, with access restricted to WANO members.
- The "European Clearinghouse on Operating Experience Feedback for Nuclear Power Plants" is an organization within the European Commission Joint Research Centre (JRC) in Petten (The Netherlands) that maintains a database of operational experience from around the world [17]. The database contains more than 55'000 events, dominated by events of minor safety relevance (licensee event reports, radiological events, etc.). The database contains events that go back to 1979 and the access can be granted on request.

- Other efforts at national levels can be found in regulatory archives compiled through reports provided by licensees, with the US Nuclear Regulatory Commission Licensee Event Reports (LERs) being the most famous and open ones (around 67'000 events of different safety significance [18]. The serious events are selected and further studied by the Accident Sequence Precursor (ASP) program that assigns risk metrics to these events, namely, conditional core damage probabilities [19] [20]. LERs and ASP reports are publicly available, yet with limited searchable annotations and navigation capacities.

In summary, nuclear operational experience is well documented, however, maintained in different unsynchronized user-specific efforts and databases that suffer remarkable limitations on openness, completeness, scope, homogeneity, practical annotations, searchability, and technical risk metrics. Recognizing these limitations, our group at the ETH Zurich have been developing an open nuclear events database focused on worldwide safety significant events that have the potential to be precursors of accidents [21, 22]. The database contains intermediate-level information and consistent classification of the events, making it accessible and transparent to the scientific community, industrial analysts, as well as the public. The database integrates information from different sources such as annual reports from national regulators, published IAEA INES events, operating experience databases, open access official reports, academic publications, serious newspaper articles, and others. All listed events in our database have a reference, with the majority coming from official sources.

The database covers events from the early days of the civil nuclear industry and up to our current days. At present, it contains slightly more than 1250 events from commercial nuclear power plants. Using our standardized classification framework (see section 2 below), each event has been systematically analyzed by multiple nuclear-safety experts and researchers, arriving at a coherent breakdown of features such as origin, cause, type of failure, operating mode, failure sequence, significance, and others. The database will be a useful asset for different statistical analyses, safety trends, accidents frequencies and predictions, contributors' importance, region-wise and technological comparisons, organizational factors, and others.

Moreover, acknowledging the complexity and multidimensionality of risk, we anticipate that the database – with its large pool of safety-relevant events and substantial features – will be able to answer the many complex and high-level questions on risks, which cannot be attained from analyzing single or limited number of events. Besides, the database can help as a potential benchmark for the adequacy and coverage of PSA (probabilistic safety assessment) models, shedding light on potential factors or dependences that might have been overlooked or inadequately treated [23]. The database is also supporting the development of generic data-driven PSA models for precursor analysis [24, 25] and will ultimately serve the greater purpose of providing big-picture views, and eventually supporting the safe operation of nuclear facilities.

The organization of the manuscript is as follows. In Section 2, we present the criteria that we have used to develop the classification of events into a coherent database. Section 3 presents the data access tool that we have developed in the form of a graphical user interface (GUI) for the ETHZ Curated Nuclear Events database. We illustrate its use by showing an example of a generated failure sequence. Section 4 presents the results of the statistical analyses of the main classification features with the goal of providing a synthetic understanding of the database. Section 5 concludes. An appendix presents the full sets of considered initiating events and systems used for the classification in the ETHZ Curated Nuclear Events database.

2. Data classification

We strive to include all events that are of safety relevance, have official INES rating of 2 or above and with accident-precursor potential. We also include general interesting and complicated events with important lessons to be learned. Approximately 66% of the included events are based on information published by the USNRC (LER and ASP reports), 10% on reports by JRC Clearinghouse, 6% on reports by the IAEA and 5% on reports by the Federal Office for the Safety of Nuclear Waste Management (BASE) in Germany. The remaining 13% of the events are based on official reports by various regulating bodies and agencies, news articles, publications from researchers and others. After a lengthy process, each of the 1256 events is characterized according to a set of classification criteria to arrive at a common taxonomy. As reporting varies from one source to another, we always try to obtain official reports containing as much technical information as possible, while standardizing the description of the events in the database. For some events whose reports have missing or for which the information is unreliable, only the explicitly stated failures are considered in our analysis and the events are accordingly labeled in the database. The database is continuously updated, therefore, for many of these events additional information can surface over time. Sections 2.1 to 2.5 below explain the used classification framework:

2.1 General information

Each event in the database is first described using a set of general information items:

- Short description of the event: a concise version of the event report, containing its most important information.
- Date of the event and location of the plant.
- The affected units by the event, relevant for multi-unit plants.
- Unit type: reactor technology (PWR, BWR, etc.), manufacturer, number of loops (in PWRs), and type of containment.
- Description of the affected systems during the event, affected component, and the total number of redundant trains.
- Common cause failure (CCF): reflects whether the event experienced a CCF (potential or actual) or did not.
- INES scores from official sources, or assessed by our team (for the majority of events) following the criteria established in [26]. Moreover, a Core Only INES rating has been implemented to differentiate core-relevant events from radiation exposure events.

2.2 Event details

Providing details for an event is often challenging due to common lack of information as well as the different reporting styles and rigor used by different countries and organizations. Nevertheless, we opted to provide sufficiently coherent details such as the origin, cause, type of the event, as well as the operating mode of the plant.

2.2.1 Origin

The origin refers to the physical location where an initiating event has originally occurred or a system was affected. In order to retain consistency, we have defined three system boundaries where the event can originate from (Fig. 1):

- Primary part: events affecting the nuclear island directly, i.e. initiating events or failures within the primary containment (loss of coolant accidents (LOCAs), reactivity induced accidents (RIAs), steam generator tube ruptures (SGTRs), failures in the emergency core cooling systems, etc.).
- Secondary part: initiating events or failures located in the "secondary" non-nuclear part of the plant, but within the plant boundary (internal floods and fires, switchyard failures, plant-centered losses of offsite power (LOOPs), failures in the service water, turbine building failures, auxiliary feedwater, emergency power systems, etc.).
- External: initiating events originating from outside of the plant boundary, without knowledge or reach of the plant personnel (external floods and fires, storms, earthquakes, tsunamis, grid-related LOOPs, etc.).

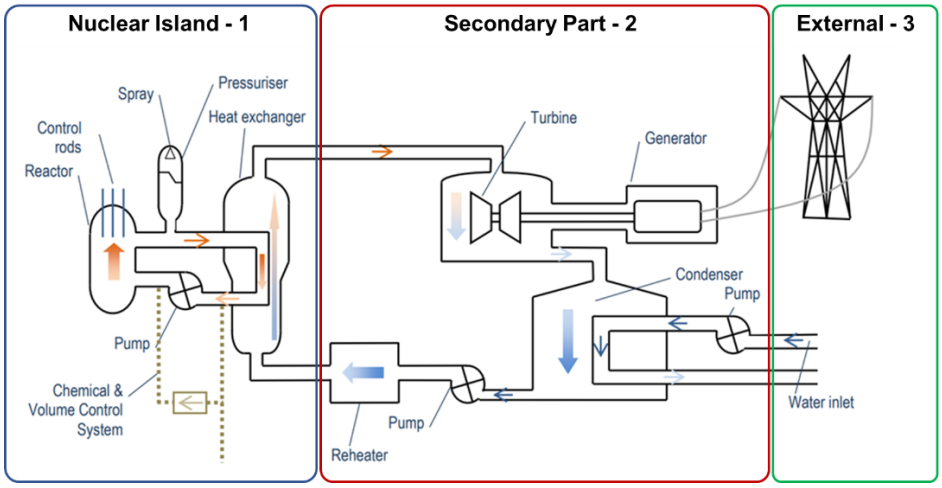


Fig. 1. Definition of plant boundaries for a pressurized water reactor (PWR) [27].

2.2.2 Type

The type of the event states the circumstances associated with the discovery of the event. This includes:

- Actual failures: cause noticeable acute problems and force an immediate response from the plant safety systems.
- Potential failures: latent errors, which may potentially result in failures of systems or trains and can greatly reduce the availability or reliability of the safety systems.

2.2.3 Operating mode

It describes the operating mode of the reactor during the event; three modes are utilized:

- Stable power: when the reactor is in a steady state power, regardless of the power level. Operating in hot standby mode is considered as stable power operation.
- Transitory state: when the reactors is in the process of increasing/decreasing power or hot shutdown, and has not reached a steady state.
- Cold shutdown state: when the reactor is subcritical, primary temperature is below the coolant threshold value of 100°C, and depressurized at one atm.

2.3 Event significance

The significance of an event is qualitatively assessed to mark events that are serious or highlight potential vulnerabilities of the plant. For an event to be considered significant, one or more of the following criteria should be fulfilled – similar to the screening criteria used in [28]:

- The event resulted in the unavailability or potential unavailability of a safety system, a safety function, or a redundant safety train for longer than allowed by technical specifications.
- The event simultaneously affected or had the potential to affect two or more safety systems or components.
- The event is an initiating event, which can result in core damage or a general transient with complications.
- The event is an initiating event followed or preceded by the failure of a safety system.
- The event resulted in a complete loss of a support system.

Several additional aspects are generally taken into account when analyzing the significance of an event, such as organizational or communicational deficiencies, frequency of occurrence of the event, success criteria, reactor operating mode, readiness/familiarity of the operator/staff with the event, and others.

2.4 Contributing factors

Contributing factors are generic factors that have caused or in some way contributed to the occurrence of the event (initiating event or system failure). The analysis and statistics of contributors are used to quantify the relative importance of the generic factors to the unreliability of safety systems and, more generally, to risk. Some contributors tend to affect a system as a whole, i.e. multiple redundant trains, and they are usually of common cause failure potential. These include:

- Design residuals, which include errors during initial design, construction errors, design modification errors, component manufacturing, lack of knowledge, incorrect actuation/trip logic, code and calculations issues, etc.
- Operator error of omission, i.e. manual actuation failures.
- Organizational/regulatory deficits and lack of safety culture contributions, communication errors, cost-cuts, etc.
- Inadequate procedures, encompassing both inadequate operating and maintenance/testing procedures.

Other contributors are most frequently bound to a single train unavailability, which include:

- Main component failures - failures of major components affecting one redundant train of a frontline or a support system (valves, pumps, breakers, emergency diesel generators (EDGs), etc.).
- Local support component failures - failures in the support systems that render a train unavailable (local power, local control and actuation, local cooling, lubrication, etc.).
- Global support component failures – they are inter-system support failures, rendering multiple trains in different safety systems unavailable (AC or DC busses, component cooling water, instrument air, etc.).
- Operator and technical staff errors (error of commission, tripping a functional train, failure to follow correct procedures, etc.).

- Testing and maintenance crew errors (errors during testing and maintenance actions, leftovers, failure to follow correct maintenance procedures, failure to detect or report apparent degraded conditions, etc.).
- Testing and maintenance unavailability: frontline or local support systems unavailability due to planned testing and maintenance actions.

Normal wear, aging, influence of the operating conditions and surroundings (stress, pressure, loads, moisture, radiation etc.) are some of the typical causes for the main and support component failures.

2.5 Failure sequences

The failure sequences feature of the database is used to demonstrate the chronological order in which an event unfolded, by focusing on the initiating event and the affected safety systems. It presents an efficient user-friendly visualization of an event, serving as a proxy for an empirical event tree. The visual representation of this feature is given in Fig. 2. This feature is envisioned to help deepen the understanding of correlations between certain safety systems, with the intent to uncover the existence of latent design and organizational errors, as well as causal factors that might affect the currently operating nuclear fleet.

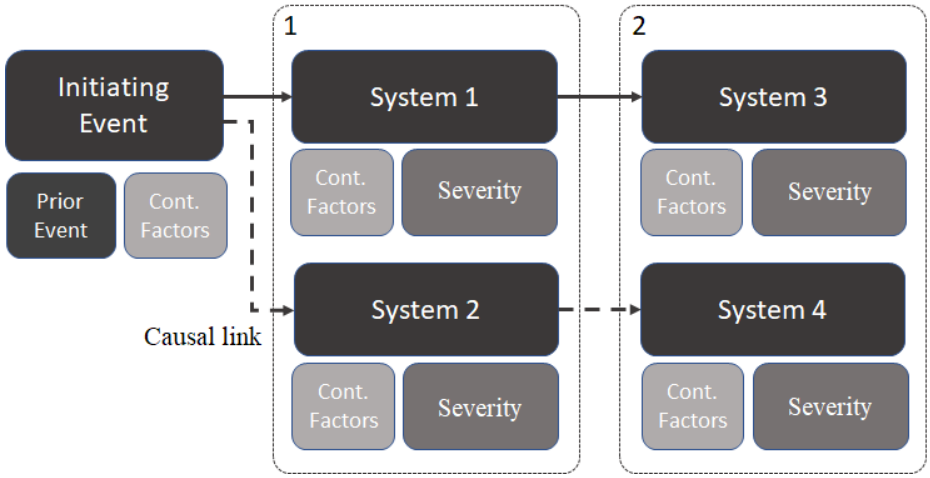


Fig. 2. Illustration of the failure sequences feature.

The failure sequence shows all the involved events and systems failures as main blocks and presents further details on these failures as descriptive blocks. The first descriptive block contains the contributing factors (*Cont. Factors*) which are covered in section 2.4. They are used in understanding the causes behind the initiating event and/or system failures. The descriptive block “prior event” is used to include the events or conditions that are relevant for the safety analysis and which occurred before the main initiating event. The severity block describes how severely a system was affected during the event. It contains the redundancy information of the components, and whether the system experienced a minor, partial, or a complete failure.

Furthermore, the failure sequences highlight any existing dependencies between the observed failures by utilizing causal links, which show if one failure was caused by another. Finally, the failure sequences use “time groups” to display simultaneous occurrences in one box (e.g. the system 1 and system 2 failures contained in dashed box 1 of Fig. 2 occurred simultaneously).

3. Database access tool

The database has a large amount of information and can be difficult to navigate. Therefore, a custom access tool was designed in Visual Basic to support a user-friendly navigation and multi-purpose utilization. With this user interface, users can filter out and extract events using the classification criteria discussed in section 2, display events and failure sequences, automatically generate statistical analyses, and export many different information and features. Fig. 3 displays the available features and possible statistics.

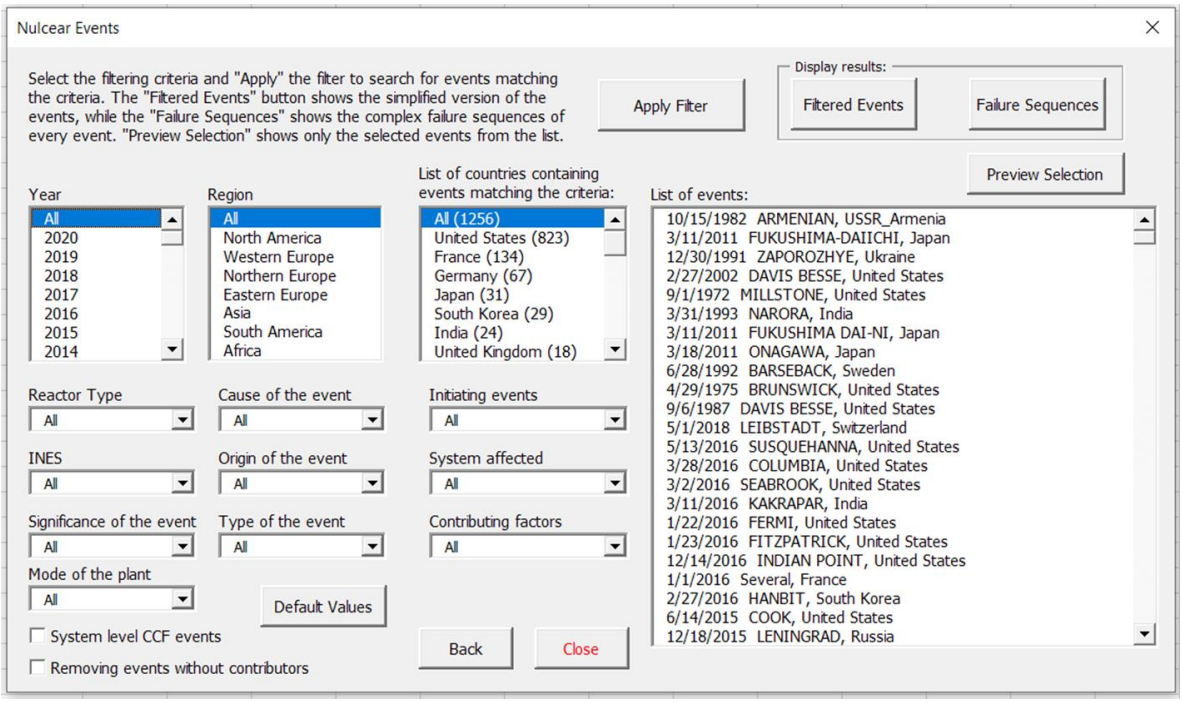


Fig. 3. Graphical user interface (GUI) of the ETHZ Curated Nuclear Events database showing filtering criteria and display options.

Fig. 4 shows an example of a generated failure sequence (as explained in Fig. 2) of the Fukushima Daiichi 2011 accident. Similar failure sequences can be generated by a single click for any event in the database. Fig. 4 is only meant to demonstrate a hands-on example of a failure sequence. However, the complete breakdown of an event contains much more information, including a curated description as explained in section 2.

Additional details regarding the usage of the access tool, meaning of the causal links, different notations, colors, and other features, can be retrieved from the database user manual on the database website [21].

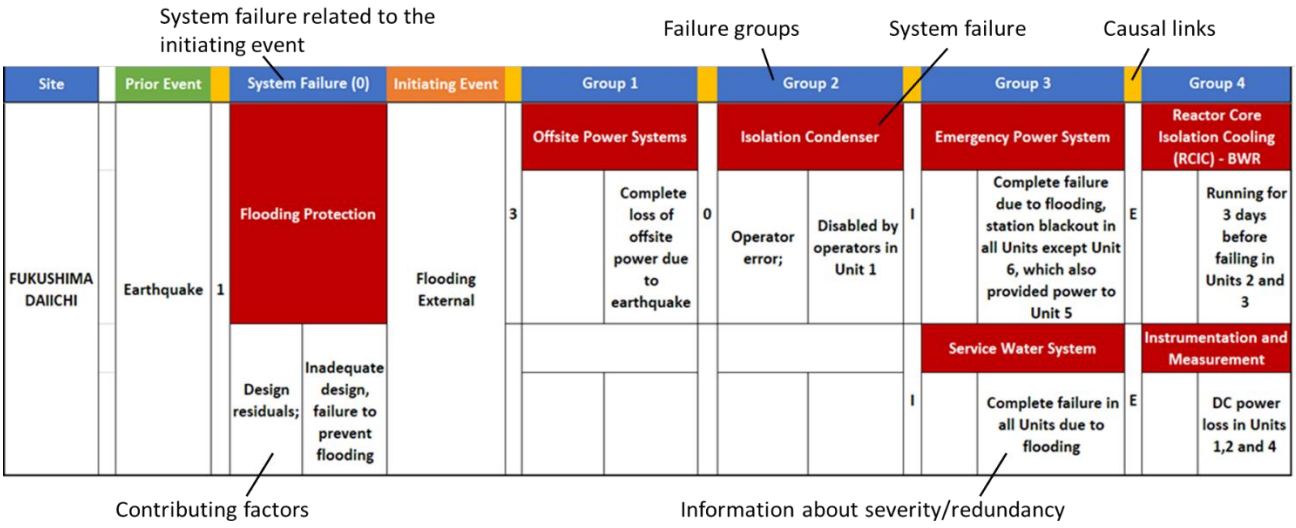


Fig. 4. Demonstration of the failure sequences using the Fukushima Daiichi 2011 nuclear accident.

4. Results and discussions

This section presents the results of the statistical analyses of the main classification features outlined before. The results aim at providing both a big picture view and a detailed analysis of characteristics of the included events.

4.1 General statistics

Divided by regions, the majority of the 1256 events of the database originated from North America with 841 events (67%), with the USA having 823 events. Western European countries follow with 272 events (22%), France being the largest contributor with 134 events. Asian[1] countries contributed with 91 events (7%), out of which Japan is leading having 31 events.

As mentioned, worldwide, there are more than 18'000 accumulated reactor-years of operating experience in commercial nuclear power plants. However, in order to maintain consistency, only the reactor years of the 352 reactors which had entries in our database have been taken into account in the subsequent analyses. Using the specific operational data of each region, the counts of events from each region were normalized, and the results of the occurrence rate per reactor-year for each region is shown in Fig. 5 (a). It should be noted that events from Europe were divided into Western (including Northern) and Eastern European events due to the fact of having different reactor designs and technologies, and different reporting styles and rates. The results indicate that North America has the highest occurrence rate - with a wide margin compared to the other regions - and this could be attributed to the high number of events originating from the USA, and their higher openness policy regarding events reporting. It is worth noting that the calculated rates should not be directly taken as a proxy for safety. However, they do definitely give an idea of the reporting practice and transparency of each region.

Pressurized light water reactors (PWRs) has the largest share in the database with 784 events (62%), followed by boiling water reactors (BWRs) with 382 events (30%). However, when taking into account the respective reactor-years of operating experience of each reactor type, the situation changes; Fig. 5 (b) shows that the rates of occurrence of events at BWRs are slightly higher that at PWRs, with an average BWR experiencing about 0.12 safety-relevant events per year.

[1] We were not successful to find and include events from China in our database.

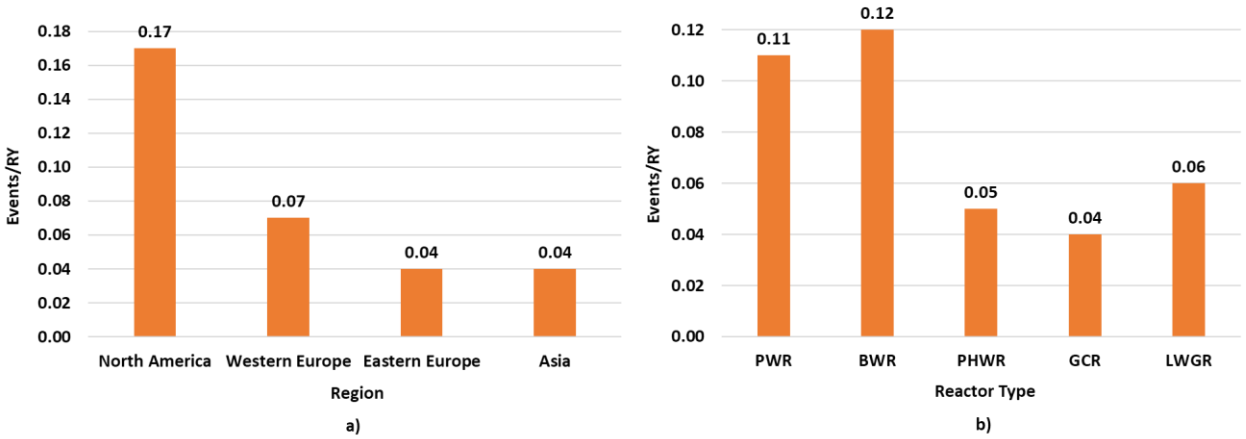


Fig. 5. Rates of events per reactor year, based on the: a) region and b) reactor type.

In section 2.2, we discussed how we classify events in the database based on their origin, type of the event, operating mode of the reactor, INES rating, and others. Based on this classification, we performed a statistical breakdown of events against different parameters. Fig. 6 shows the shares of the different reactor operating modes, origins, and failure types in the database. It should be noted that the origin of the event is only related to the initial trigger, which can be an initiating event or a system failure and is not an indicator for the further chain of the event.

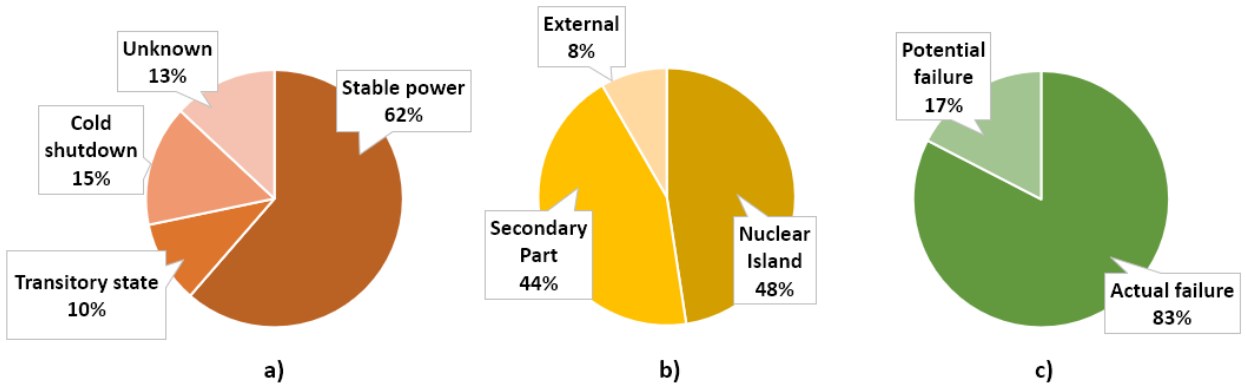


Fig 6. Breakdown of the number of events based on the: a) operating mode of the reactor; b) origin of the event; c) type of failure.

From Fig. 6 (a), it can be concluded that the majority of events occurred while the reactor was operating at stable power (62%). Keeping in mind that, most of the times, reactors are in power operation mode (the global median capacity factor was 86% in 2019 [13]), the high number of events occurring in this mode is not surprising. The number of safety relevant events occurring in cold shutdown and transitory states (15% and 10% respectively) is significant, bearing in mind the relatively short duration of these operation modes. This further stresses the importance of staying vigilant at all times: during normal operation, the reactor operating conditions (temperature, pressure, flux, etc.) can be challenging and the events tend to be quite serious physically. In transitory states, the reactor physical conditions change and the needed operator actions can lead to some unstable or undesirable conditions. Moreover, while the reactor is in cold shutdown, many safety systems and components can be unavailable due to testing and maintenance activities, therefore operational teams must be attentive and prepared for sudden disturbances or initiating events. Unfortunately, for 13% of the included events, the mode of the reactor was not disclosed in the official reports.

It can be seen from Fig. 6 (b) that the majority of events originated from either the nuclear island or the non-nuclear (secondary) part of the plant (48% and 44% respectively), while 8% of the events had

an external origin. This is quite interesting as it implies that events occurring in the non-nuclear part are as frequent and serious as events originating from the nuclear island, implying that similar attention should be given to the non-nuclear systems, structures, and components during the design phase, and in safety analyses.

As previously discussed, events can be divided into actual and potential, with the actual ones being events that cause an acute distress to the plant and require immediate action from the safety systems and/or the operators. In contrast, the potential failures are latent errors or deficiencies that could manifest themselves during some initiating events or unfavorable conditions. Events will be considered as potential failures only if no acute failures were observed in the whole chain of the event.

The chart in Fig. 6 (c) shows that the vast majority of events in the database were actual failures, with potential failures comprising only 17% of the events. This number represents only the aggregate share of potential failures in the whole database. However, plotting their share over time shows that potential failures have been increasing in relative terms (normalized by the total number of events per year), especially in the last 25 years (Fig. 7). This increase in reporting and realizing potential failures can be seen as an indication of the effectiveness of frequent inspections and regulatory checks, design changes, creep-related failures, procedural updates, and back-fits due to learning from experience [29].

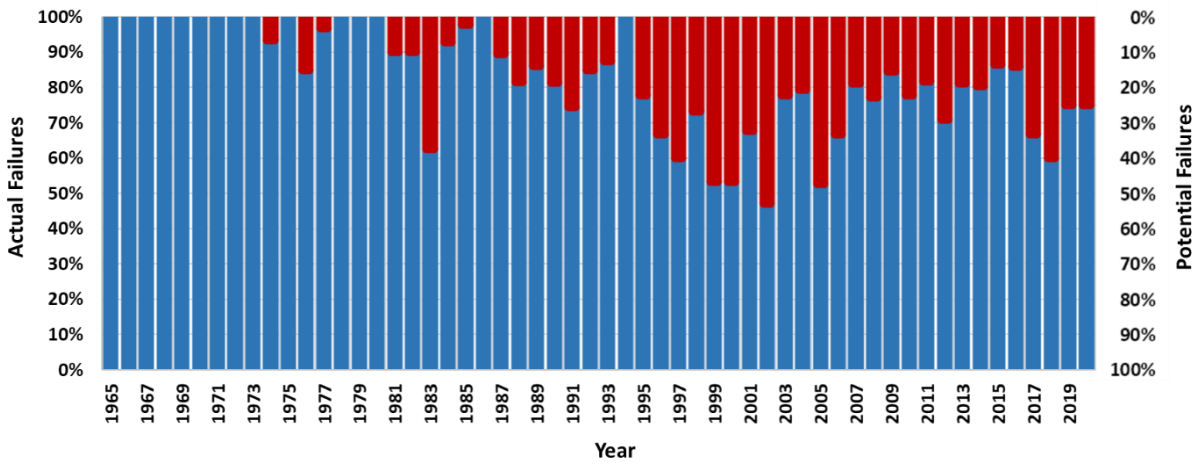


Fig. 7. Share of actual (blue) and potential (red) failures of the total events per year.

4.2 Severity of events

The guidelines for determining whether an event is significant or not was discussed in section 2.3. Following these guidelines, the number of identified significant events currently in the database is 1022, i.e. 81% of the total events. This is in line with our goal to mainly include and focus on events that are of safety relevance and are candidates to be labeled as precursors.

Moreover, as discussed in section 2.1, we have assigned a Core Only INES rating for each event to circumvent emphasis on events related to radiation exposure and injuries. The proposed technical risk metric is more relevant for the core, and integrates well with the probabilistic safety assessment framework. Fig. 8 shows the number of events in each severity group (INES between 0 and 7). As expected, the majority of included events have a low INES score, with anomalies and incidents (INES 0 to 2) comprising 97% of the events, and major incidents (INES 3) 2.6% of the events. Accidents (INES 4 to 7), fortunately, are very rare and were observed in only 0.8% of the total. However, they have provided major lessons and triggered major backfits worldwide.

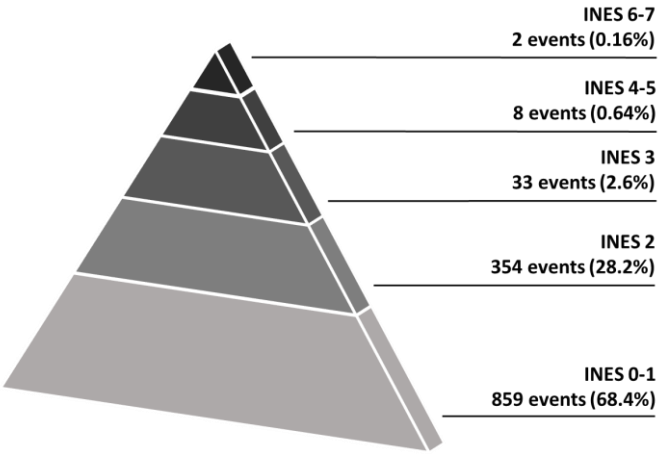


Fig. 8. Number of events based on their Core Only INES score.

Another way to look at these scores is to observe their distribution over time. The distribution of events based on their INES score per year of occurrence is portrayed in Fig. 9. The figure shows that the vast majority of nuclear accidents (80%), i.e. INES 4 or higher, occurred in the early days of nuclear power (1965-1980), when experience was very limited, industrial safety knowledge was embryonic, and transparent reporting was lacking. With the mounting operating experience and the lessons learned from the three major accidents: Three Mile Island 2 (1979), Chernobyl (1986) and Fukushima-Daiichi (2011), major changes in design, organization, communication, transparency and safety culture have been undertaken over the years, shaping the civil nuclear power industry into one of the safest and most reliable energy technologies. This have been reflected with the reduced number of serious incidents (INES 3) and accidents in the later years. Nevertheless, the Fukushima Daiichi accident remains a grim reminder that the occurrence of beyond-design-basis events and late implementation of safety upgrades can be devastating for the structural integrity of the plant.

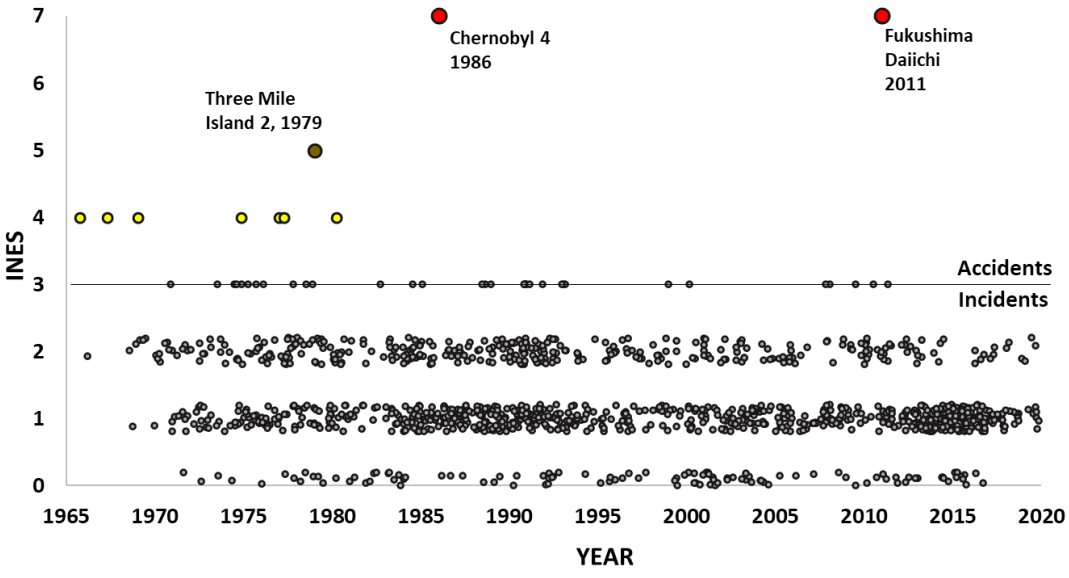


Fig. 9. Distribution of events based on their Core Only INES score per year of occurrence. For visibility, points are spread around their INES and year values.

4.3. Macro-analysis of contributing factors

Factors contributing to initiating events and systems failures were first discussed in section 2.4. These factors can be grouped into three macro-categories: technical, human and organizational factors (Fig.

10). Furthermore, we have realized that many events which were triggered by an external origin do not have contributors, as all of the subsequent system failures were caused by the external event. For this reason, in this analysis, the external initiators were added as a separate macro-category.

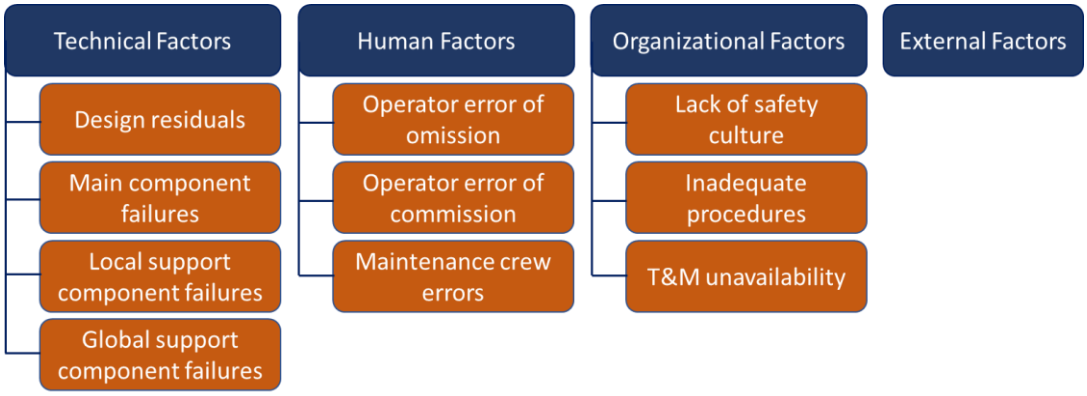


Fig. 10. Macro-classification of contributing groups. T&M means testing and maintenance.

Every event was analyzed based on this classification in order to observe the occurrence frequency of these contributors, as well as to study their importance. For 99 events (8% of the total), we assigned no contributing factors in the database, due to lack of information in their respective references. Therefore, these events are excluded from the subsequent discussion. The results from this analysis are presented in Table 1.

The vast majority of events had a single contributor (838 events – 72%), with the most frequently occurring groups being the technical factors with 42%, followed by human factors with 17%. Combinations of two contributor groups are very common and they were identified in 286 events (25%), with the most frequent one being the technical-organizational factors with 10%. It is also interesting to observe that a total of 33 events (3%) had a combination of 3 contributor groups simultaneously occurring, while a combination of all 4 contributing groups was never observed.

The cumulative contribution of technical factors is 63% of the total 1157 assessed events, human factors 30%, organizational factors 27%, and external initiators 9%. Surprisingly, organizational factors occur almost as frequently as the human factors. Thus, more attention needs to be given to organizational and safety culture retrofits by plant owners, operators and regulatory bodies.

Table 1. Macro-analysis of the contributing categories

Macro contributor	Number of events	Percentage of total
Only Technical	486	42.0%
Only Human	193	16.7%
Only Organizational	112	9.7%
Only External	47	4.1%
Technical-Human	70	6.1%
Technical-Organizational	113	9.8%
External-Technical	35	3.0%
Human-Organizational	57	4.9%
External-Human	5	0.4%
External-Organizational	6	0.5%
Technical-Human-Organizational	21	1.8%
External-Technical-Human	4	0.3%
External-Human-Organizational	2	0.2%
External-Technical-Organizational	6	0.5%
External-Technical-Human-Organizational	0	0.0%
Total	**1157**	**100.0%**

This preliminary analysis gives a "bird's view" of the leading contributors. However, delving deeper into the frequency of individual contributors (micro-contributors) will give us a better understanding of the outlined results.

4.4 Micro-analysis of causal and contributing factors

For the "micro-analysis", we will zoom in the already discussed "event-level" and move to a more detailed "failure-level" view, by considering the various systems that were affected during the chain of each event. The basis for this approach was outlined by the failure sequences presented in section 2.5. The previously discussed causal links aid in determining the connection between the potential causes and the resulting systems failures. The analysis considered 41 systems including

- safety systems (the different emergency core cooling systems (ECCS), auxiliary feedwater, emergency power system, etc.),
- systems necessary for normal operation of the plant (offsite power systems, main feedwater, service water system, etc.) and
- additional "systems", which are more closely related to a specific boundary encompassing multiple safety and/or non-safety grade components (primary cooling system, reactor pressure vessel, etc.).

For a complete list of the considered systems, please refer to the Appendix (Figs. A.2 and A.3).

Having this in mind, the results show that, in the 1256 events of the ETHZ database, a total of 1887 system failures were observed. The majority were safety-grade systems with 1230 failures (65%), while the remaining 657 failures (34%) were non-safety grade "normal operation" systems. Referring to the failure severity of the systems, around 32% of the systems had experienced a total loss of function, 29% partial, and the remaining 39% were only affected with no loss of function observed.

Two analyses will be presented in the following sections: one discussing the occurrence of initiating events with their contributing factors, and the second discusses the occurrence of safety system failures as well as their contributing factors. The second analysis will be performed only for the systems of the most common reactor types in the database, namely pressurized water reactors (PWR), boiling water reactors (BWR), and pressurized heavy water reactors (PHWR), which represent 97% of all events.

4.4.1 Analysis of initiating events

Around 48% (601 occurrences) of the events in the database contain an initiating event. Out of the 601 observed initiating events, the most dominating ones were the general transients with 221 events (37%), followed by loss of offsite power (LOOP) with 168 events (28%) (Fig. 11). The presented percentages of initiating events are in agreement with their relative occurrence rates in the USNRC generic values presented in [30, 31], which is in accordance with the USNRC being the major contributor to events in the database. For a complete list of the considered initiating events, please refer to the Appendix (Fig. A.1).

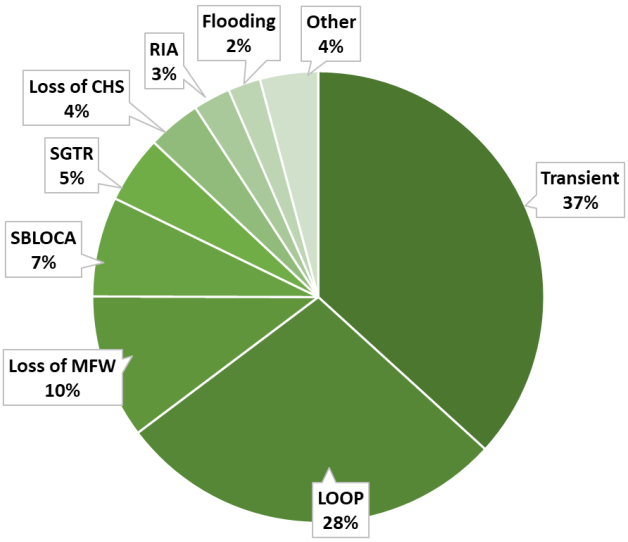


Fig. 11. Rate of occurrence of individual initiating events out of the total number of observed initiating events in the database. Meaning behind the abbreviations: LOOP – loss of offsite power; MFW – main feedwater; SBLOCA – small break loss-of-coolant accident; SGTR – steam generator tube rupture; CHS – condenser heat sink; RIA – reactivity induced accident.

By considering the underlying factors that can lead to the occurrence of an initiating event, the following causal factors were defined in addition to the contributing factors introduced in section 2.4:

- External factors: originating outside of the plant boundaries as defined in section 2.2.1 (e.g. grid disturbances leading to a loss of offsite power event).
- Previous initiators: other initiating events directly causing the main initiating event.
- Previous system failures: failures in a system affecting another, which ultimately triggered an initiating event. Generally, these events occur due to unanticipated interactions -- which are usually of mechanical/physical nature -- between systems (e.g., a problem in the turbine governor causing a generator load swing, and ultimately triggering a loss of main feedwater initiating event).

A total of 680 causal factors for the 601 initiating events were observed (the factors are not mutually exclusive, i.e. one initiating event can be caused by multiple factors). The vast majority of causal factors were the micro-contributing factors with 527 occurrences (78%) as shown in blue in Fig. 12. The most prominent ones among them were the main component failures (20%), followed by design residuals

(16%), testing and maintenance (T&M) errors (14%), and support component failures (12%). The majority of initiating events occurred due to failures within the plant boundaries. Nevertheless, there is a significant contribution of external factors with 93 occurrences (14%), and it should go without saying that the potential threats from external causes should never be underestimated.

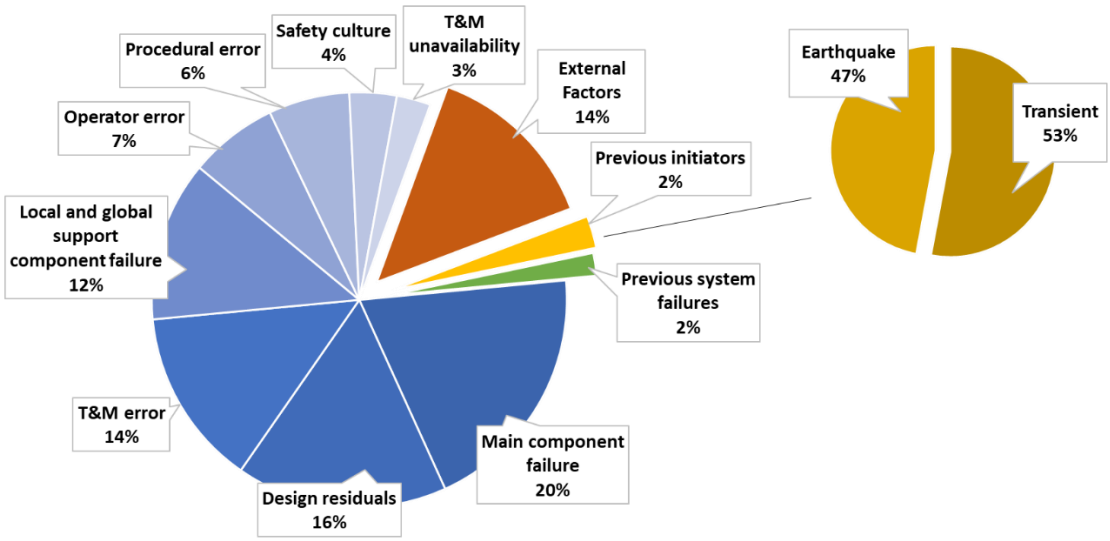


Fig. 12. Leading causes for the occurrence of initiating events. Meaning behind the abbreviation: T&M – testing and maintenance.

The causal contribution of previous system failures to initiating events is 2% of all occurrences.

Finally, previous initiators caused initiating events in only 2% of the cases, with them being either earthquakes or general transients.

4.4.2 Analysis of safety systems

Drawing a parallel to the discussion of initiating events above, a system failure can occur due to one or more of the following causal factors, in addition to the contributing factors introduced in section 2.4:

- Previous initiators: system failures partially or completely caused by an initiating event (e.g. LOOP causing loss of emergency core cooling systems (ECCS)).
- Previous system failures: system failures partially or completely caused by a preceding failure of another system due to unanticipated mechanical/physical interaction.

4.4.2.1 Analysis of PWR safety systems failures

Pressurized water reactors (PWRs) were present in 784 events, or 62% of the total events in the database, and in this analysis, we will focus only on the safety systems that were affected in these events. In PWR events, 818 safety systems failures occurred, the majority of which were related to failures in the emergency power system (145 occurrences – 18%), auxiliary feedwater system (122 occurrences – 15%) and high-pressure injection system (94 occurrences – 11%) as shown in Fig. 13.

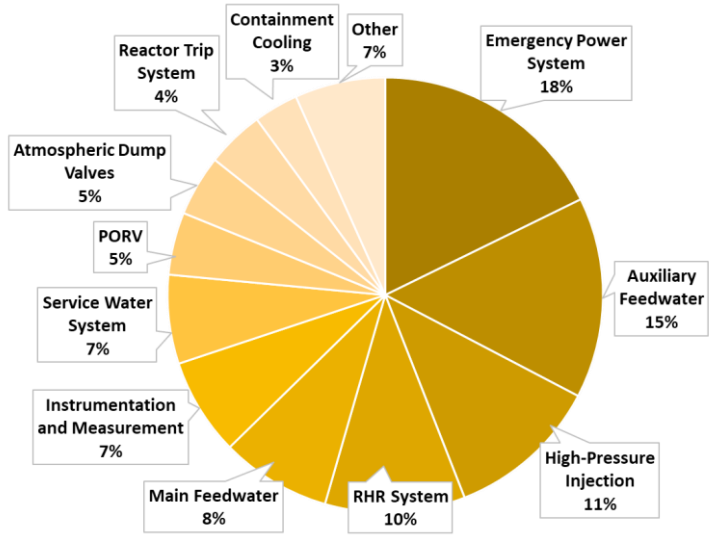


Fig. 13. Rate of occurrence of individual safety system failures out of the total number of observed safety system failures in PWRs. Meaning behind the abbreviation: PORV – pilot operated relief valve; RHR – residual heat removal.

The causes can be traced back to 887 factors, with the micro-contributing factors being the vast majority with a 90% share (shown in blue in Fig. 14). The most prominent ones among them were the design residuals with 197 (22%), followed by testing and maintenance errors with 154 occurrences (17%), main component failures (14%), and support component failures (14%). The share of safety systems failures caused by previous initiators (initiating events) is low, with only 38 occurrences (4%), the majority of which were transients (17 occurrences). Finally, the causal contribution of previous system failures to failures in PWR safety systems was 1%.

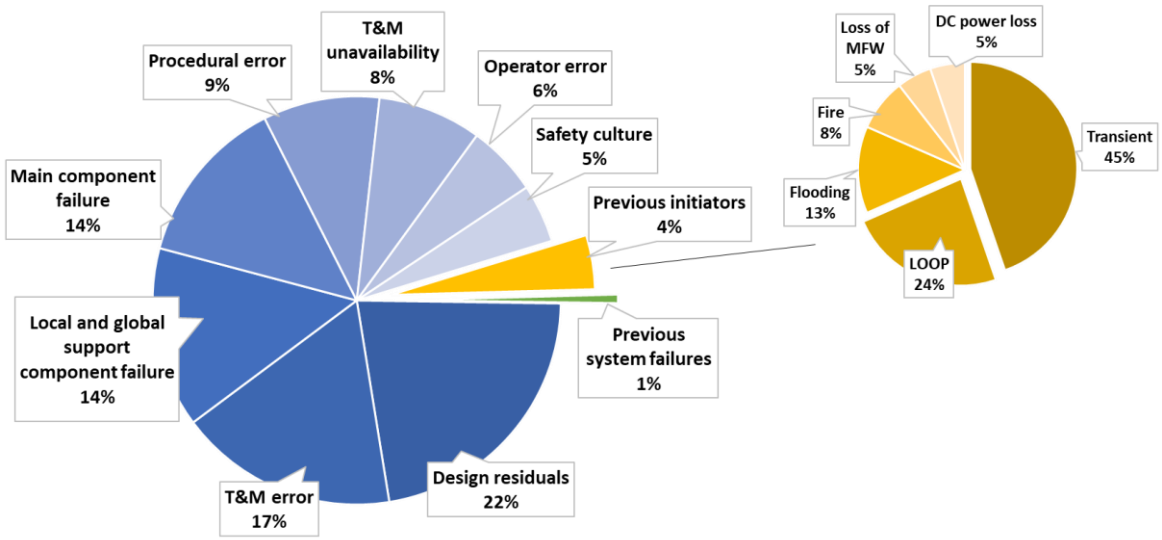


Fig. 14. Leading causes for the occurrence of safety systems failures in PWRs. Meaning behind the abbreviations: T&M – testing and maintenance; MFW – main feedwater; LOOP – loss of offsite power, DC – direct current.

4.4.2.2 Analysis of BWR safety systems failures

Boiling water reactors (BWRs) had 382 events (30% of the total events in the database) with 466 safety system failures. The leading system failures were those in the emergency power system with 77 occurrences (17%), followed by the high-pressure coolant injection system with 56 (12%) and residual heat removal system with 55 occurrences (12%) (Fig. 15).

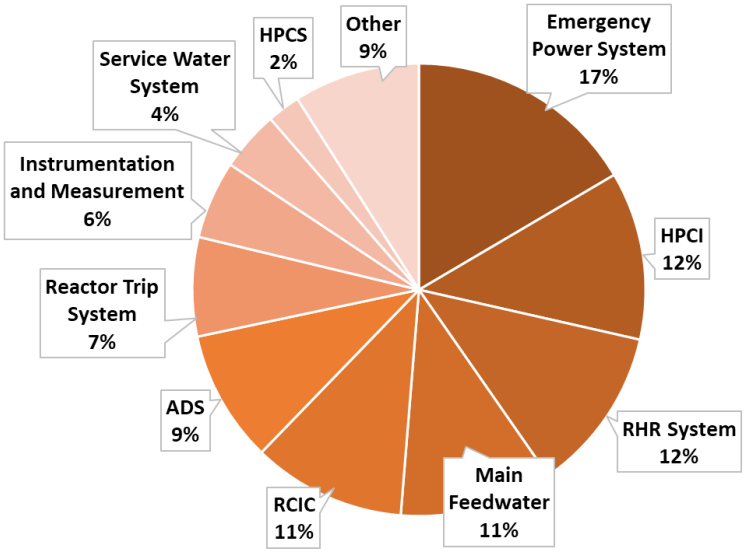


Fig. 15. Rate of occurrence of individual safety system failures out of the total number of observed safety system failures in BWRs. Meaning behind the abbreviations: RCIC – reactor core isolation cooling; HPCI – high pressure coolant injection; ADS – automatic depressurization system; HPCS – high pressure core spray; RHR – residual heat removal.

The same approach outlined in the discussion of PWR safety system failures regarding the causal factors is also used in this analysis. In this way, 462 causal factors were identified, and their relative contributions are presented in Fig. 16. The leading causes were again related to the micro-contributing factors (84%) as shown in blue, with design residuals being the most common cause having 106 occurrences (23%), followed by support component failures (16%), and main component failures (13%). The contribution of previous initiators (initiating events) to safety systems failures appears to be significantly higher compared to PWRs, with 49 occurrences (11%). In no small part, this was aggravated by the Great East Japan Earthquake in 2011, as flooding was the direct cause for 13 safety system failures, i.e. 27% of the total failures caused by initiating events. The contribution of previous system failures to failures in BWR safety systems was 1%.

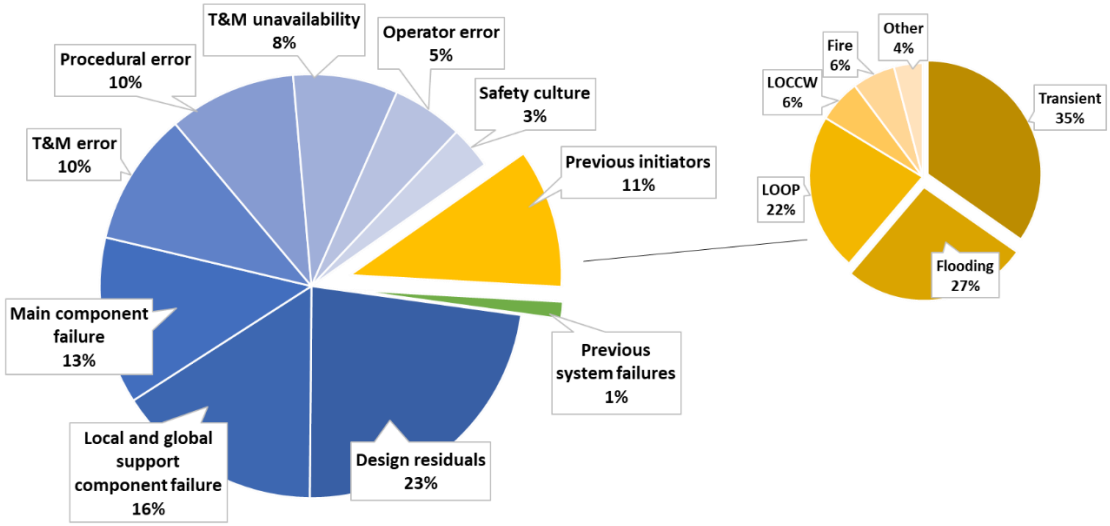


Fig. 16. Leading causes for the occurrence of safety systems failures in BWRs. Meaning behind the abbreviations: T&M – testing and maintenance; LOOP – loss of offsite power; LOCCW – loss of component cooling water.

4.4.2.3 Analysis of PHWR safety systems failures

Pressurized heavy water reactors (PHWRs) are affected by 50 events in the database, i.e.4% of the total 1256 events. The same approach outlined for the previous reactor types will be also used in this analysis. In these PHWR events, 45 safety system failures were observed, with 55 causal factors. The most commonly affected safety systems were the residual heat removal system with 10 occurrences (22%), followed by the high-pressure injection with 7 occurrences (16%) as shown in Fig. 17. The leading causes were once again the contributing factors, with main component failures (11 occurrences – 20%) being the most common, followed by the testing and maintenance errors (16%), and operator errors (15%) as shown in Fig. 18. Compared to both PWRs and BWRs, the share of failures caused by previous initiators (initiating events) were higher (16%), with the majority occurring due to internal and external flooding. In any case, let us keep in mind the relative scarcity of the data on PHWRs in the database.

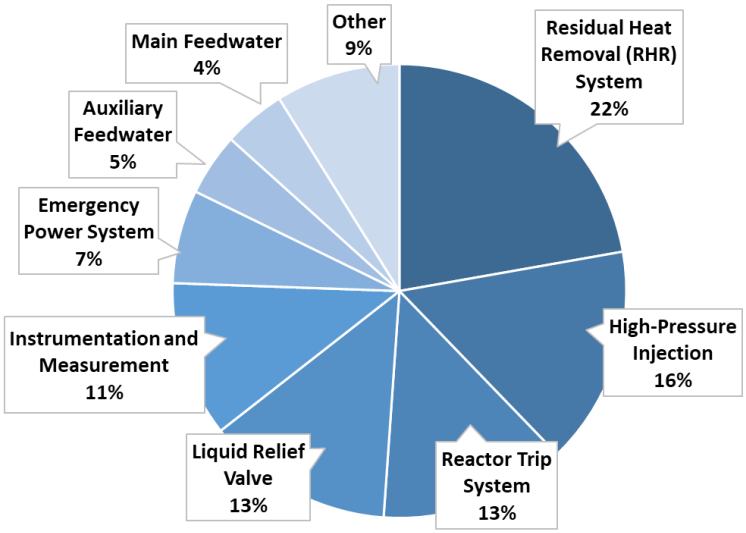


Fig. 17. Rate of occurrence of individual safety system failures out of the total number of observed safety system failures in PHWRs.

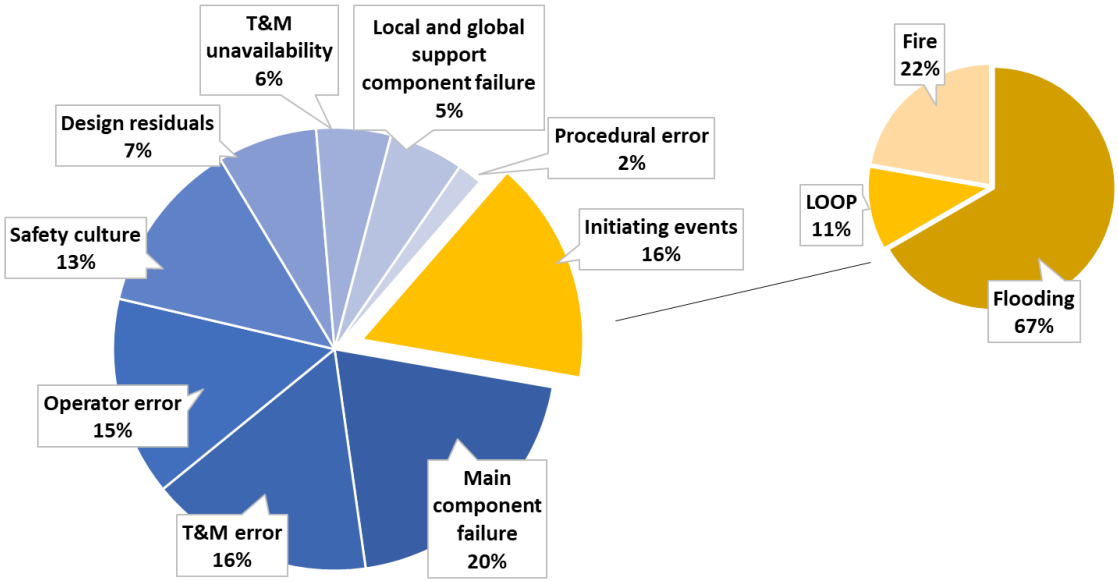


Fig. 18. Leading causes for the occurrence of safety systems failures in PHWRs. Meaning behind the abbreviations: T&M – testing and maintenance; LOOP – loss of offsite power.

5. Conclusions

In this paper, the structure, features and motivations behind the ETHZ Curated Nuclear Events database were presented. With more than 1250 events, it is the largest open databases of safety-relevant events concerning commercial nuclear power plants in the world. Our database addresses important limitations in international data collection efforts, such as openness, harmonization, navigability, and assessment consistency. This work is in line with our philosophy of fostering risk information exchange to more intensively learn from the past, and it will ultimately serve the greater purpose of the safe operation of nuclear facilities. Every event is analyzed by our technical team using well-established and consistent classification criteria, while the user access tool provides a multitude of filtering and analytical options.

The discussions presented in the previous sections highlight important and novel takeaways:

- Events having origins outside the nuclear island were as numerous as those within, stressing the importance of giving adequate attention to the secondary and external regions.
- Events have frequently occurred during transitory and cold shutdown states, therefore, plant operators should avoid "lowering the guard" even if the reactor is not at full power or in stable operation.
- The overall leading initiating events were general transients, followed by loss of offsite power events, while safety systems related to emergency power and emergency core cooling were the most common system failures. This is in agreement with their respective relative unreliability numbers based on industrial experience [30].
- The most commonly identified contributing factors were of technical nature (63%); however, human and organizational factors were very important, with their impact extending to 30% and 27% of all events, respectively. This is in line with the focus of the literature on the importance of human and organizational culture factors, and their contribution to the safety of nuclear power plants [32]. Moreover, our findings confirm those of other researchers [33] who argue that human, management, and organizational factors play a role as important as technical factors.
- The micro-analysis of contributors showed that across-the-board design residuals are dominating the unreliability of safety systems, which emphasizes the need to focus more on design verification coding and testing. Design residuals can be latent, with the potential to cause a major failure when combined with another contributor, e.g. a human error. It is interesting to compare these findings with other research results: Moura et al. [6], who have done an extensive causality analysis for major accidents in different high-technology industries, have found that design failures were the most frequent contributors to accidents in critical infrastructures. Moreover, Kinnersley and Roelen [34] found that design errors were the root cause for about 50% of accidents and incidents in the aviation and the nuclear industries. Our work has confirmed the importance of the contribution of design residuals to accidents and incidents, although using a far richer and larger dataset.

The ETHZ Curated Nuclear Events Database and the work behind it can be used as unique educational mean for practitioners, academics, regulators, and other interested audience. The approach used in collecting and classifying events can be easily adapted to other fields and for other critical infrastructures. Furthermore, due to the effort done to standardize and homogenize the events, descriptions, and input fields, machine learning techniques such as text mining can be well-suited to extract further features and hidden knowledge as done in other fields using structured reports of accidents and databases [35]. The database, along with the access tool and user manual, are publicly available on: http://er-nucleardb.ethz.ch/. Further important insights, lessons, precursory signals, and unique statistics, are presented in our follow-up paper [36].

Appendix:

The full sets of the considered initiating events and systems used for the classification in the ETHZ Curated Nuclear Events database are presented in this section.

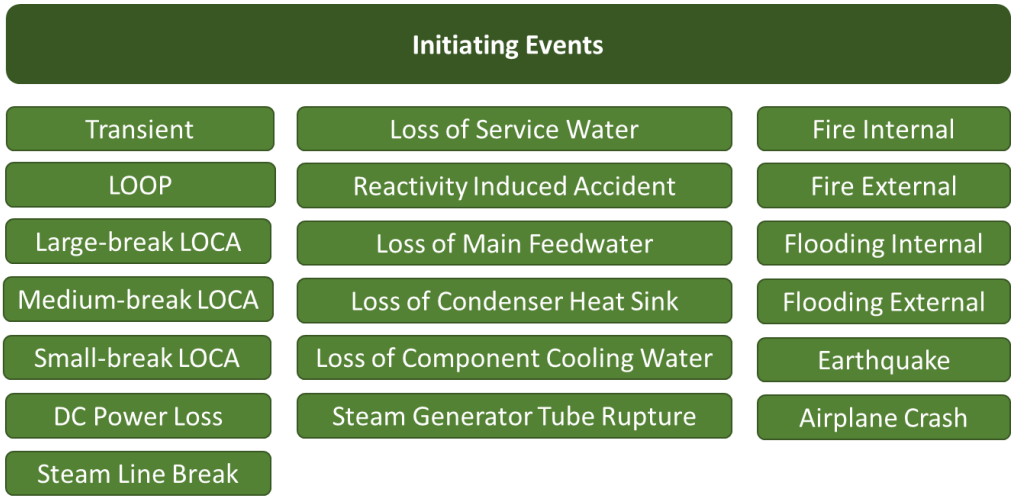


Fig. A.1. Considered initiating events in the database. Abbreviations: LOOP – loss of offsite power; LOCA – loss-of-coolant-accident.

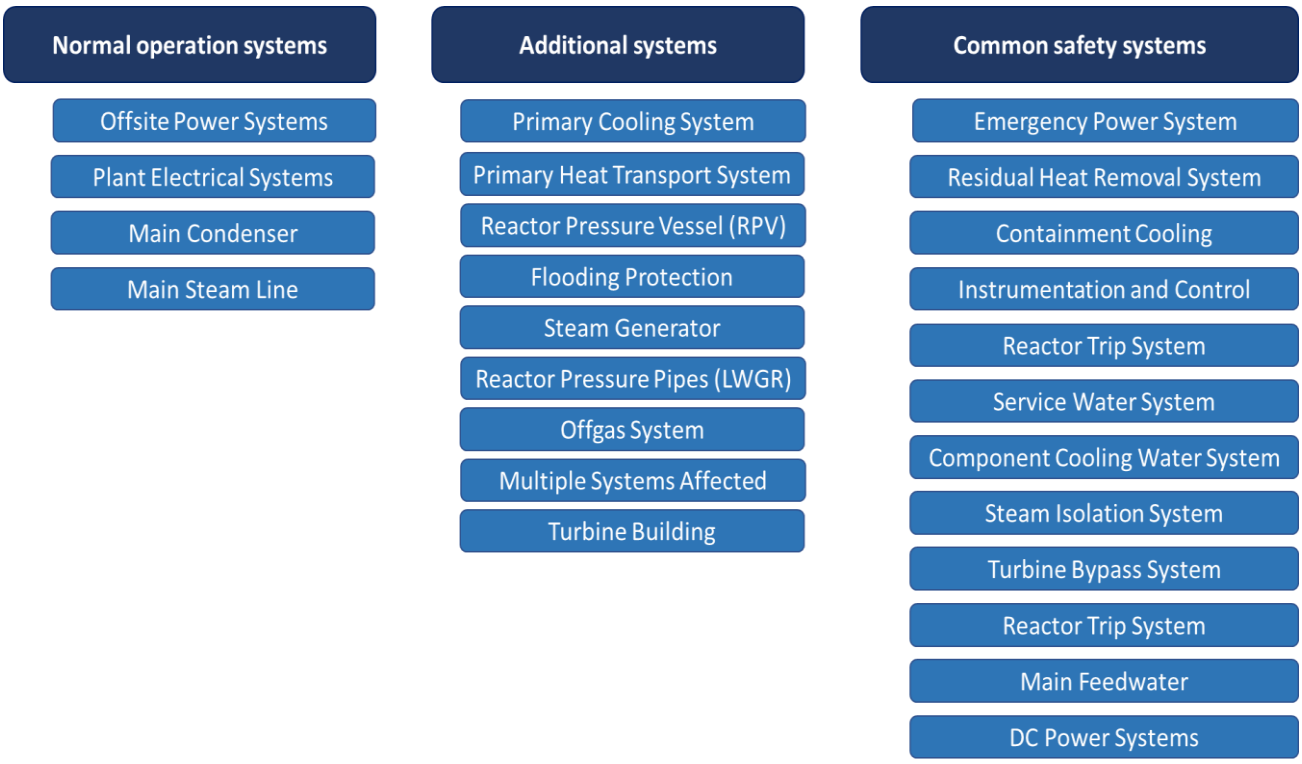


Fig. A.2. Considered common systems encompassing all reactor types in the database.

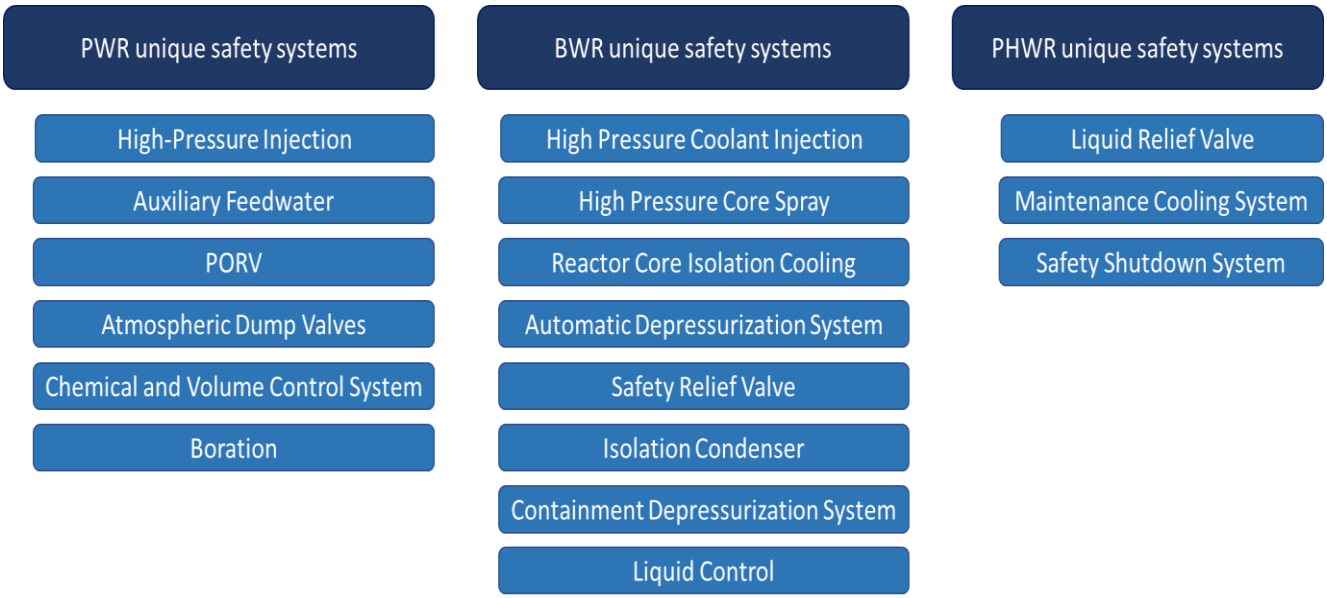


Fig. A.3. Considered systems specific for the most common reactor types in the database.

References

1. Gordon, R.P.E., *The contribution of human factors to accidents in the offshore oil industry.* Reliability Engineering & System Safety, 1998. **61**(1): p. 95-108.
2. Chernov, D. and D. Sornette, *Man-made catastrophes and risk information concealment*. 2016: Springer.
3. Chernov, D. and D. Sornette, *Critical risks of different economic sectors*. 2020: Springer.
4. Gnoni, M.G. and J.H. Saleh, *Near-miss management systems and observability-in-depth: Handling safety incidents and accident precursors in light of safety principles.* Safety science, 2017. **91**: p. 154-167.
5. Zou, Y., Wang, Wei, Zio, Enrico, Zhang, Li, Jiang, Jianjun, Xiao, Zhi, Fei, Yinliang, Čepin, Marko, *An integrated framework for analysing operational events in China nuclear power plants.* Annals of Nuclear Energy, 2019. **130**: p. 192-199.
6. Moura, R., Beer, Michael, Patelli, Edoardo, Lewis, John, Knoll, Franz, *Learning from major accidents to improve system design.* Safety science, 2016. **84**: p. 37-45.
7. Moura, R., Beer, Michael, Patelli, Edoardo, Lewis, John, *Learning from major accidents: Graphical representation and analysis of multi-attribute events to enhance risk communication.* Safety science, 2017. **99**: p. 58-70.
8. Hauge, S., Hokstad, Per, Håbrekke, Solfrid, Lundteigen, Mary Ann, *Common cause failures in safety-instrumented systems: Using field experience from the petroleum industry.* Reliability Engineering & System Safety, 2016. **151**: p. 34-45.
9. Preischl, W. and M. Hellmich, *Human error probabilities from operational experience of German nuclear power plants.* Reliability Engineering & System Safety, 2013. **109**: p. 150-159.
10. Preischl, W. and M. Hellmich, *Human error probabilities from operational experience of German nuclear power plants, Part II.* Reliability Engineering & System Safety, 2016. **148**: p. 44-56.
11. Park, J., Y. Kim, and W. Jung, *Calculating nominal human error probabilities from the operation experience of domestic nuclear power plants.* Reliability Engineering & System Safety, 2018. **170**: p. 215-225.
12. Kröger, W., *Securing the operation of socially critical systems from an engineering perspective: new challenges, enhanced tools and novel concepts.* European Journal for Security Research, 2017. **2**(1): p. 39-55.
13. IAEA, *IAEA Releases 2019 Data on Nuclear Power Plants Operating Experience*. 2020.
14. IAEA, *IRS Guidelines – Joint IAEA/NEA International Reporting System for Operating Experience*. 2010: Vienna.
15. IAEA, *Nuclear Events Web-based System (NEWS)*. 2020: retrieved from https://www-news.iaea.org/AboutNews.aspx.
16. WANO, *Performance Analysis Program*. 2020: retrieved from https://www.wano.info/services/performance-analysis.
17. JRC, E., *Clearinghouse on Operating Experience Feedback*. 2020: retrieved from https://clearinghouse-oef.jrc.ec.europa.eu/search/oef_records.
18. U.S.NRC., *Licensee Event Report Search (LERSearch)*. 2020: retrieved from https://lersearch.inl.gov/Entry.aspx.
19. U.S.NRC., *Accident Sequence Precursor (ASP) Program*. 2020: retrieved from https://www.nrc.gov/about-nrc/regulatory/research/asp.html.
20. Johnson, J.W. and D.M. Rasmuson, *The US NRC's accident sequence precursor program: an overview and development of a Bayesian approach to estimate core damage frequency using precursor information.* Reliability Engineering & System Safety, 1996. **53**(2): p. 205-216.
21. Ayoub, A., Stankovski, Andrej, Wheatley, Spencer, Kröger, Wolfgang, and Sornette, Didier, *ETHZ Curated Nuclear Events Database*. 2020: retrieved from http://er-nucleardb.ethz.ch/.
22. Ayoub, A., Stankovski, Andrej, Kröger, Wolfgang, and Sornette, Didier *Status of the ETHZ Curated Nuclear Events Database*. in *30th European Safety and Reliability Conference and 15th*

Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15). 2020. Venice, Italy.
23. Mosleh, A., *PRA: a perspective on strengths, current limitations, and possible improvements.* Nuclear Engineering and technology, 2014. **46**(1): p. 1-10.
24. Ayoub, A., Nusbaumer, Olivier, Kröger, Wolfgang, and Sornette, Didier *Simplified/Harmonized PSA: A Generic Modeling Framework*, in *International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2019)*. 2019, American Nuclear Society (ANS): Charleston, SC, USA.
25. Ayoub, A., Kröger, Wolfgang, and Sornette, Didier, *Generic Probabilistic Safety Assessment Models for International Precursor Analysis Applications*, in *International Youth Nuclear Congress (IYNC)*. 2020: Sydney, Australia.
26. IAEA, *INES The International Nuclear and Radiological Event Scale User's Manual*. 2013, Vienna.
27. Lokhov, A., *Technical and economic aspects of load following with nuclear power plants.* NEA, OECD, Paris, France, 2011. **2**.
28. U.S.NRC, *Accident Sequence Precursor (ASP) Program - Summary Description*. 2008: Washington, DC.
29. Sornette, D., W. Kröger, and S. Wheatley, *New Ways and Needs for Exploiting Nuclear Energy*. 2018: Springer.
30. Eide, S., Wierman, TE, Gentillon, CD, Rasmuson, DM, Atwood, CL, *Industry-average performance for components and initiating events at US commercial nuclear power plants*. 2007, Nuclear Regulatory Commission, NUREG/CR-6928.
31. Poloski, J., D. Marksberry, and U. Atwood, *Rates of initiating events at us nuclear power plants*. 1999, NUREG/CR-5750, US Nuclear Regulatory Commission, Washington (DC).
32. Morrow, S.L., G.K. Koves, and V.E. Barnes, *Exploring the relationship between safety culture and safety performance in US nuclear power operations.* Safety Science, 2014. **69**: p. 37-47.
33. García-Herrero, S., Mariscal, MA, Gutiérrez, José M, Toca-Otero, Antonio, *Bayesian network analysis of safety culture and organizational culture in a nuclear power plant.* Safety science, 2013. **53**: p. 82-95.
34. Kinnersley, S. and A. Roelen, *The contribution of design to accidents.* Safety Science, 2007. **45**(1-2): p. 31-60.
35. Hughes, P., Robinson, Ryan, Figueres-Esteban, Miguel, Van Gulijk, Coen, *Extracting safety information from multi-lingual accident reports using an ontology-based approach.* Safety science, 2019. **118**: p. 288-297.
36. Ayoub, A., Stankovski, Andrej, Kröger, Wolfgang, and Sornette, Didier, *Precursors and Startling Lessons: Statistical analysis of 1250 events with safety significance from the civil nuclear sector* Reliability Engineering & System Safety, 2021. Under Review.

Chapter 3

Precursors and startling lessons: Statistical analysis of 1250 events with safety significance from the civil nuclear sector

We analyze the ETH Zurich open curated database of 1250 worldwide nuclear events focused on safety significance with potentials for precursors, presented in the companion paper. We find that major accidents always trigger a wave of "reactive" reporting as well as changes in regulatory or corporate management that last 5 to 6 years, mostly due to increased alertness, improved transparency, uncovering latent design errors, and heightened public pressure. The leading causes for multi-unit events are found to be external triggers and design issues, confirming the need to adapt PSAs to cover multi-unit events accordingly. Common-cause failures (CCF) are found to occur fairly frequently, at different levels, and can significantly erode the safety of the plant. From the lessons learned from this analysis, we suggest that frequent review of components design and operating procedures, employing different teams for testing and maintenance activities on redundant trains, and sharing operational experience between plants of similar designs, are some of the steps that should be taken in order to limit future occurrences of CCFs and beyond that further improve plant safety. We identify some quantitative signs of aging for plants after the age of 25. Our findings stress the need for larger recording, reliance, and sharing of operational data to support learning from experience and avoid reoccurrence of accidents and events.

Based on **Ayoub, A.,** Stankovski, A., Kröger, W., & Sornette, D. (2021). Precursors and startling lessons: Statistical analysis of 1250 events with safety significance from the civil nuclear sector. *Reliability Engineering & System Safety*, 107820.

1. Introduction

Evolving large-scale engineered systems that our societies depend on, and which are inherently hazardous, call for predictive analysis of potential risks. As statistical information of direct use is limited by nature, analytical methods incorporating data and "lessons learned from the past" are needed to model the behavior of systems. The latter is based on compiling and evaluating data of experienced failures and events at different levels of abstraction. When dealing with interdependent critical infrastructure systems and their involved complexity, traditional risk modeling usually turns out to be insufficient to cover all their aspects and mechanisms [1]. A vivid example of less complex, but complicated, systems are nuclear power plants, made of thousands of components, systems, and structures, connected through diligent mechanisms. The corresponding high levels of redundancy and diversification, as well as separation, ensure utmost safety for their operation. Despite their high level of sophistication, nuclear power plants are not autonomous, as they require uninterrupted human surveillance, operation, and maintenance. Additionally, a nuclear power plant is not an independent entity that can be modeled in isolation from its site and operational environment. On the one hand, a nuclear plant heavily relies on its external environment during its normal operation (offsite power grid,

water intake). On the other hand, the external environment can be an extremely perturbing factor for the safe operation of a plant (earthquakes, floods, grid disturbances, power losses, water conditions). All these inherent complications, dependencies, man-machine interactions, external factors, and above all, the cultural and organizational aspects that shape many actions and consequences, make it extremely hard for mathematical models -- especially ones aiming at assessing risks -- to capture adequately the behavior of the plant. Nevertheless, traditional methods based on decomposition and causality, as well as human reliability analysis, appear to remain very useful and well suited.

As an illustrative example, probabilistic safety assessment (PSA) is a prominent risk framework that is extensively used in the nuclear power industry to identify design weaknesses and check whether the safety concept is balanced [2]. In particular, PSA models aim at quantifying nuclear power plants risks by:

1- postulating and analyzing what could go wrong from within the plant and from the outside;
2- how likely is it to happen, and if it happens;
3- what are the consequences.

With more than 40 years of utilization, PSAs have reached high levels of advancement that make them very robust and reliable in assessing risk. PSAs have even become part of the licensing process. However, due to the aforementioned complexities in nuclear power plants, PSAs still suffer major limitations, with completeness being a very prominent one [3, 4], i.e. it is mathematically impossible to prove that PSA models can cover all conceivable accident scenarios and scopes.

Operational experience appears to be very useful in these situations, as it can provide a rich information source supporting risk models [5]. In addition to helping in the initial development of the models, lessons learned from operational experience often trigger amendments and improvements to the models. Besides, operational experience provides an empirical basis for the estimation of components reliability parameters and initiating events frequencies [6]. Furthermore, as many intrinsic features and system characteristics manifest themselves in empirical events, operational experience can be very useful to assess and validate mathematical models. Apart from modeling support, operational experience has been used to aid improvements and post-design modifications. For example, major accidents in the nuclear power industry have triggered industry-wide retrofits and stress tests [7], with the most prominent being the post TMI control room changes, post Chernobyl RBMK design changes, and the post Fukushima “Diverse and Flexible Coping Strategies FLEX” backfits [8].

Realizing the potential stemming from operational data, industries and researchers started paying increased attention to observe, record, and utilize real incidents and inadequacies to learn from mistakes and prevent their reoccurrence [9-12]. In this regards, Moura et al. [13] have compiled a dataset of 238 major accidents from different heavy industries, and developed a new approach to test and validate risk models, study causal interactions, and improve systems designs and robustness. Zhang and Mahadevan [5] utilized a database of historical aviation accidents and developed a Bayesian network to model causal relationships and facilitate probabilistic inference to support accidents investigation and risk analysis. Wheatley et al. [14] utilized a dataset of about 200 nuclear accidents and incidents, with several severity annotations, to empirically study the safety performance of nuclear power plants, and estimate the financial risks and likelihoods of major accidents.

Worldwide civil nuclear operations have accumulated more than 18’000 reactor-years [15] of experience, providing substantial amounts of data, a subset of which we try to utilize in this paper. Specifically, we are using the ETHZ Curated Nuclear Events Database [16], to extract important lessons

and identify potential precursory signals. The database currently contains more than 1250 safety important events from around the world, making it by far the largest open-source, comprehensive, and academically driven initiative in the world. It serves all communities, from nuclear operators, regulatory agencies, scientists, and the public. It is used to provide various input for precursor analysis and other statistical analyses [17, 18], with the aim to properly assess the safety of modern nuclear power plants, and identify trends and patterns of associated risks. With this amount of such high quality data, supported by its detailed and rich analyses and features, we aim at extracting reliable statistics leading to insights that can help averting future disasters or costly precursors.

2. Data structure and description

Operational data in the civil nuclear industry is well recorded at national levels, mandated by regulatory requirements (a vivid example are the USNRC licensee event reports [19] and Accident Sequence Precursor program (ASP) [20, 21]. At the international level, different efforts exist -- with different scopes and aims -- to collect operational experience; major examples include: World Association of Nuclear Operators [22], International Atomic Energy Agency Reporting System [23], European Clearinghouse on Operating Experience Feedback for Nuclear Power Plants [24]. However, these efforts in general are either not publicly available, actor-oriented, lack homogeneity (different reporting styles), and lack practical annotations and searchability (usually in the form of static reports).

Realizing these limitations, we have compiled a unique database, namely, the ETHZ Curated Nuclear Events Database [16], with more than 1250 safety significant events around the world, covering the whole time-period of civil nuclear power operation. The events in the database have been systematically analyzed by multiple nuclear-safety experts, providing a curated intermediate-level description, and coherent breakdown of features such as origin of the event, causes and contributors, type of failure, operating mode, failure sequence, significance, and many others. A detailed explanation of the database features, classification criteria, and definitions, can be found in the companion paper [25]. The database along with its custom-made graphical user-interface, provide an open access, user-friendly, and information-rich asset for the scientific community, industrial analysts, as well as the public.

3. Statistical analyses

The analyses, statistics, and interpretations presented in this paper are based on the data contained in our database. They are related to several different topics that we believe might give significant and novel insights for researchers and the industry, including the occurrence rate of events, the analysis of single and multi-unit sites, common cause failures (CCFs), quantitative aging signs, and the reliability of safety functions and systems.

3.1. Occurrence rate of events over time

In order to study the likelihood of occurrence of accidents and precursors, we examine the evolution of their rate over time. We define λ_t, the rate of occurrence of events per reactor in year t. Given that events are rare and are sparsely spread in time, we take the simplest assumption that their temporal distribution is Poissonian, in other words there is no correlation between successive events, and the distribution of waiting times between one event and the next one is exponential with rate λ_t. Then, the statistical estimate of λ_t is simply $\hat{\lambda}_t = \frac{N_t}{r_t}$, where N_t is the number of observed events in year t,

and r_t is the number of operating nuclear reactors in year t. Under this assumption, the variance of λ_t is $Var(\lambda_t) = \frac{\lambda_t}{r_t}$, which can be calculated using the estimate $\hat{\lambda}_t$ to evaluate confidence intervals in a standard way. Fig. 1 shows the calculated rates, $\hat{\lambda}_t$ (solid dots), along with their Poisson standard errors (represented by the error bars) defined as the square-root of $Var(\lambda_t)$. Furthermore, the number of operating reactors over time, r_t, is also shown in Fig. 1 (continuous solid line).
It should be noted that only reactors which have event entries in the database are taken into account in this analysis in order to maintain consistency.

Four distinctive periods can be observed based on the occurrence rate of events:

- Early period (1965-1985) – early days of nuclear power defined by limited knowledge, insignificant operating experience, and lack of transparency. This period has a pronounced volatile nature with large variances in the rates of events, mainly due to the low reporting and low number of operating reactors. The average rate of events per reactor year, λ, of that period is quite high with $\lambda = 0.16$. During this period, the Three Mile Island accident occurred (March, 1979), which triggered a swarm of events afterwards, most probably due to increased safety awareness and design changes.
- Chernobyl cluster (1986-1992) – sudden increase in reported events triggered by the Chernobyl accident, with $\lambda = 0.13$ events per reactor year. This period is characterized by reactive reporting, increase of transparency, safety reviews and major changes, general negative public perception of nuclear power, as well as related public pressure on policy makers.
- Calm periods (1993 – 2010; 2017 – 2020) – largely "uneventful" periods where the implementation of lessons learned from the previous accidents, frequent inspections and the slightly diminishing public pressure might have led to a decrease in witnessed and reported events. A decline of attentiveness by plant operators and regulatory bodies might also contribute to this trend. The average rate of events per reactor year for these two periods is $\lambda = 0.07$ and $\lambda = 0.06$, respectively.
- Fukushima cluster (2011-2016) – in the wake of the Fukushima Dai-ichi nuclear accident, new waves of reactive reporting, uncovering of latent design deficits and vulnerabilities (e.g. by stress-tests), and regulatory changes were triggered, leading to a new spike in events with a $\lambda = 0.14$ events per reactor-year.

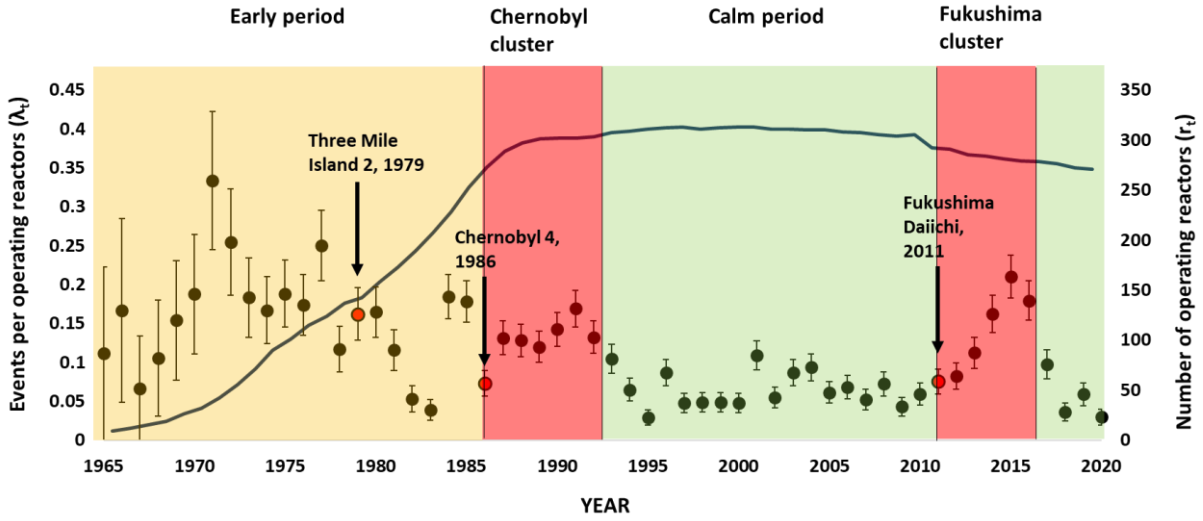


Fig. 1. Occurrence rate of events per reactor-year (solid dots with error bars, left axis) and the number of operating reactors appearing in our database (continuous solid line, right axis).

The effects of the Chernobyl and Fukushima accidents are evident, with pronounced periods of heightened awareness (characterized by an increase of events rates) lasting for 5 to 6 years. As

discussed, a possible explanation for this trend appears to be the increase in transparency, public pressure and sudden uncovering of latent errors. A contributing factor could also be the typical duration of executives' terms and mandates in office of 5-6 years, who tend to enforce a strict safety culture following major accidents, which in turn trickles down to employees and subordinates and allow for increased – intra and inter – reporting habits and transparency [26, 27]. Following this 5–6-year period of alertness, we observe a calm period of low event rates, likely due to the effects of implemented safety and regulatory improvements. A concerning factor possibly contributing to this trend can be "lowering of the guard" of operators and regulators, on account of the diminishing public pressure over time. Therefore, in order to avoid another major accident after a calm period, licensees must retain good communication and transparency habits both internally and with the regulators. Similar to war drills performed by militaries to maintain combat readiness in times of peace, top management and regulators must demand a high level of attentiveness during "calm periods". Furthermore, the plant and operators' response should constantly be challenged with postulated accident scenarios and simulations, in analogy to war drills. The regulators must also have an overview of whether all changes stemming from lessons learned are properly and efficiently implemented by the licensees.

3.2. Analysis of events at single- and multi-unit sites

Historically, PSAs and risk models have principally been single-unit oriented, where the focus was the specific reactor under analysis, independent from other reactors on site. In recent years, advancements have been made to adapt the classical PSA models to cover multi-units at the same site [28, 29]. Studying the nature of events in the database, we observed several instances of multi-unit occurrence, which can be attributed to one or more of the following reasons:

1. External events originating outside of the plant boundary that can indiscriminately target one or multiple units on the site.
2. Shared components between units of the same site. The components can be part of safety-related systems (emergency power, essential service water), or belong to systems necessary for normal operation of the plant (offsite power, normal service water, condenser water intake, etc.). Failure of these shared components would trigger a simultaneous response from all affected units (e.g. failure of a cross-tied emergency diesel generator).
3. Acute or potential failures of non-shared components that, nevertheless, share the same design flaws, inadequate operating procedures, or safety culture deficiencies (e.g. identifying a design problem in the high-pressure injection pump of one unit that is inherent to other pumps of other units on the site).

The database contains events which have occurred in 352 reactors across 143 nuclear sites. Of these sites, 97 (68%) are multi-unit sites that contain 306 reactors. Moreover, around 71% of the 1256 events occurred at multi-unit sites (897 events), with 84% out of these events affecting only one unit on the site, and 14% impacting multiple units simultaneously (Fig. 2). The figure also shows a breakdown of the type of trigger which led to the event, i.e. whether it was an initiating event or a pure system failure; the latter refers to events where no initiating event was observed. The share of the individual initiating events is also displayed. The most common type of trigger affecting multi-units is pure system failures (68%), with the remaining being initiating events (32%). On the other hand, initiating events and pure system failures have equal shares when one unit is affected on the site. What can be immediately observed is that loss of offsite power (LOOP) events dominate the initiating events affecting multiple units, while on the other hand, transients and small break loss-of-coolant accidents (SBLOCA) are more tied to a single unit at the site.

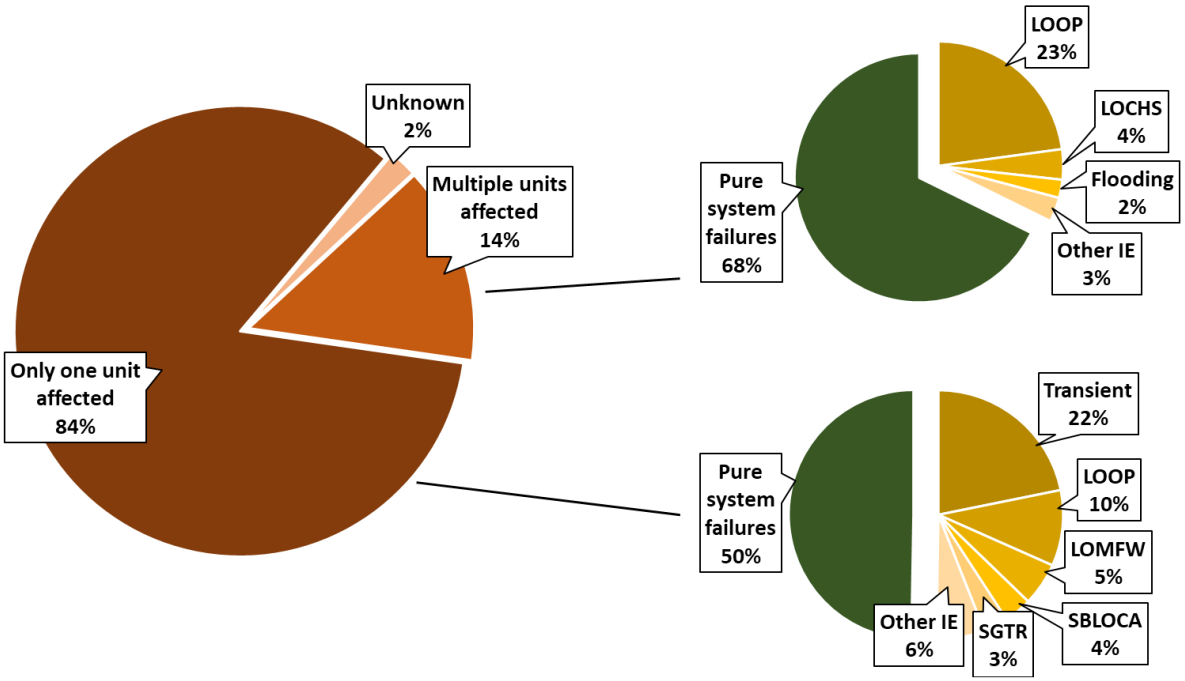


Fig. 2. Fraction of affected units at multi-unit sites (left), and analysis of the type of trigger (right): pure system failures (green) and initiating events (yellow). Used abbreviations: LOOP – loss of offsite power; LOCHS – loss of condenser heat sink; IE – initiating event; LOMFW – loss of main feedwater; SBLOCA – small break loss-of-coolant accident; SGTR – steam generator tube rupture.

When analyzing the origins of the events (Fig. 3), the majority of initiating events affecting multiple units had external origins (66%), while external events affecting only one unit are at 9%. The share of initiating events originating in the secondary part is also fairly high (27%), which is expected as these include systems shared between multi-units. Finally, we can infer that initiating events originating in the nuclear island are less likely to affect more than one unit (44% for single affected units compared to 7% for multi-units). This breakdown is in line with the aforementioned reasons 1 and 2 (external origins, and shared components respectively).

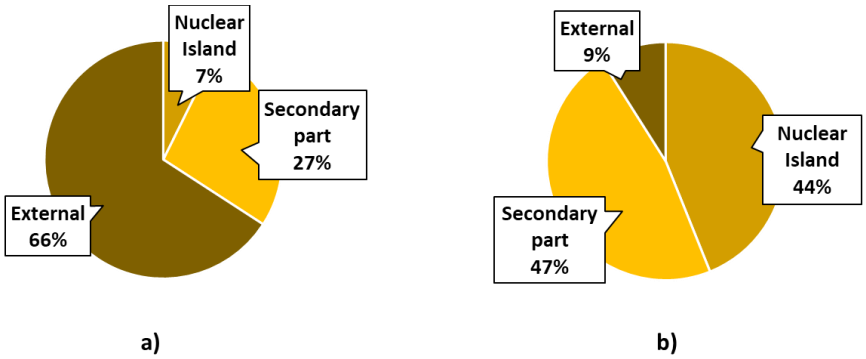


Fig. 3. Origin of the initiating event affecting: a) multiple units; b) one unit.

Shifting our focus to events containing pure system failures on multi-unit sites, only 86 events affected multiple units. Up to 41% of these failures were related to the emergency power and service water systems, which commonly have shared components between units, while the remaining 59% were related to systems usually contained in a single unit. Identifying the contributing factors for failures affecting one or multiple units (Fig 4.), we can infer that the vast majority of system failures affecting

multiple units had causes rooted in design flaws (62%), followed by procedural deficiencies (10.5%). These results confirm our previously identified reasons 2 and 3 for multi-unit occurrences, namely having shared components between the units, or having identical design issues in similar components at multiple units. Regarding single affected units at multi-unit sites, design problems and testing and maintenance (T&M) related errors were the most prominent with 24% each.

The outlined observations can help in the development process of multi-unit PSAs:

1. knowing their minor share, this questions the "substantial" need for multi-unit considerations and the assumed interdependencies, and
2. the results can orient the focus of multi-unit PSAs towards important initiating events, triggers, origins, systems, and contributors.

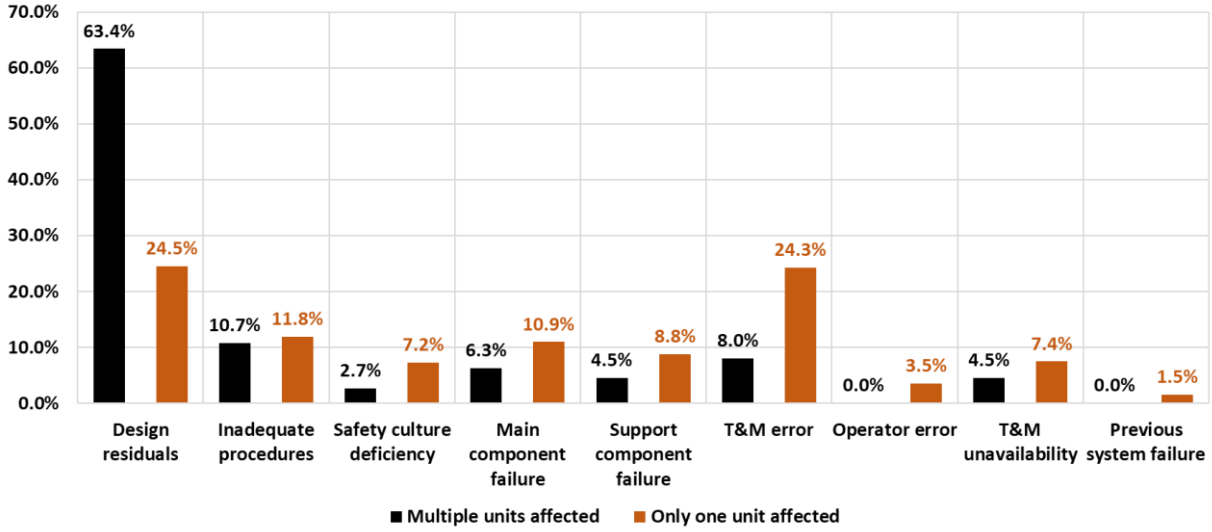


Fig. 4. Factors contributing to system failures which have affected multiple units (black), and only one unit (orange), at multi-unit sites.

3.3. Analysis of common cause failures (CCFs)

Common cause failures (CCFs) are a subset of dependent failures that concurrently result in the unavailability of two or more redundant components/trains of a safety system or function due to the same reason. They can be acute, prompting immediate response from the plant, or potential (latent)[2]. CCFs usually dominate the unreliability/unavailability of safety systems and challenge the effective redundancy. They can be due to one or more of the following reasons:

- Technical factor – redundant trains very often have the same design and operating conditions. This means that, if there is a design problem in one, or some harsh operating conditions, the other trains will have the same problem.
- Human factor – the same maintenance teams in some plants perform their activities on multiple redundant trains, implying that the team is very likely to commit identical errors that threaten the system and lead to a CCF. Additionally, some operator errors have the potential to affect multiple trains.

[2] Potential CCF: conditional on the occurrence of an event, all redundant trains of a system would have failed, e.g. non-conforming seismic dampers would cause all emergency diesel generators to fail in case of a seismic event.

- Organizational factor – inadequate maintenance and operating procedures usually affect multiple trains. Moreover safety culture deficiencies can affect redundant trains, but even more, a bad safety culture have the potential to affect the whole plant.

In the database, 218 common cause failure occurrences were observed, of which 126 (58%) were acute and 92 (42%) were potential. It should be noted that only failures that were explicitly specified in the events reports to affect multiple redundant trains were counted in this analysis. A breakdown of the detailed contributing factors for these CCF events are presented in Fig. 5. Multiple factors can simultaneously contribute to the occurrence of a failure, therefore, in this regard, the factors are not mutually exclusive. Design residuals[3] contributed to the majority of CCF events, both acute and potential. Their presence is especially pronounced in potential CCFs with a staggering 70% share of all latent failures. Inadequate procedures were also a very frequent contributor and equally impacting both types of CCFs, while testing and maintenance (T&M) errors[4] were surprisingly quite common in acute CCFs.

This analysis reaffirms the importance of verification and scrutiny of the design of components, as well as operating procedures. Frequent reviews, inspections, and sharing of operational experience between plants of similar designs – and plants having similar suppliers and manufactures – is necessary in order to limit the future occurrence of CCFs. Additionally, if possible, different teams should be deployed for performing T&M activities on components in redundant trains, to insure some diversification and avoid the occurrence of identical errors due to inadequate knowledge, or failure to follow instructions.

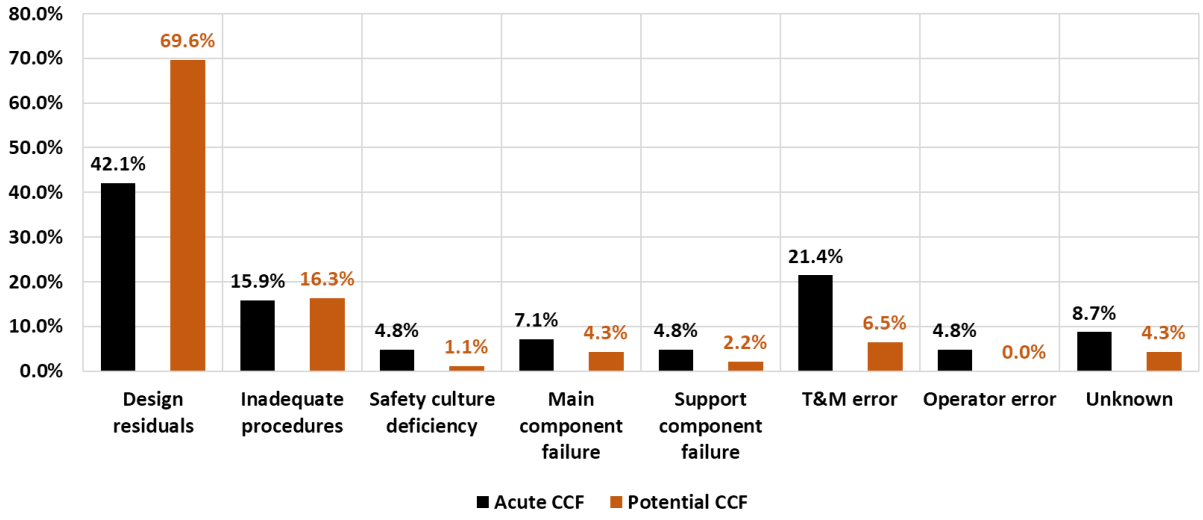


Fig. 5. Contributing factors to common cause failures (CCF).

3.4. Quantitative aging signs

Component aging implications have been a growing concern for regulators, plant operators and component manufacturers. Quantitatively, in reliability analysis, one of the most common aging demonstrations is depicted by the bathtub curve of the failure rate of a component [30], which shows high component failure rates during the early periods (infant mortality), a constant rate during the majority of the lifespan, and finally, increased rates at the end of its lifetime (wear-out/aging phase). We anticipate that the cumulative aging of components and their interactions should reveal

[3] Design residual CCF example: components (e.g. pumps, valves, etc.) from redundant trains having the same design or manufacturing flaw.

[4] Testing and maintenance team CCF example: wrong servicing of pumps in redundant trains of a system due to failure in following maintenance instructions.

themselves at a plant level by resulting in signs and more frequent occurrences of events. For this analysis, the following adaptations were performed on the dataset:

- Only events exhibiting contributing factors of technical nature that are likely to be related to aging were taken into account. These include events that contain design-related issues and failures of main and support components. Events that exclusively had failures of human and organizational nature were discarded.
- Events that have simultaneously affected multiple reactors were split into separate events if the reactors were at a different age. The age of the reactor was calculated based on the time of occurrence of the event.

Additionally, a postulated reactor survival rate was calculated based on the experience of 80 permanently shut down reactors that have event entries in the database. Although reactors can be shut down due to multiple reasons (aging, reduced safety, political pressure, financial viability, etc.), this rate calculates the fraction of remaining operating reactors beyond a certain age. Our data shows that around 50% of all reactors are expected to shut down after the age of 30, while less than 10% of reactor are expected to remain operational after the age of 45 (orange curve in Fig. 6).

After calculating the age of a reactor at which an event occurred, the events count per reactor age are plotted in Fig. 6, normalized by the reactor survival rate values. This normalization is necessary in order to get a correct estimate of events counts for every age, by correcting for shut down reactors, and taking into account the survival of reactors beyond a certain age. In other words, the normalization corrects for the fact that a reduced number of operating reactors after a certain age is expected to also yield a reduced number of events. The distribution of events count vs reactor age exhibits a very interesting behavior (solid dots in Fig. 6). Although not like the classic bathtub curve due to the rather "shy" infant mortality period, the results show an increase in observed events as the reactors age, especially pronounced after the age of 25 years. Reactors past this age appear to be more likely to suffer component failures, or have latent design problems due to technological limits, which also coincides with the usual lifespan of some major components in a nuclear power plant, such as emergency diesel generators, motor-driven pumps, transformers, etc. In conclusion, this analysis shows some traces of aging signs in nuclear power plants after 25 years of operation. Therefore, frequent testing, inspections, and preventive maintenance of components, as well as design reviews and updates must be performed to maintain safe and sustainable operations.

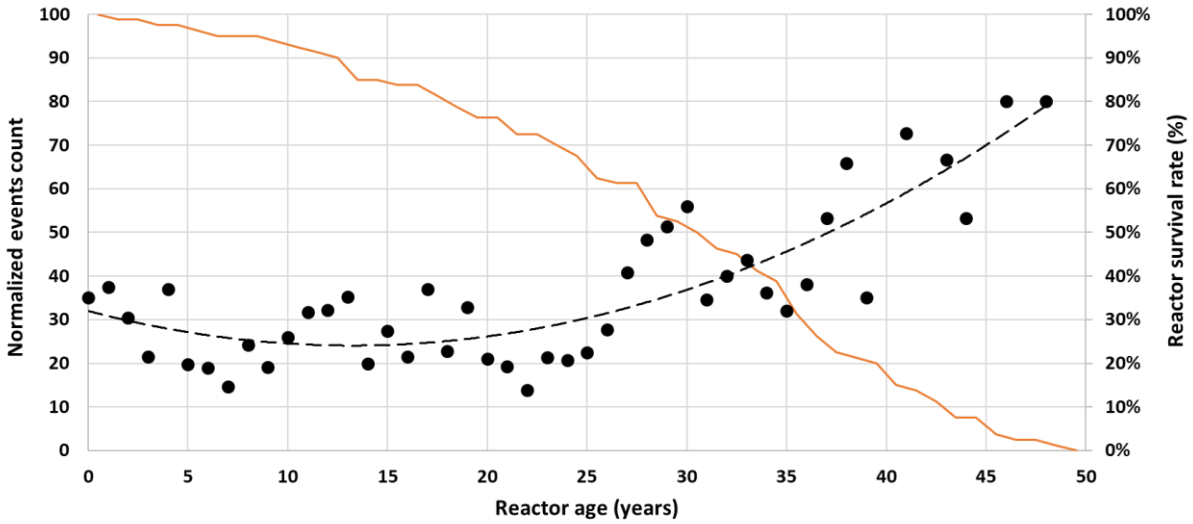


Fig. 6. Effects of aging in nuclear power plants. Number of events (solid dots) normalized by the postulated reactor survival rate (orange curve).

4. Insights and lessons learned from operating experience

Learning from operating experience, efficiently implementing changes, and objectively identifying problems in operating reactors, are very effective when it comes to preventing accidents. After the Chernobyl-4 and the Fukushima Dai-ichi accidents, substantial efforts have been made to increase communication, transparency, and information sharing between countries and regulators in order to continuously increase the level of safety of nuclear power plants. Different countries have different strategies when it comes to identifying problems and implementing changes. An illustrious example is France, where nearly all reactor lines have a similar design and are managed by one operator - Électricité de France (EDF). This is a double-edged sword, as uncovered design issues can plague multiple reactors by default, but on the other hand, addressing them inherently increases the safety of the whole fleet. In the database, at least 15 events can be identified where a problem occurred at one reactor, only for EDF to realize that many reactors in the fleet were affected by the same problem. The majority of these events were related to post-Fukushima safety measures, such as resilience of important safety systems and components to flooding and earthquakes.

Addressing known problems in a timely manner can be invaluable in preventing serious accidents. One shining example from the database is the Fort Calhoun event of January 2010, when external flooding barriers were upgraded after being deemed insufficient. The following year, waves exceeding the height of the initial barriers struck the plant and would have probably caused serious flooding damage if the new barriers had not been installed the previous year. Unfortunately, such nice outcome is not always the rule, as often plants are slow to implement needed changes due to economic considerations, or if the threatening events are deemed unlikely (Fukushima and the TEPCO story serve as an infamous example).

In the following sections 4.1 to 4.3, we will discuss multiple topics with one common goal – to put emphasis on the importance of learning from operating experience to predict and avoid accidents by implementing changes and exchanging insights with operating peers.

4.1. Precursors to major accidents

In this section, we try to highlight some of the forerunners of the three major nuclear accidents and we discuss how they could have been utilized to foresee and prevent the accidents. We confirm the fact that failing to learn from previous accidents and precursors, and failing to implement respective changes, are the main reasons behind the occurrence of the major accidents [31].

4.1.1. Forerunners and lessons learned from the Three Mile Island 2 accident

One of the most defining moments in nuclear power history is the Three Mile Island (TMI) 2 accident. The accident started at 4 a.m. on March 28, 1979 when loss of main feedwater occurred due to a technical failure. The auxiliary feedwater system was inoperable due to a maintenance error, when all valves were inadvertently left in a closed position. The pilot-operated relief valve (PORV) opened to relieve reactor pressure, but failed to reclose, effectively causing a small break loss-of-coolant accident (SBLOCA). Due to poorly designed instrumentation, the PORV position indicators were ambiguous, causing the operators to believe that there was no leak, and hence, to trip the automatically activated high-pressure injection (HPI) system that provided water makeup to the core, effectively leading to a core dry out and a subsequent meltdown. Fortunately, the next operator shift identified the problem and reactivated the HPI, preventing further core melting. The release of radioactive isotopes was contained within the building. This event had a widespread impact on the industry as a whole, triggering massive design revisions of the plants (primarily control room designs), and discussions about the importance of safety culture, proper training of operating and maintenance personnel, as well as communication between different teams.

In hindsight, there were many instances of similar occurrences (forerunners) around the world which led to less severe outcomes, and lessons stemming from these events were, unfortunately, not well learned and implemented, until the aftermath of the TMI-2 accident. At least three clear forerunners to TMI-2 have been identified, with two of them following a completely identical failure sequence: both Beznau-1, 1974 and Davis Besse, 1977 incidents occurred due to a stuck-open PORV, and the ambiguous PORV position indicators prevented the operators from correctly identifying the condition. In both of these incidents, the vigilance of the operators prevented further escalation, as they noticed signs of a SBLOCA and acted on their intuition. It is also jarring to see that, one year before the TMI-2 accident, another event occurred at TMI-2, which involved a stuck open PORV and accordingly, a SBLOCA. This event occurred 1 month before the plant was commissioned, presumably during hot functional testing of the reactor. Both Beznau-1 and Davis Besse were designed by American companies, Westinghouse Electric and Babcock & Wilcox (B&W), respectively. The US Nuclear Regulatory Commission (NRC) failed to identify that the ambiguous PORV position indicator is a serious problem that can plague many plants of similar design. More specifically, B&W failed to learn from the Davis Besse incident and failed to implement changes or provide appropriate operator training to other plants sharing their design, including TMI-2.

In addition to the above qualitative discussion, a quantitative analysis have been performed in Fig. 7, showing the cumulative number of events when a SBLOCA was caused by a stuck-open PORV over time in our database. The clear sharp increase in the cumulative number of forerunners before the 1979 TMI-2 accident could be seen as a very good sign of the predictability of the TMI-2 accident (resembling a bubble with an accelerating price in financial markets [32].

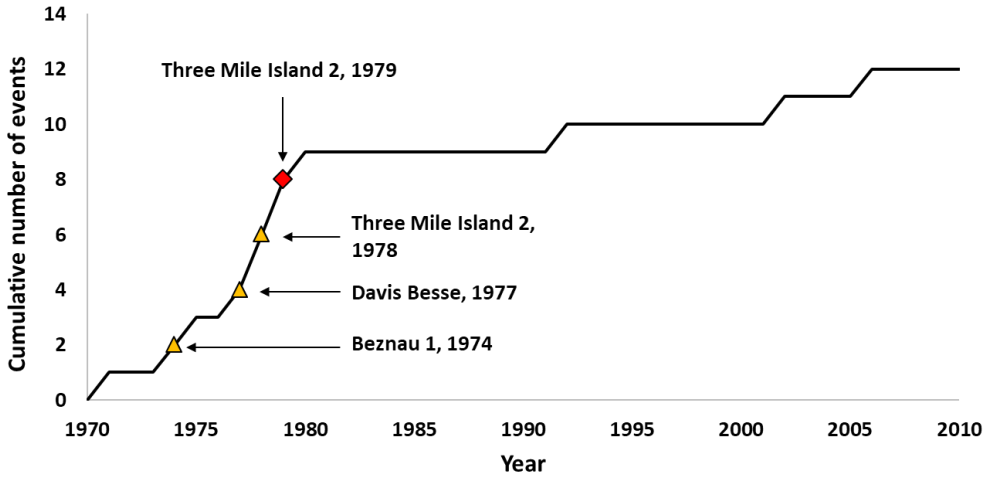


Fig. 7. Cumulative number of events where failed (stuck-open) pilot-operated relief valves (PORVs) resulted in a small break loss-of-coolant accident. Highlighted are the Three Mile Island 2 accident of 1979 (red) and its major forerunners (orange).

Following the TMI-2 accident, we can observe a change of regime, demonstrated with the reduced number of events (plateauing) related to stuck-open PORVs SBLOCA incidents; only 4 events have occurred in the 40 years following the accident (0.1 events/year). This is a decrease by a factor of 10 when compared with the pre TMI-2 period, where 8 events occurred in only 9 years (~1 event/year). This encouraging quantitative finding can be attributed to the post TMI corrective design changes, frequent inspections, increased communication levels (with regulators and between countries), and improved training.

4.1.2. Forerunners and lessons learned from the Chernobyl 4 accident

The Chernobyl-4 accident of 1986 was the most severe nuclear accident in the history of civil nuclear power. The RBMK light water graphite reactor (LWGR) design was inherently flawed in multiple aspects: a positive void coefficient; a positive scram effect where control rods had a graphite tip, which, although useful for normal operation for smoothing out the neutron flux, inadvertently aided in neutron moderation thus increasing reactivity; the core was massive, with uneven flux distribution and physical conditions that were difficult to model; instrumentation for reactivity measurement were unavailable for values below 10% of rated power; there was no containment to prevent radiation release in case of an accident. Additionally, Soviet plants at the time had a seriously deficient safety culture, organizational procedures, and personnel training: lack of transparency and censoring of outspoken critics of the design led to a false belief of “imperviousness” of the reactors; unavailability of decent modeling software led to a poor understanding of phenomena such as fuel burnup; the staff rarely questioned supervisors due to fear of consequences.

The accident started around 1 a.m. with a turbo-generator rundown test, one of the important emergency operating modes. After the start of the test, the reactor power suddenly dropped, prompting the operators to raise completely some of the control rods in order to increase the power. Unbeknownst to them, the low power operation and high fuel burnup led to a build-up of the neutron poison Xenon-135, which was the reason why the power was unresponsive to the lifting of control rods. After the power increased, the test commenced at 1:22 a.m. and rundown was performed on 4 main feedwater pumps, which reduced the coolant flow. This resulted in a sudden power increase (positive void coefficient), prompting the operators to drop the control rods (having a positive scram deficit), which led to an instantaneous power excursion. The uncontrollable reactivity and the drastically increasing temperature and pressure ultimately led to core meltdown and a large steam explosion, which destroyed the reactor core and the building, followed by graphite burning that contributed to a wide-spread release of radioactive isotopes.

Due to the lack of transparency, the exact number of Chernobyl-4 forerunners is unknown. In our database, we have 2 events that appear to meet the criteria, although information about them is also limited. These events are Leningrad-1, 1975 and Beloyarsk-2, 1977, both of which suffered a melting of fuel channels (one channel at Leningrad, and approximately half of the core at Beloyarsk), due to a loss of coolant, presumably aggravated by the positive void coefficient issue of the RBMK design. One of the hypothesized reasons for the event at Beloyarsk is testing of a new cooling water purification system, although no official explanation was given by the Soviet Union. Needless to say, the design and organizational issues brought up before were well known by the regulatory body, however, they failed to act in time to avoid the occurrence of more serious accidents. This further stresses the importance of transparent reporting, communication between plant operators and regulators, and generally learning from operating experience. The effects of the Chernobyl accident were far-reaching in the nuclear world, spawning a period of heightened awareness, panic reporting, increase of transparency, and major organizational and design changes for RBMKs.

4.1.3. Forerunners and lessons learned from the Fukushima Dai-ichi accident

The Fukushima Dai-ichi nuclear accident of March 11, 2011 was a grim reminder of the devastating potential of beyond design-basis accidents. The accident occurred as an aftermath of a tsunami triggered by the magnitude 9 Tohoku Earthquake. Before the event, units 1, 2 and 3 were in normal power operation, unit 4 was refueling with unloaded fuel, and units 5 and 6 were under cold shutdown. The earthquake caused a loss of offsite power to all units, and reactors 1, 2 and 3 were tripped. Emergency diesel generators (EDGs) started and provided emergency power to all units. Units 2 and 3 were cooled using the reactor core isolation cooling (RCIC) system, while the unit 1 used the isolation

condenser, which was cyclically operated to cool down the reactor. The isolation condenser tripped when the tsunami occurred, and stayed isolated due to lack of any power. The tsunami hit shortly afterwards, with waves exceeding the protection of the plant, completely flooding the EDGs and service water systems and resulting in a station blackout. The RCIC continued operating in units 2 and 3 but was tripped eventually due to loss of DC power control, and units 1, 2 and 3 started overheating. Units 5 and 6 were newer, having higher flood barriers, therefore, one EDG in unit 6 managed to survive and provided power to the cooling systems of both units through a cross-tie. The plant operator Tokyo Electric Power Company Holdings (TEPCO) failed to bring external EDGs to the site on time, resulting in a core melt in units 1, 2 and 3. Hydrogen build up resulted in an explosion and breach of containment, and radioactive isotopes were released in the surrounding area. Thousands of people were ultimately displaced, although no casualties have been reported as a direct consequence of the accident thus far. Three other plants in Japan were also affected by the Tohoku Earthquake and the tsunami (see Fig. 8), meaning that a larger catastrophe could have occurred, but fortunately, the EDGs in these plants were not completely flooded.

Despite the beyond design-basis nature of the trigger of the Fukushima Dai-ichi accident, steps could have been taken to avoid or at least mitigate the effects of such a devastating natural phenomenon. In our database, we have mapped out several events that can be considered forerunners to the Fukushima accident, where lessons were not well learned and implemented. Two events are considered to be flooding-related forerunners, while we would also like to put emphasis on two additional events that can be seen as forerunners in a station blackout sense (Fig. 8). The flooding events are the Blayais incident of 1999, and Madras-2, 2004. In both events, the flooding protection of the plants was insufficient, leading to multi-component failures and threatening the cooling capabilities of the reactors. In Blayais, the offsite power supply was lost but, fortunately, the EDGs were unaffected by the flooding. Madras suffered an identical scenario as Fukushima, with a 9.1 earthquake triggering a tsunami that overwhelmed the protection of the plant. Fortunately, only the condenser and seawater pumps were lost, while the EDGs and service water system remained operational. These serious precursor events should have triggered an industry-wide debate regarding the integrity of coastline nuclear plants and the threats of beyond design tsunamis, as well as the proper protection of vital equipment. Additionally, knowing that the newer units on the Fukushima site – namely units 5 and 6 that managed to avoid core damage – had higher flood barriers, raises the question if the plant operator and regulators were aware of the potential flooding vulnerability of older units, knowing that the vital equipment were not properly protected in the event of any flooding exceeding the design basis.

Furthermore, the station blackout events of Kola 1-2, 1993 and Maanshan 1-2, 2001 are emphasized because both of these plants avoided core damage thanks to attaching external (swing) power sources (EDGs, reversible motor-generators) after a station blackout occurrence. These events demonstrated the importance of having available, and easy to deploy, power sources in the near vicinity of the plant, but still far enough to not be affected by the same external initiators. Fukushima Dai-ichi, unfortunately, did not have such power sources available, and the lack of communication/transparency between TEPCO and the government resulted in a failure to bring additional EDGs to the site on time.

The effects of the Fukushima Dai-ichi accident and its lessons had a major impact on the nuclear industry. Multiple design changes related to natural hazards were implemented around the world, such as the stress tests within Europe and the external power sources retrofits. Work has also been done in improving transparency and communication between companies and regulatory bodies, as well as with the general public.

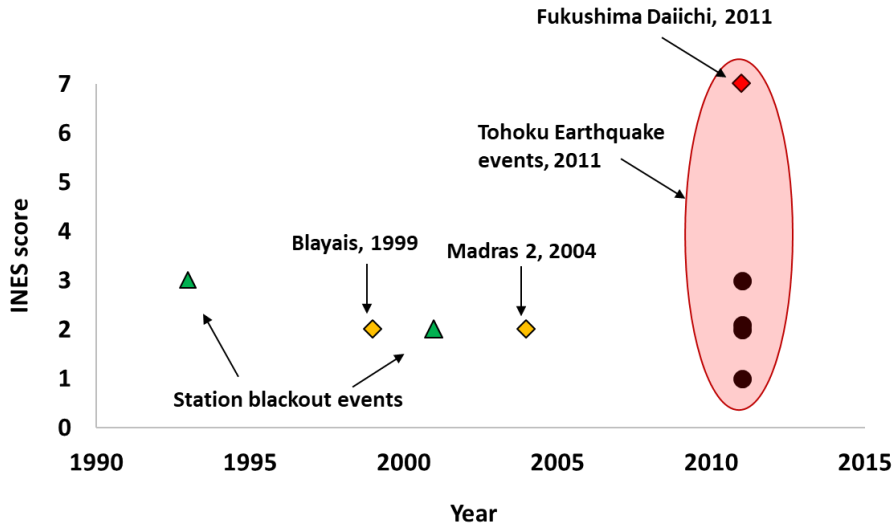


Fig. 8. Forerunners to the Fukushima Dai-ichi accident. Events shown in the figure: Tohoku Earthquake events of March 11, 2011 are Fukushima Dai-ichi 1, 2, 3, 4, 5, 6; Fukushima Dai-ini 1, 2, 3, 4; Tokai 2; and two events at Onagawa-2. Station blackout events are the Kola 1, 2, 1993; and Maanshan 1, 2, 2001.

4.2. Primary water stress corrosion cracking (PWSCC) events

Component failures rooted in the design, choice of materials, and manufacturing process, always have the potential to affect multiple plants. This was the case with the clustering of primary water stress corrosion cracking (PWSCC) events identified in the 80's and early 2000's in the United States. The three major clusters that can be observed are: PWR main feedwater events, BWR recirculation piping events, and PWR reactor pressure vessel (RPV) leakage events (Fig. 9). The root cause for all these PWSCC clusters was the usage of material that was susceptible to stress corrosion (due to lack of knowledge), although their implications varied significantly.

The PWR main feedwater events cluster mostly included acute occurrences, defined with rupture of pipes in the heat extraction and re-heater lines causing immediate plant shutdowns. Only the last event (Trojan, 1987) was prevented before it occurred, as the maintenance team identified signs of accelerated corrosion on the main feedwater pipes and immediately took action. This is a good indication of learning from experience, as Trojan already suffered a similar problem in 1982, so the maintenance team was aware of the problem and worked on preventing its reoccurrence. It is unknown if these phenomena extended beyond the three affected plants shown in Fig. 9 (Trojan, Oconee, Zion).

The BWR recirculation piping degradation events were first identified in Monticello and Nine Mile Point plants in 1982. In Nine Mile Point-1, leaks were observed from the piping, so the plant operators immediately shut down the reactor and opted to replace the pipes. This prompted a series of investigations across multiple BWR plants where the same material was used, leading to the later discoveries presented in the figure. In total, 5 plants were affected and costly repairs were performed to remedy the problem. Knowing the potential severity of a recirculation piping rupture (dangers of LOCA), this cluster of events serves as a good example of how transparency and good communication between plant operators and the regulatory body can trigger reviews, and aid in preventing serious incidents.

By far, the most significant of the clusters is the RPV leakage events in the early 2000's. Identified in 11 reactors, this "pandemic" of events involved leakage from the control rod drive mechanism nozzles due to PWSCC. PWRs use borated water for neutron flux control, which can quickly corrode susceptible material, as was the case in these events. This material susceptibility problem could have had

disastrous consequences as the structural integrity of the reactor pressure vessel was threatened. The most serious of the events, the Davis Besse "near-miss" of 2002, had immense corrosion damage on the RPV head due to borated water leakage from a cracked control rod drive mechanism – only 9.5 mm of steel cladding were left, holding the high pressure (17 MPa) coolant in the vessel. If the vessel had been breached, a large break loss-of-coolant accident (LBLOCA) would have occurred, debris could have clogged the emergency core cooling system, and the ability of the plant to combat this situation would have been put into question. Fortunately, this was avoided as the problem was identified during the scheduled inspections, triggered after several precursory events had occurred in early 2001 (Fig. 9). The good communication and transparent approach between regulators and operators of the plants prevented any accident from occurring.

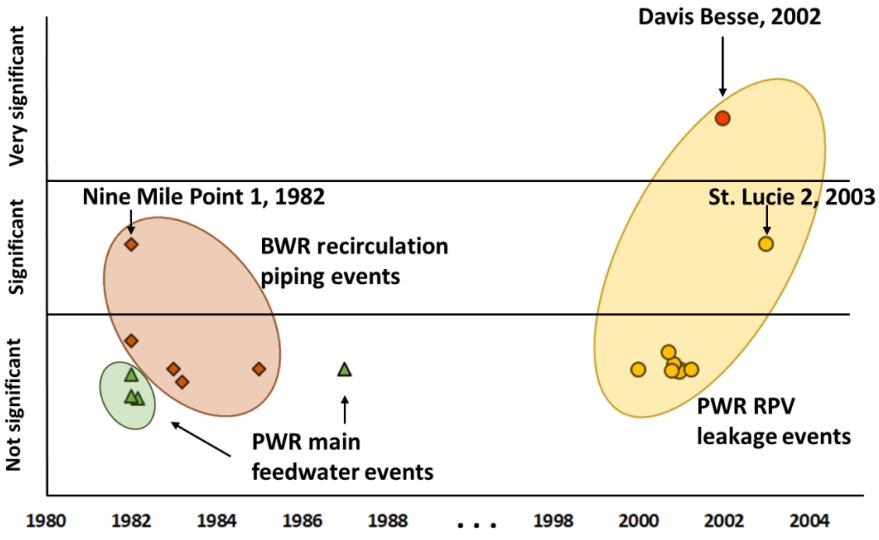


Fig. 9. Clustering of events caused by leakage due to PWSCC. PWR main feedwater events: Oconee-2, 1982; Zion-1, 1982; Trojan, 1982, 1987. BWR recirculation piping events: Nine Mile Point-1, 1982; Monticello, 1982; Pilgrim, 1983; Browns Ferry-3, 1983; Peach Bottom-2, 1985. PWR RPV events: Oconee-1, 2000; ANO-1, 2001; Crystal River-3, 2001; North Anna-2, 2001; Oconee 2, 3, 2001, Palisades, 2001; Surry-1, 2001; Three Mile Island-1, 2001; Davis Besse, 2002; ST. Lucie-2, 2003.

4.3. Interesting events insights based on operating experience

The information presented so far has been largely based on observations of known accidents, problems, systems, and phenomena. However, the database contains some important events that are interesting, strange, unanticipated, or generally difficult to model using the standard PSA models. These observations and events have important takeaways that will be emphasized in this section.

4.3.1. Propagating events

The importance of redundancy of individual trains was already discussed and how steps must be taken to prevent failures to propagate within the system (dependent and common cause failures). However, inter-system and inter-unit failure propagations can also occur, and the consequences can be quite serious. This behavior is difficult to model in standard PSAs and, based on our experience, usually occurs due to latent design errors and component failures. Two events will be presented that have inter-unit propagation, and one intra-unit event having unexpected interaction between different systems.

(Smolensk 2, July 1990)

During testing the automatic activation of a unit 1 emergency power source, the maintenance team inadvertently damaged the cable insulation, causing a short circuit and a fire. The fire damaged unit 2 cables that were laid nearby, causing a loss of two emergency power buses, loss of power to two reactor coolant pumps and a reactor scram. The placement of cables in close proximity to each other for both units was considered to be a serious design flaw.

(Calvert Cliffs-2, February 2010)

One reactor coolant pump (RCP) at unit 1 tripped due to a ground fault. The breakers failed to isolate the ground fault close to the source, which then propagated and tripped the station auxiliary transformer (SAT). All RCPs and condenser recirculation pumps at unit 2 lost power, resulting in an automatic reactor trip from 99.5% power. The loss of the SAT additionally resulted in a loss of the power to one of the safety buses, prompting one emergency diesel generator (EDG) to start. However, it tripped shortly after due to a low lubrication oil pressure. The reactor was ultimately stabilized.

4.3.2. Challenge to the Swiss cheese model

The Swiss cheese model has been always used to highlight the importance of several layers of defense, and the unlikelihood of accidents in complex and reliable technologies. Although to a large extent, this is a very representative model, nevertheless, accidents and events have shown that anomalies can align, even independently, forming a challenge to the multi-layers model. Here, we give some prominent examples of interesting events from our database, where multiple failures happened independently, questioning the unlikelihood of these multiple “unlikely occurrences”. Additionally, this brings questions regarding trusting the individual probabilities and numbers, independence assumptions, validity of reductionism, the role of feedback loops, and others.

(Brunswick, April 1975)

At 10-percent power, a safety relief valve (SRV) was stuck open, rendering the reactor core isolation cooling (RCIC) system inoperable. Operators failed to scram the reactor according to the emergency operating procedures. The high-pressure coolant injection (HPCI) system failed to run as a result of high torus level. Loop B of the residual heat removal (RHR) system failed due to a failure in its respective service water supply. The reactor scrammed automatically after a manual closure of the main steam isolation valve (MSIV).

(Davis Besse, September 1987)

While the plant was in full power operation, a failure in the main feedwater flow transmitter caused an increased flow to the steam generators, causing reactor overcooling and reactivity increase. The operators wanted to insert some control rods to reduce and control the power. However, they inadvertently inserted the axial power shaping rods, causing a power spike; the reactor tripped on the high neutron flux signals. During the event, other unrelated anomalies also occurred: a breaker failure caused a loss of power to one safety bus, a service water pump failed to automatically start due a maintenance error, an atmospheric dump valve and a turbine bypass valve failed open causing excessive cooling, finally, the RHR system was slightly affected due to a void in the discharge piping owed to a nitrogen leakage.

4.3.3. Plant level common cause failures

Systems reliability is known to be threatened by common-cause failures, where CCFs dominate the unreliability quantification of a redundant system. Nevertheless, thanks to experience, CCFs at components level have been well understood and taken into account in reliability analysis, and systems

are designed in a way to minimize the interactions between components and common-cause type of failures through the different concepts of diversification. However, some events in the database surprisingly show signs of a more serious type of CCFs, i.e. at a higher level, namely, at system/plant-level. Plant-level CCFs describe failures and interactions between different independent systems, which are not typically taken into account in PSA modeling. In this section, we give some examples of events showing plant-level CCF potential, which could eventually dominate the core damage sequences.

(COOK, October 1999)

An evaluation of the high-energy line break (HELB) program identified important equipment that were not qualified for the harsh environment resulting from a HELB, or would have been damaged by jet impingement from the break. Potentially affected systems include: auxiliary feedwater (AFW), safety and non-safety-related 600 VAC and lower voltage switchgears, emergency diesel generators (EDGs), component cooling water (CCW), auxiliary building ventilation equipment, cables and conduits inside the containment, and other equipment located near 1- the pressurizer surge line, 2- the chemical volume control system (CVCS) letdown, 3- the steam generator blowdown piping, and 4- HELB doors. The cause of this plant-level CCF is the fact that dynamic loads have not been adequately taken into account; the event triggered several plant modifications and HELB procedural changes.

(Cooper, June 2007)

Multiple systems potentially affected, specifically, the residual heat removal system and the high-pressure coolant injection, due to inadequate post-fire operating procedures.

4.3.4. Unusual errors during testing and maintenance activities

Understanding human related failures is difficult due to its complex nature, and it is the basis of human reliability analysis. In this paper and in [25], the contributions of human related failures were discussed, showing that they very often have a significant, and sometimes a dominating, share of the contributing factors, especially failures related to T&M activities. This section presents some completely unusual examples of maintenance errors, where the team could not foresee the consequences of their actions, or the lack of focus or information have led to bizarre occurrences.

(Davis Besse, April 1980)

During cold shutdown, core cooling was provided by residual heat removal (RHR) pump 2, with pump 1 being unavailable due to maintenance. Mechanical vibrations due to maintenance work in the switchgear room suddenly caused a breaker ground relay to actuate, causing two essential buses to trip. The loss of the buses caused problems in the RHR pump 2, as the logic circuit transferred the suction of the pump to the sump, which was empty. This resulted in air being drawn into the suction of the pump, which tripped and resulted in the loss of reactor cooling. The pump was recovered after 2.5 hours and reactor cooling was re-established.

(Brokdorf, July 1995)

While the plant was shut down and the core was unloaded to the spent fuel pool, the T&M team erroneously started activities on emergency diesel generators (EDGs) 4 and 8 instead of the designated 1 and 5, making them inoperable. This condition did not cause acute distress to any safety system, but a loss of offsite power event would have led to loss of spent fuel cooling. However, the long grace period for manually starting the EDGs and the additional measures in place would have been sufficient to quickly re-establish the spent fuel cooling.

(Pickering-5, July 1995)

In a bizarre turn of events, two technicians carried out maintenance work on the fast shutdown system of the wrong reactor (reactor 5 instead of reactor 6), disabling the system for the reactor that was operating at full power at the time.

(Monticello, December 2014)

During testing of one emergency diesel generator (EDG), a non-licensed operator erroneously adjusted the settings of the governor belonging to the other EDG. This effectively caused both EDGs to be declared inoperable.

5. Conclusions

With more than 1250 insightful events from commercial nuclear power plants, the ETHZ curated nuclear events database is the largest open-access database in the world. In addition to the constructive discussions offered in [25], the present paper has presented important analyses and industry insights with the goal of raising awareness to several key aspects threatening the safety and reliability of nuclear power plants.

Important takeaways, which can be highlighted from the discussions, include:

- Major accidents always trigger a wave of “reactive” reporting, mostly due to increased alertness, improved transparency, uncovering latent design errors, and heightened public pressure. This trend appears to last 5 to 6 years after which the implemented design changes inevitably lead to safer operation and lower number of events. Additionally, changes in regulatory or corporate management, which usually takes place in cycles of 5-6 years, can result in lower alertness and weakened transparency culture, and lead to deteriorating reporting habits. A good approach that can be borrowed from the military is the war drill practice, i.e. in order to keep the level of vigilance high requires to constantly challenge the peacefulness of operation, and to have accident mockups and simulations, which can keep the plant operators and personnel alert at all times.
- The leading causes for multi-unit events are external triggers and design issues. These factors must be taken into account the most, when adapting PSAs to cover multi-unit events.
- Common-cause failures (CCFs) occur fairly frequently and can completely erode the safety of the plant. Frequent review of component design and operating procedures, employing different teams for T&M activities on redundant trains, and sharing operational experience between plants of similar designs, are some of the steps that should be taken in order to limit future occurrences of CCFs.
- Quantitative signs of aging can be observed for plants after the age of 25. Therefore, frequent testing, inspections, and design reviews and updates should be performed by the licensees.
- Learning from previous accidents and precursors is essential in preventing the occurrence of new accidents. This calls for a larger recording, reliance, and sharing of operational data to support learning from experience and avoid reoccurrence of accidents and events.
- Important lessons can be learned from events, as qualitative insights can be very beneficial. Raising awareness to these issues can potentially bring light to similar vulnerabilities in currently operating plants.

The ETHZ nuclear events database can be tremendously beneficial to many interested parties, including researchers, industry partners and the general public. We trust that, with increased regulations for operational monitoring, events recording, increased automation and sensor technology levels, aided by big data and machine learning capacities, we are reaching a level of unprecedented abilities for learning and predicting. The structure and utilization of the database can serve as best

practice for other areas in industry. The database, along with the access tool and user manual, are publicly available at: http://er-nucleardb.ethz.ch/.

References

1. Kröger, W. and E. Zio, *Vulnerable Systems*. 2011: Springer Publishing Company, Incorporated.
2. Sornette, D., W. Kröger, and S. Wheatley, *New Ways and Needs for Exploiting Nuclear Energy*. 2018: Springer.
3. Mosleh, A., *PRA: a perspective on strengths, current limitations, and possible improvements.* Nuclear Engineering and technology, 2014. **46**(1): p. 1-10.
4. Kröger, W. and D. Sornette. *Reflections on Limitations of Current PSA–Methodology*. in *International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA)*. 2013.
5. Zhang, X. and S. Mahadevan, *Bayesian network modeling of accident investigation reports for aviation safety assessment.* Reliability Engineering & System Safety, 2021. **209**: p. 107371.
6. Birkhofer, A. and K. Köberlein, *Data Situation and the Quality of Risk Assessment*, in *Reliability Data Collection and Use in Risk and Availability Assessment*. 1986, Springer. p. 3-15.
7. Kröger, W., D. Sornette, and A. Ayoub, *Towards Safer and More Sustainable Ways for Exploiting Nuclear Power.* World Journal of Nuclear Science and Technology, 2020. **10**(03): p. 91.
8. Duffey, R.B., *The Risk of Extended Power Loss and the Probability of Emergency Restoration for Severe Events and Nuclear Accidents.* Journal of Nuclear Engineering and Radiation Science, 2019. **5**(3).
9. Mach, P. *Life management and operational experience feedback-tools to enhance safety and reliability of the NPP*. in *PROCEEDINGS OF THE 2nd INTERNATIONAL SYMPOSIUM ON SAFETY AND RELIABILITY SYSTEMS OF PWRs AND VVERs*. 1997. Brno, Czech Republic.
10. Rasmussen, J., *Risk management in a dynamic society: a modelling problem.* Safety science, 1997. **27**(2): p. 183-213.
11. Khakzad, N., F. Khan, and N. Paltrinieri, *On the application of near accident data to risk analysis of major accidents.* Reliability Engineering & System Safety, 2014. **126**: p. 116-125.
12. IAEA, *Nuclear Power Plant Operating Experience*. 2018, INTERNATIONAL ATOMIC ENERGY AGENCY: Vienna.
13. Moura, R., Beer, Michael, Patelli, Edoardo, Lewis, John, Knoll, Franz, *Learning from accidents: interactions between human factors, technology and organisations as a central element to validate risk studies.* Safety Science, 2017. **99**: p. 196-214.
14. Wheatley, S., B. Sovacool, and D. Sornette, *Of disasters and dragon kings: a statistical analysis of nuclear power incidents and accidents.* Risk analysis, 2017. **37**(1): p. 99-115.
15. IAEA, *IAEA Releases 2019 Data on Nuclear Power Plants Operating Experience*. 2020.
16. Ayoub, A., Stankovski, Andrej, Kröger, Wolfgang, Sornette, Didier *Status of the ETHZ Curated Nuclear Events Database*. in *30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15)*. 2020. Venice, Italy.
17. Ayoub, A., W. Kröger, O. Nusbaumer, and D. Sornette, *Simplified/Harmonized PSA: A Generic Modeling Framework*, in *International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2019)*. 2019, American Nuclear Society (ANS): Charleston, SC, USA.
18. Ayoub, A., W. Kröger, and D. Sornette, *Generic Probabilistic Safety Assessment Models for International Precursor Analysis Applications*, in *International Youth Nuclear Congress (IYNC)*. 2020: Sydney, Australia.
19. U.S.NRC., *Licensee Event Report Search (LERSearch)*. 2020: retrieved from https://lersearch.inl.gov/Entry.aspx.
20. U.S.NRC., *Accident Sequence Precursor (ASP) Program*. 2020: retrieved from https://www.nrc.gov/about-nrc/regulatory/research/asp.html.
21. Johnson, J.W. and D.M. Rasmuson, *The US NRC's accident sequence precursor program: an overview and development of a Bayesian approach to estimate core damage frequency using precursor information.* Reliability Engineering & System Safety, 1996. **53**(2): p. 205-216.
22. WANO, *Performance Analysis Program*. 2020: retrieved from https://www.wano.info/services/performance-analysis.

23. IAEA, *IRS Guidelines – Joint IAEA/NEA International Reporting System for Operating Experience*. 2010: Vienna.
24. JRC, E., *Clearinghouse on Operating Experience Feedback*. 2020: retrieved from https://clearinghouse-oef.jrc.ec.europa.eu/search/oef_records.
25. Ayoub, A., Stankovski, Andrej, Kröger, Wolfgang, and Sornette, Didier, *The ETH Zurich Curated Nuclear Events Database: Layout, Event Classification, and Analysis of Contributing Factors.* Reliability Engineering & System Safety, 2021.
26. Chernov, D., Ayoub, Ali, Sansavini, Giovanni, and Sornette, Didier, *Averting disaster before it strikes: how to ensure your subordinates warn you while there is still time to act*. 2022: Springer. Handbook to be published.
27. Chernov, D., Sornette, Didier, Sansavini, Giovanni, and Ayoub, Ali, *No one told the boss. Case studies of major disasters and failures of upward feedback about observed risks before and during disasters*. 2021: Springer. Book to be published.
28. Lim, H.-G., Kim, Dong-San, Han, Sang Hoon, Yang, Joon Eon, *Development of logical structure for multi-unit probabilistic safety assessment.* Nuclear Engineering and Technology, 2018. **50**(8): p. 1210-1216.
29. Modarres, M., T. Zhou, and M. Massoud, *Advances in multi-unit nuclear power plant probabilistic risk assessment.* Reliability Engineering & System Safety, 2017. **157**: p. 87-100.
30. Birolini, A., *Reliability engineering: theory and practice*. 2013: Springer Science & Business Media.
31. Dechy, N., J.-M. Rousseau, and F. Jeffroy, *Learning lessons from accidents with a human and organisational factors perspective: deficiencies and failures of operating experience feedback systems.* Nuclear safety: new challenges, gained experience and public expectations. Paris, 2011. **7**.
32. Sornette, D., *Why stock markets crash: critical events in complex financial systems*. Vol. 49. 2017: Princeton University Press.

Chapter 4

Generic and adaptive probabilistic safety assessment models: Precursor analysis and multi-purpose utilization

Motivated by learning from experience and exploiting existing knowledge in civil nuclear operations, we have developed in-house generic Probabilistic Safety Assessment (PSA) models for pressurized and boiling water reactors. The models are computationally light, handy, transparent, user-friendly, and easily adaptable to account for major plant-specific differences. They cover the common internal initiating events, frontline and support systems reliability and dependencies, human-factors, common-cause failures, and account for new factors typically overlooked in many developed PSAs. For quantification, the models use generic US reliability data, precursor analysis reports and studies, the ETHZ Curated Nuclear Events Database, and experts' opinions. Moreover, uncertainties in the most influential basic events are addressed. The generated results show good agreement with assessments available in the literature with detailed PSAs. We envision the models as an unbiased framework to measure nuclear operational risk with the same "ruler", and hence support inter-plant risk comparisons that are usually not possible due to differences in plant-specific PSA assumptions and scopes. The models can be used for initial risk screening, order-of-magnitude precursor analysis, and other research and pedagogic applications especially when no plant-specific PSAs are available. Finally, we are using the generic models for large-scale precursor analysis that will generate big picture trends, lessons, and insights.

Based on **Ayoub, A.,** Kröger, W., & Sornette, D. (2021). Generic and adaptive probabilistic safety assessment models: Precursor analysis and multi-purpose utilization. *Nuclear Engineering and Technology.* Under Review.

1. Introduction

Due to the rare nature of severe accidents in the nuclear industry (core damage and large releases), it is very hard to quantify its risk on a pure empirical basis. Therefore, probabilistic frameworks such as Probabilistic Safety Assessment (PSA) [1] have provided a sound alternative for risk estimation by system decomposition and making use of failure data at a more basic level (e.g. components level) to derive system-level behavior. PSA is performed at three sequential levels [2]:

1- PSA Level 1 models the plant's response to initiating/perturbing events and aims at quantifying the risk of a core damage, namely, core damage frequency (CDF) per reactor-year.
2- PSA Level 2 models the respective containment response to the accident/initiator, and aims at quantifying the radioactive release to the environment, namely, large early release frequency (LERF) or large release frequency (LRF) per reactor-year.
3- PSA Level 3 models the offsite consequences of the release, and aims at quantifying the risk to the public (frequency and impact on public health and the environment, as well as direct costs).

Moreover, PSA frameworks are used to quantify the risk of operational experience through precursor analysis. A precursor is an observed event resembling a truncated accident sequence (accident sub-chain) that could lead to an accident (e.g. core damage) if combined with additional adverse conditions [3]. Precursor analysis is a hybrid empirical-probabilistic method to estimate operational risks such as CDF, by mapping the observed event sequence to the PSA model, and calculating the remaining distance (probability) to core damage. Precursor analysis have been used by regulators around the world to monitor plants' risk over time [4], and provide an alternative robust estimate of CDF other than PSA CDFs [5].

Over the time, and through its extensive use – both for regulatory and risk-informed decision-making purposes – PSA witnessed rapid developments and reached high levels of details and sophistication. It evolved as a very plant-specific and site-specific method, capturing the very details of each plant. However, it remains difficult to use or understand outside the circle of their developers or super-experts [6]. The resulting complexities, in addition to the absence of a standardized PSA methodology and scope, made it difficult to compare results of different PSAs [7], and hindered possibilities for design-to-design and plant-to-plant safety comparisons. Therefore, PSAs became less suitable to understand industry-wide performance and big picture safety insights and trends.

Some researchers and organizations started efforts to establish generic PSA models or PSA platforms to facilitate exchanges and understanding. For example, the Open PSA Initiative [8, 9] started an open platform to encourage peer review and transfer of ideas and PSA lessons, and to reach a common PSA representation worldwide. The Spanish Nuclear regulator (CSN) has initiated a PSA harmonization activity to construct generic and standardized PSA models for the Spanish nuclear fleet to achieve a licensee-independent risk-view, targeted inspection activities, and unified platform for precursor analysis [10]. The Nordic PSA Group (NPSAG) started a project to harmonize PSA and improve its transparency and comparability [11, 12]. At EDF (Electricité de France), efforts are done to simplify PSA representation through modularization and "object-oriented" modeling [13].

In this work, we offer a step forward towards PSA harmonization and handiness. We present our final in-house PSA models for light water reactors (LWRs) initially introduced in [6, 14]. We have developed an open and generic PSA models for pressurized and boiling water reactors (PWRs and BWRs) in SAPHIRE (a probabilistic risk and reliability assessment software tool, which stands for *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations*) [15]. The models cover all common internal initiating events, with intermediate complexity generic event trees and fault trees capturing important design differences without going to the detailed component level connections and layouts. This mentality of going simple and generic allowed for accounting for important contributors and lessons learnt from analyzing hundreds of precursors in our ETHZ nuclear events database [16, 17].

The developed PSA models proved to be well suited to perform efficient precursor analyses, providing representative order-of-magnitude risk estimates of operational events. The models will offer an unbiased framework to compare operational events and precursors at different plants by annealing-out many plant-specific differences as a result of going generic, hence forming a basis for inter-plants comparisons. By pooling worldwide nuclear operational experience, the models will allow us to understand big picture safety insights and trends. Our PSAs can be used to support plant-specific PSAs, and with their neat and simplified representation, they will provide an open and transparent framework that is ready to be employed when no access to detailed PSAs is provided (e.g. by research institutes, universities, NGOs and other organizations).

The organization of the manuscript is as follows. In Section 2, we present our modeling philosophy and approach. Sections 3 and 4 presents our detailed PWR and BWR models respectively. Section 5 discusses the quantification of the models. Section 6 presents applications of hands-on precursor

analysis and examples. Section 7 concludes. An appendix at the end shows some modeled event trees and fault trees.

2. Modeling philosophy

Although LWRs differ in design and layout between different countries and vendors, nevertheless, the physics is basically the same and all plants utilize the same safety functions. In this work, we have developed generic, yet adaptive PSA models for both PWRs and BWRs, where each of the two models contains a set of linked event trees and fault trees of intermediate details. Each model is organized in a way suitable to describe all reactors of the same technology, with room for customization/adaptation to account for differences and design-specificities in available systems, configurations, degree of redundancy, human interventions and automation level, and support dependence. Depending whether a specific plant design has a specific safety system/function or not, its top events will be put to its nominal fault tree failure value or to a fail-state (Fail True). For example, the high pressure sump recirculation (HPR) function in PWRs is only available in some plants (mainly in US plants), and similarly for BWRs, with the differences in the available systems between the various construction lines such as the isolation condenser (IC), high pressure core spray (HPCS), and reactor core isolation cooling (RCIC).

Our nuclear events database [16] has been a major asset supporting many of our modeling needs, assumptions, and decisions. The developed models cover internal initiating events that are either very frequent, very serious, classical design-basis events, or appeared as precursors in our database. Furthermore, PSA level 1 event trees are developed for each initiating event, with two end states, 1- core damage (CD) when no sufficient core cooling is provided, and 2- success (OK) when the safety functions manage to cool the core and bring the reactor to a stable and safe state (within 24 hours).

Events and functions of the event trees are quantified with devoted fault trees that quantify failure probabilities at an aggregated train level -- without going into very components details. Support systems contributions are captured within the fault trees, and have both a global and a local element. Global support failures are failures on inter-system shared support trains, hence affecting trains in different safety systems (e.g. a shared AC bus), while local support failures are failures limited to a single train within a specific safety system (single pump component cooling circuitry or local activation/control logic circuity). Moreover, the fault trees include important human factors and human-related actions realized in our database [17], such as operator errors of omission and commission (EOO and EOC respectively), testing and maintenance (T&M) errors, and T&M unavailabilities. Common-cause failures (CCFs) are considered at two levels, a plant-level CCF[5] inferred from events within our database [18] that is modeled at the event tree level, and a typical system-level CCF modeled at the fault tree level. The conservative Beta-factor model was adopted for CCF quantification (details in section 5).

Recovery potentials are explicitly modeled in the fault trees as basic events, however, conservatively put to a failure state for most of the safety systems. Recovery of emergency diesel generators (EDGs) and some other support systems (e.g. offsite power) is an exception, as they are outside the containment and are generally, and realistically, easier to recover. Nevertheless, to be fair in our precursor analysis, cross-tying and recovery possibilities are credited whenever they are explicitly mentioned in the event following the logic used in the USNRC Accident Sequence Precursor program (ASP) [19].

[5] Failures or potential failure in different systems, due to the same cause or some interactions, and this is typically not taken into account in PSA modeling. It includes deficits in safety culture, organizations, designs, and procedures, that tend to affect multiple systems, and sometimes the whole plant.

Our models are limited to PSA level 1, hence generating CDF estimates only. For the LERF/LRF assessment (PSA level 2), we provide a rough estimate using the one-tenth rule of thumb, i.e. a conditional containment failure probability of 10% [20, 21]; hence LERF is estimated as one-tenth of the CDF. This assumption was also used in the precursor analysis calculations, unless there was a containment bypass or a containment function failure during that precursor, in such a case, the LERF is equal to the CDF. Finally, our models are limited to the "at power" operation mode only.

3. PWR models

For PWRs, we have considered the following internal initiating events:

- General transients (including loss of main feedwater).
- Complicated transients:
    - Steam generator tube rupture (SGTR).
    - Loss of condenser heat sink (LOCHS).
    - Main Steam line break (MSLB).
- Loss of coolant accidents (LOCAs):
    - Small break LOCA (SBLOCA).
    - Medium break LOCA (MBLOCA).
    - Large break LOCA (LBLOCA).
- Total loss of support functions:
    - Loss of offsite power (LOOP).
    - Total loss of service water – both essential and normal (TLOSW).
    - Loss of normal service water (LONSW).

For each of these initiators, an event tree is developed, encompassing safety systems/functions and their backups, needed to mitigate core damage. Table 1 lists these generic safety functions and the respective modeled safety systems/top events.

Table 1. Generic PWR safety functions and the associated modeled safety systems/top events

Safety Functions	Safety Systems/Top Events
Reactivity control and reactor sub-criticality	• Reactor trip (SCRAM and emergency boration)
Primary circuit integrity and pressure control	• Pilot operated relief valves (PORV) • Feed and Bleed (F&B) • Secondary side steam dump
Core re-flooding and primary inventory conservation	• High pressure injection system (HPIS) • Re-flooding accumulators • Low pressure injection system (LPIS)
Maintaining core cooling (including long-term residual heat removal)	• Main Feedwater (MFW) • Emergency/auxiliary Feedwater (AFW) • Residual heat removal (RHR) system (both shutdown cooling and sump recirculation modes) • High pressure sump recirculation (HPR)

Additionally considered events include:

- Emergency power supply failure (EPS).
- Early and late offsite power recovery.
- Service water system recovery.
- Ruptured steam generator isolation.
- Main steam-line isolation.
- Plant-level CCFs (as explained in section 2).
- Reactor coolant pump (RCP) seal LOCA.

Most of the modeled events -- especially for systems with multiple redundant trains -- have comprehensive fault trees quantifying their reliability following the modeling philosophy explained in section 2, covering frontline, support, human, and CCF contributions.

Table 2 shows a summary statistics of the structures used in our PWR PSA, having 77 fault trees, 11 event trees, and more than 2 million cutsets.

Table. 2. Summary statistics of the PWR PSA model

Data Type	Number of Records
Fault Trees (Tops and Transfers)	77
Event Trees (Tops and Transfers)	11
Basic Events	249
Gates	418
Sequences	114
Cutsets	> 2,000,000

Figs. 1, 2, and 3 show some examples of our developed PWR event trees and fault trees. A full access to the PWR PSA models is available at Mendeley Data (http://dx.doi.org/10.17632/y9wfgyk6nz.1#folder-d062efaf-c881-46aa-b7c1-73be535bf5c0).

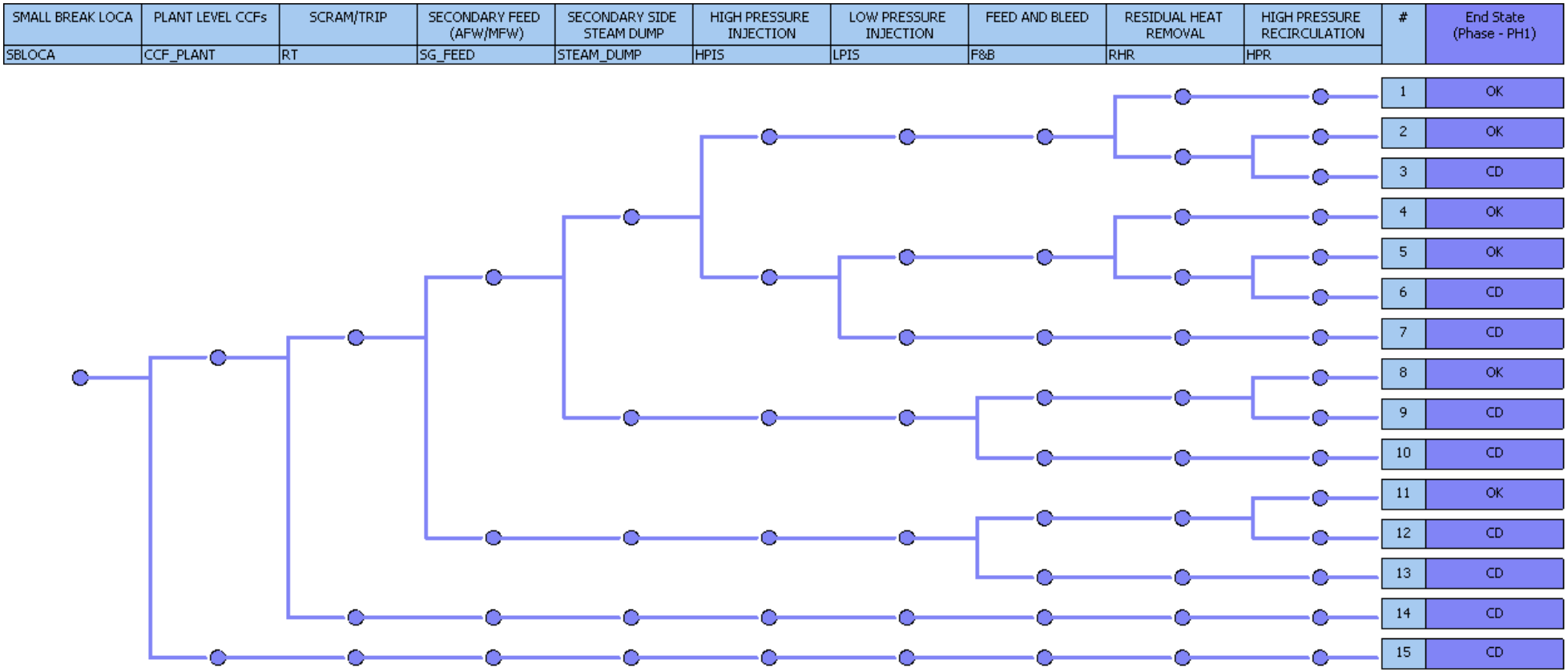


Fig. 1. An example of a developed PWR small-break LOCA event tree with two end-states: core damage (CD) and no core damage (OK)

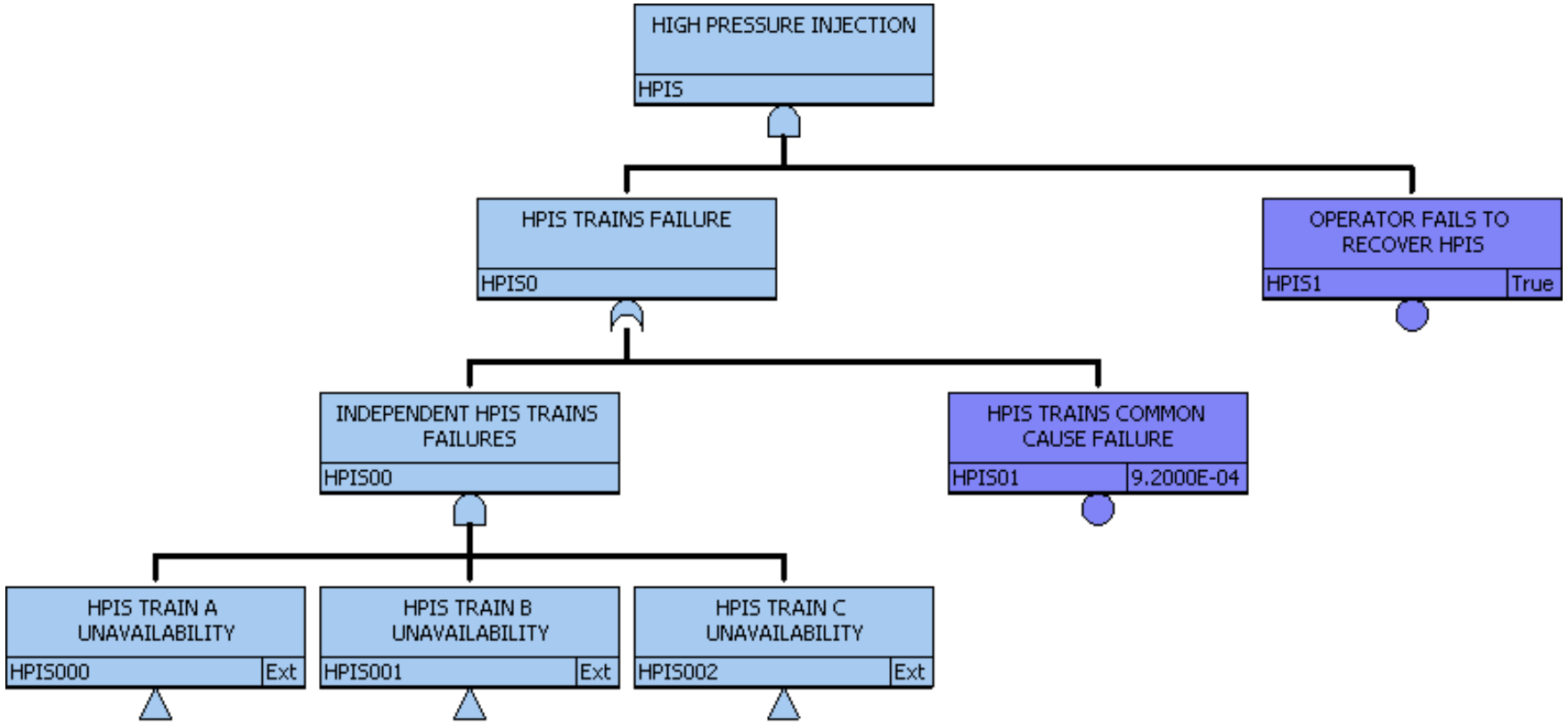


Fig. 2. An example of a developed PWR high-pressure injection system fault tree (see Fig. 3 for the transfer train fault tree)

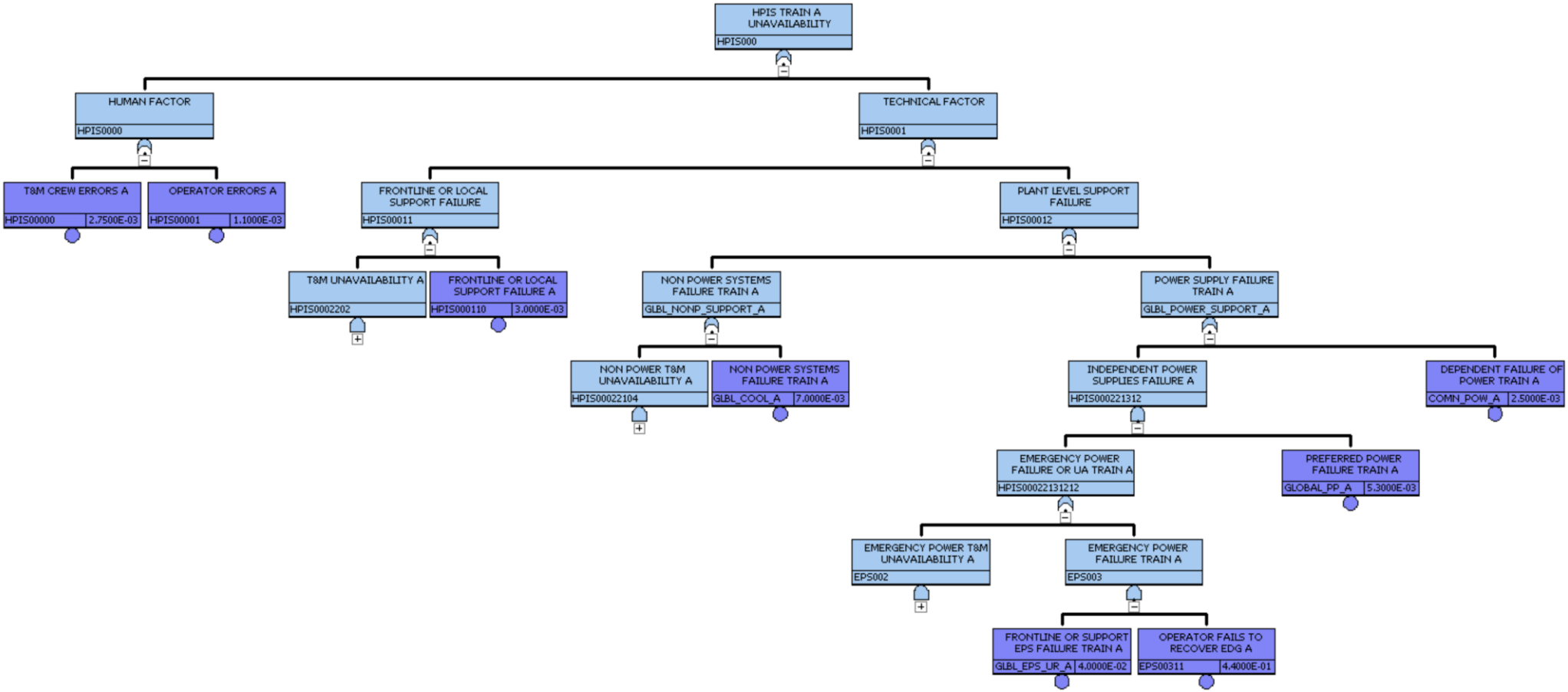


Fig. 3. Part of the PWR high-pressure injection train fault tree (for paper presentation purposes, additional branches are hidden under the '+' signs)

4. BWR models

For BWRs, we have considered internal initiating events similar to those modeled for PWRs with the exception of steam generator tube ruptures and main steam line breaks.

As in PWR models, an event tree is developed for each initiating event, encompassing safety systems/functions, and their backups. Table 3 lists these generic safety functions and the respective modeled safety systems/top events in our BWR PSA.

Table 3. Generic BWR safety functions and the associated modeled safety systems/top events

Safety Functions	**Safety Systems/Top events**
Reactivity control and reactor sub-criticality	• Reactor trip (SCRAM and emergency boration)
Primary circuit integrity and pressure control	• Safety relief valves (SRVs) • Reactor depressurization (automatic and manual)
Core re-flooding and primary inventory conservation	• Main Feedwater (MFW) • Condensate system (COND) • High pressure coolant injection (HPCI) • High pressure core spray (HPCS) • Reactor core isolation cooling (RCIC) • Control rod drive injection (CRD) • Low pressure coolant injection (LPCI) • Low pressure core spray (LPCS) • Alternative low pressure injection sources (fire, service water, or others)
Maintaining core cooling (including long-term residual heat removal)	• Isolation condenser (IC) • Power conversion system (PCS) • Residual heat removal (RHR) system (both shutdown cooling and suppression pool cooling modes)

Additionally considered events include:

- Emergency power supply failure (EPS).
- Early and late offsite power recovery.
- Service water system recovery.
- Plant-level CCFs (as explained in section 2).

Most of the modeled events have comprehensive fault trees quantifying their reliability following the modeling philosophy explained in section 2, covering frontline, support, human, and CCF contributions.

Table 4 shows a summary statistics of the structures used in our BWR PSA, having 75 fault trees, 9 event trees, and more than 2 million cutsets.

Table. 4. Summary statistics of the BWR PSA model

Data Type	Number of Records
Fault Trees (Tops and Transfers)	75
Event Trees (Tops and Transfers)	9
Basic Events	224
Gates	221
Sequences	98
Cutsets	> 2,000,000

Figs. A. 1 and A. 2 in the appendix show an example of a developed BWR event tree and fault tree. A full access to the BWR PSA models is available at Mendeley Data (http://dx.doi.org/10.17632/y9wfgyk6nz.1#folder-d062efaf-c881-46aa-b7c1-73be535bf5c0).

5. Data and quantification

For hardware unreliability data, and testing and maintenance unavailabilities (T&M UA), we are using US generic component reliability and availability data from the 2015 update of the NUREG/CR-6928 [22], aggregating components reliability parameters (both frontline and support components) to come up with a train failure probability estimate. The US, having the largest nuclear fleet, serves as a very good representative sample. An 8 hours mission time was used for the injection functions (e.g. HPIS), and 24 hours for the recirculation and decay heat removal phase (e.g. AFW, RHR) and global power and cooling support systems (e.g. EDGs, component-cooling pumps). Similarly, for initiating events frequencies and their uncertainty distributions, the 2015 update of the NUREG/CR-6928 was used.

For human error probabilities (EOO) and recovery actions, we used generic estimates similar to the classical methodologies of THERP, ATHENA, and the old USNRC precursor studies [23-26], depending on the feasibility of the operator action and recovery potentials (time, stress, prescriptive procedure, etc.). Regarding some basic events deduced from our database, such as EOC and T&M errors, we used their relative importance (occurrence frequency) in the database, as well as some expert's opinion, as proxies for their probabilities.

For computational purposes, we only model uncertainties in the most influential basic events based on their calculated importance measure (Fussell-Vesely, Risk reduction, Birnbaum Importance) [27], these include initiating events frequencies, plant-level CCFs, system-level CCFs, and EOOs. Furthermore, we also account for uncertainties in our database-estimated basic events (EOC, T&M errors, plant-level CCF).

Generally speaking, for system-level CCFs, a Beta-factor uniform distribution with [2%-20%] support (range) was adopted, including a worst-case scenario of 20% share of CCFs according to [28]. Going one level up, i.e. to plant-level CCF, the Beta-factor here is envisioned to go down 1 to 2 orders of magnitude (based on our database frequencies), therefore, we employ a plant-level Beta-factor uniform distribution with support [0.02%-2%] which is in line with the findings of [29], calculating a slightly less than 2% intersystem Beta-factor. Taking a classical system failure probability of about 10^{-4} per demand, a plant-level CCF uniform distribution with support [2 10^{-8} to 2 10^{-6}] is expected. For human errors and other uncertain parameters where no further information are given, a uniform (non-informative) distribution spanning one-order of magnitude is used following expert's opinion.

Table 5 presents all the modeled PWR and BWR initiating events along with their respective frequency distribution [22].

Table 5. PWR and BWR initiating events frequency distributions per reactor year (for explanation of acronyms, see section 3)

Initiating Event	**Frequency Distribution**
General Transient (PWR)	Gamma (α = 7.9, β = 11.6)
General Transient (PWR)	Gamma (α = 11.8, β = 16)
LOCHS (PWR)	Gamma (α = 2.5, β = 52)
LOCHS (BWR)	Gamma (α = 3.7, β = 33)
SGTR (PWR)	Gamma (α = 2.5, β = 1500)
MSLB (PWR)	Gamma (α = 10.5, β = 1660)
SBLOCA PWR (sum of all small LOCAs)	Gamma (α = 0.4, β = 535)
SBLOCA BWR (sum of all small LOCAs)	Gamma (α = 0.4, β = 106)
MBLOCA (PWR)	Gamma (α = 0.3, β = 1997)
MBLOCA (BWR)	Gamma (α = 0.4, β = 4418)
LBLOCA (PWR)	Gamma (α = 0.3, β = 50800)
LBLOCA (BWR)	Gamma (α = 0.3, β = 25420)
LOOP	Gamma (α = 54.5, β = 1750)
TLOSW	Gamma (α = 0.5, β = 2032)
LONSW	Uniform ($5\ 10^{-4}$, $5\ 10^{-3}$)*

*Experts opinion, α and β are the Gamma distribution shape and rate parameters respectively

Table 6 shows some of the modeled basic events, that are common to both PWRs and BWRs, along with their respective nominal values/distributions. More examples are presented in the appendix (Tables A.1 and A.2). For brevity, we only present a sample of the whole list, and the reader is referred to the accompanying SAPHIRE PSA models for the full data.

Table 6. A sample of PWR and BWR common basic events and their nominal values

Basic Event	**Nominal Value or Distribution**
General Train-level EOC	Uniform ($2\ 10^{-4}$, $2\ 10^{-3}$)**
General Train-level T&M Errors	Uniform ($5\ 10^{-4}$, $5\ 10^{-3}$)**
Operator Fails to Recover an EDG	Uniform ($8\ 10^{-2}$, $8\ 10^{-1}$)*
Early Offsite Power Recovery	Uniform ($5\ 10^{-2}$, $5\ 10^{-1}$)*[30]
Late Offsite Power Recovery	Uniform ($2\ 10^{-2}$, $1.2\ 10^{-1}$)*[30]
SW Recovery	Uniform ($1\ 10^{-3}$, $1\ 10^{-2}$)*
Operator Fails to Initiate Emergency Boration	Uniform ($5\ 10^{-3}$, $5\ 10^{-2}$)*[31]
Failure of a Safety Power Bus (Including Breaker Failure)	$2.5\ 10^{-3}$
Global SW/CCW Train UR	$7\ 10^{-3}$
Global SW/CCW Train UA	$1.3\ 10^{-2}$
Operator Fails to Actuate RHR	Uniform ($5\ 10^{-4}$, $5\ 10^{-3}$) [32]
RHR CCF	Uniform ($1.7\ 10^{-4}$, $2\ 10^{-3}$)

*Experts opinion; **Database-estimated basic events; CCW: Component Cooling Water

For a numerical exercise, we adapted our PWR PSA models to match a generic Westinghouse (W) PWR. Fig. 4 shows its CDF distribution generated using a large Latin hypercube sample of the model's uncertain parameters and basic events.

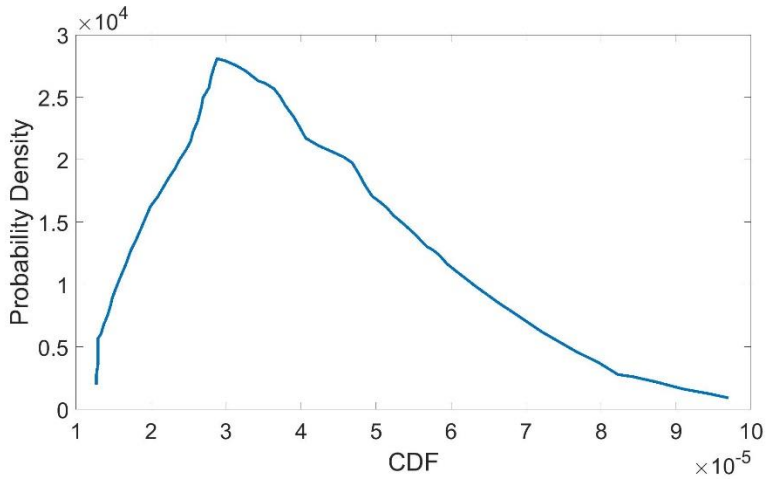


Fig. 4. Calculated CDF distribution of a generic PWR (W) with the following uncertainty statistics: mean 3.9 10^{-5}, standard deviation 1.6 10^{-5}, and 5th and 95th percentiles 1.7 10^{-5} and 7 10^{-5} respectively.

Table 7 shows the PSA results of different Westinghouse plants and a generic PWR found in the literature. The table presents the mean CDF, along with the 5th and 95th percentiles (p_{05} and p_{95}) if available, thus serving as a benchmark for our generic PSA calculations.

Table 7. Literature PSA results of different PWRs (internal events only)

	CDF p_{05}	**Mean CDF**	**CDF p_{95}**
Surry (W) [33]	6.8 10^{-6}	4 10^{-5}	1.3 10^{-4}
Sequoyah (W) [32]	1.2 10^{-5}	5.7 10^{-5}	1.8 10^{-4}
Ringhals (W) **[34]**	NA	2 10^{-5}	NA
A Generic PWR **[35]**	NA	3 10^{-5}	NA

For a typical General Electric (GE) BWR-4 plant design, our PSA model produces the following CDF distribution generated using Latin hypercube sampling (Fig. 5).

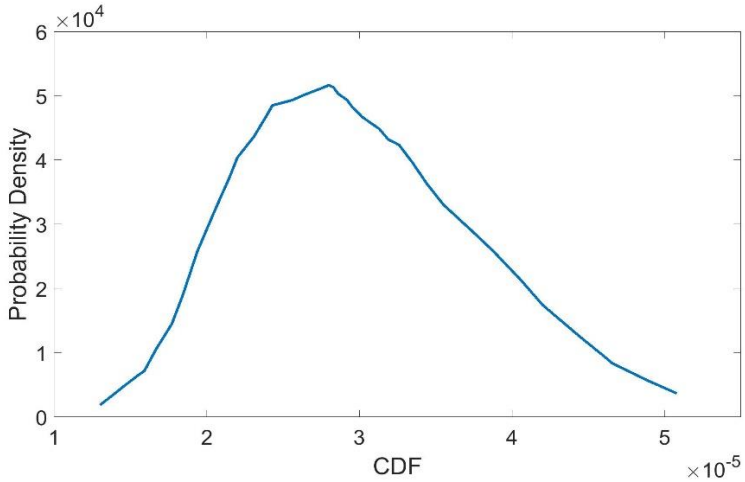


Fig. 5. Calculated CDF distribution of a typical GE BWR-4 design with the following uncertainty statistics: mean 2.9 10^{-5}, standard deviation 7.8 10^{-6}, and 5th and 95th percentiles 1.8 10^{-5} and 4.3 10^{-5} respectively.

Table 8 shows the PSA results of different BWR-4 plants and a generic BWR found in the literature. The table presents the mean CDF, along with the 5th and 95th percentiles (p_{05} and p_{95}) if available, thus serving as a benchmark for our generic PSA calculations.

Table 8. Literature PSA results of different BWRs (internal events only)

	CDF p_{05}	**Mean CDF**	**CDF p_{95}**
Peach Bottom **[34]**	$2\ 10^{-7}$	$4.5\ 10^{-6}$	$9\ 10^{-5}$
Forsmark **[34]**	NA	$1.1\ 10^{-5}$	NA
A Generic BWR **[36]**	NA	$1.87\ 10^{-5}$	NA

Even though our models do not go to the plant-specific details, nor they are meant to replace industrial PSAs, the obtained results (Fig. 4 and 5) show a very good agreement with the literature ranges as depicted in Tables 7 and 8. In fact, the mean CDFs collected from the literature fit well within the calculated CDF distributions, and even more, our calculated CDF point estimates reasonably match the literature values shown in the tables.

Moreover, thanks to the easy arrangement and handiness of our PSA models, if the user is not satisfied with the generic estimates, and is interested in a more plant-specific experience, he/she can always zoom-in to the specific model parts, and adapt them or use more specific data, to get more satisfying results.

6. Precursor analysis and examples

As mentioned, one of the primary development goals of our PSA modeling approach is to have flexible models that are suitable to perform efficient and large-scale precursor analysis of events at different PWRs and BWRs around the world. In this section, we will give a hands-on precursor analysis illustration and application using our models.

To start with, a precursor analysis can be seen as a mapping of the empirical event or sequence of events at some plant to its respective PSA model. Therefore, if an event occurred, its corresponding basic event probability in the PSA model is adapted accordingly (either set to failure, i.e. probability of one, or modified depending on the degree of degradation). Now the question that a precursor analysis is interested in answering is: *what is the probability of arriving to a core damage due to the deterministic occurrence of that specific event?,* i.e. it is a conditional probability of core damage. This "conditional probability" serves as an estimate of the remaining defense against core damage after the observed events/failures have occurred, and hence it can be used to rank the risks of operational events.

Precursors can be of two types [37], the first involves a degraded plant condition (failure or degradation of systems/components) without the occurrence of an initiating event, and the other involves an initiating event with or without degraded plant conditions. For the first type, the probabilities of the basic events affected by the condition are modified accordingly, and hence, the adjusted PSA will be calculating a conditional core damage frequency (CCDF). A conditional core damage probability (CCDP) is then calculated as $CCDP = 1 - e^{-CCDF*T}$, where T is the condition duration. This CCDP is now compared with the base-case (i.e. unconditional) core damage probability CDP_0, defined as $CDP_0 = 1 - e^{-CDF_0*T}$, CDF_0 being the nominal core damage frequency. Finally, the risk metric for the degraded plant condition, for a duration T, is the incremental increase in core damage probability $\Delta CDP = CCDP - CDP_0$. For the second type of precursors, one of the postulated initiating events has actually happened, in addition, there might be some degraded plant

conditions at the time of the initiating event. Therefore, for this type, the probability of the initiating event that has actually occurred is set to one, and all the other initiating events are set to zero. Additionally, the basic events affected by the condition are adjusted similar to the condition assessment case. The PSA model will now calculate a CCDP directly rather than a CCDF; this CCDP represents the risk metric for an initiating event precursor.

For events involving external initiators, the precursor analysis is done through capturing their manifested internal plant effects. For instance, if an earthquake led to some primary circuit pipe breaks (e.g. SBLOCA) and a failure of some equipment (e.g. EDGs), then the precursor risk is quantified by modelling a SBLOCA initiating event, and a concurrent EDG failure.

While performing the precursor analysis, plant design technicalities relevant to the event in hand are revisited and the respective models are adapted accordingly. Therefore, cross-tying, human intervention, and recovery possibilities will be credited whenever they are explicitly mentioned in the event under analysis. Furthermore, CCF basic event(s) of the affected system(s) are re-examined in case of CCF potential. Concretely, if, in a precursor, a component/train of a redundant system fails, and the remaining redundant components/trains had the potential to fail from the same cause, then Q_t in the Beta-factor model[6] [38] is set to one, hence the CCF contribution Q_n is $\beta . Q_t = \beta . 1 = \beta$.

To put some flesh on the concept, we hereby provide numerical examples of both precursor types. Note that our estimates tend to be fairly conservative as we generally do not account for systems recovery in the nominal case (as previously discussed).

Degraded plant condition precursor:

Take a precursor at a (W) PWR involving a non-recoverable one-month unavailability of a turbine driven auxiliary feedwater (TDAFW) pump. Assuming the AFW system of this plant consists of 1 turbine driven pump and 2 motor driven pumps, our PSA model of this precursor generates the CCDF uncertainty distribution shown in Fig. 6, with mean of 7.4 10^{-5}/year.

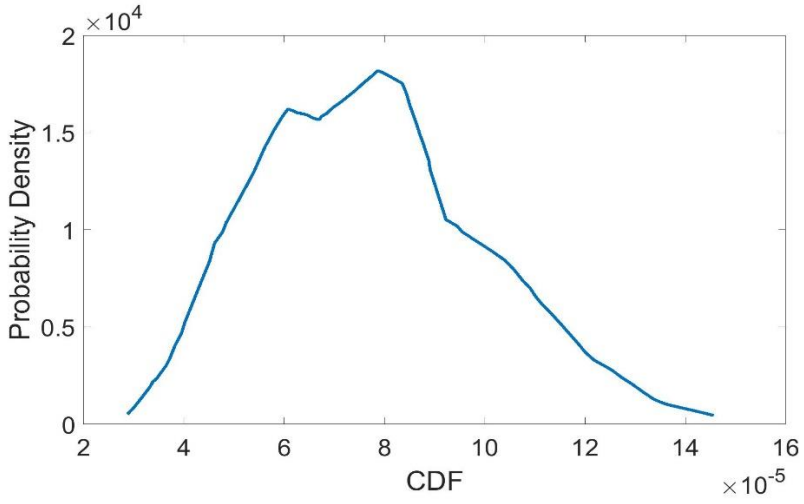


Fig. 6. CCDF distribution of a PWR (W) TDAFW pump unavailability event

[6] $\beta = \frac{Q_n}{Q_1 + Q_n} = \frac{Q_n}{Q_t}$, where Q_n is the CCF contribution (failure probability due to totally dependent failures), Q_1 is the component (i.e. train) failure probability due to independent causes, Q_t is the total failure probability of a component (i.e. train) both from independent and dependent causes.

$$CCDP \approx CCDF * T = \left(\frac{7.4\text{E}^{-5}}{\text{year}}\right)\frac{1\ month}{12\ \frac{months}{year}} = 6.1\ 10^{-6}.$$

The CDF_0 for a generic (W) PWR is 3.9 10^{-5} (Fig. 6), hence, $CDP_0 \approx CDF_0 * T = 3.2\ 10^{-6}$. Therefore, the incremental increase in core damage probability during the one-month exposure to this precursor is $\Delta CDP = 2.9\ 10^{-6}$, consequently, an incremental increase in large early release probability $\Delta LERP \sim 2.9\ 10^{-7}$ is expected.

Initiating event precursor:

Take a precursor at a GE BWR involving a LOOP and a failure of 1 out of 2 available EDGs – with recovery. Our PSA model of this precursor – for a generic BWR/4/5/6 production series – calculates the CCDP uncertainty distribution shown in Fig. 7, with mean CCDP of 1.3 10^{-3} (hence a conditional LERP ~ 1 10^{-4}).

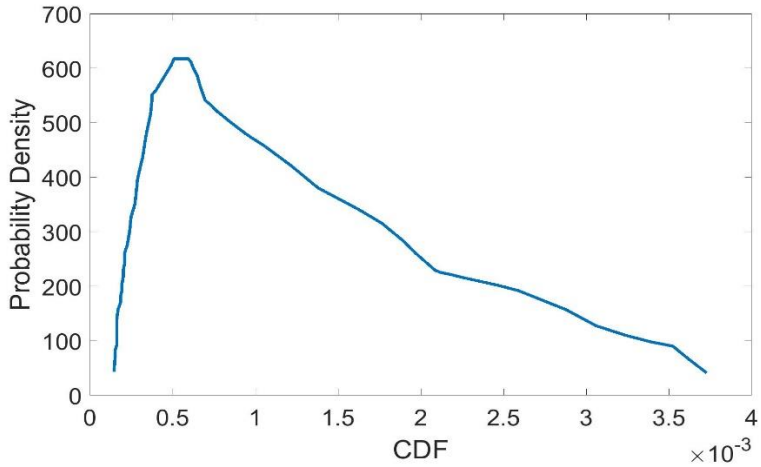


Fig. 7. CCDP distribution of a GE BWR LOOP event concurrent with an EDG unavailability

7. Conclusions and future work

In this work, we have presented the final results of our in-house generic PSA models for PWRs and BWRs. These models cover all common internal initiating events, with intermediate complexity generic event trees and fault trees capturing major design differences (redundancy, automation level, support dependence, etc.) without going to the details. This mentality of going simple and generic allowed for accounting for important lessons learnt from hundreds of precursors in our curated ETHZ Curated Nuclear Events Database [18], hence, supporting the quest for PSA completeness.

The developed models have attractive characteristics and are adaptable to account for plant-specific differences and new factors (EOC, T&M errors, Plant CCF, and others). Thanks to these characteristics, the models are foreseen to:

- Serve as a complementary framework that can aid plant-specific PSAs and answer big picture questions safety concerns.
- Provide an efficient platform for order-of-magnitude precursor analysis.
- Act as a fast first filter for precursors that can be used for initial screening and generic risk insights.
- Offer an unbiased framework – by annealing-out many plant-specific differences (as a result of going generic) – to compare precursors and risks at different plants, hence, help to learn and suggest cost-effective back-fits.

- Provide PSA models that could be used for different applications, when no access to plant-specific PSAs is provided (research institutes, universities, public, etc…).
- Help new comers and developing countries, serving as a starting point for their plant-specific PSAs as they are easy to understand and adapt.
- Support the PSA harmonization goal.

The models are now deployed for a large-scale precursor analysis for about 1000 worldwide safety-relevant events from our database. The unique outcome of this effort will be used to generate many empirical and statistical lessons, assess nuclear operational risks, and provide a framework for precursor's simulation and accident's prediction. It will help to observe developing minor failures over time to identify and monitor signals that may announce catastrophic collapse, and eventually develop active control and possible remedies through risk-informed decision-making.

Acknowledgement

The authors would like to acknowledge the continuous support provided by the Gösgen and the Leibstadt nuclear power plants in Switzerland throughout the project.

Appendix:

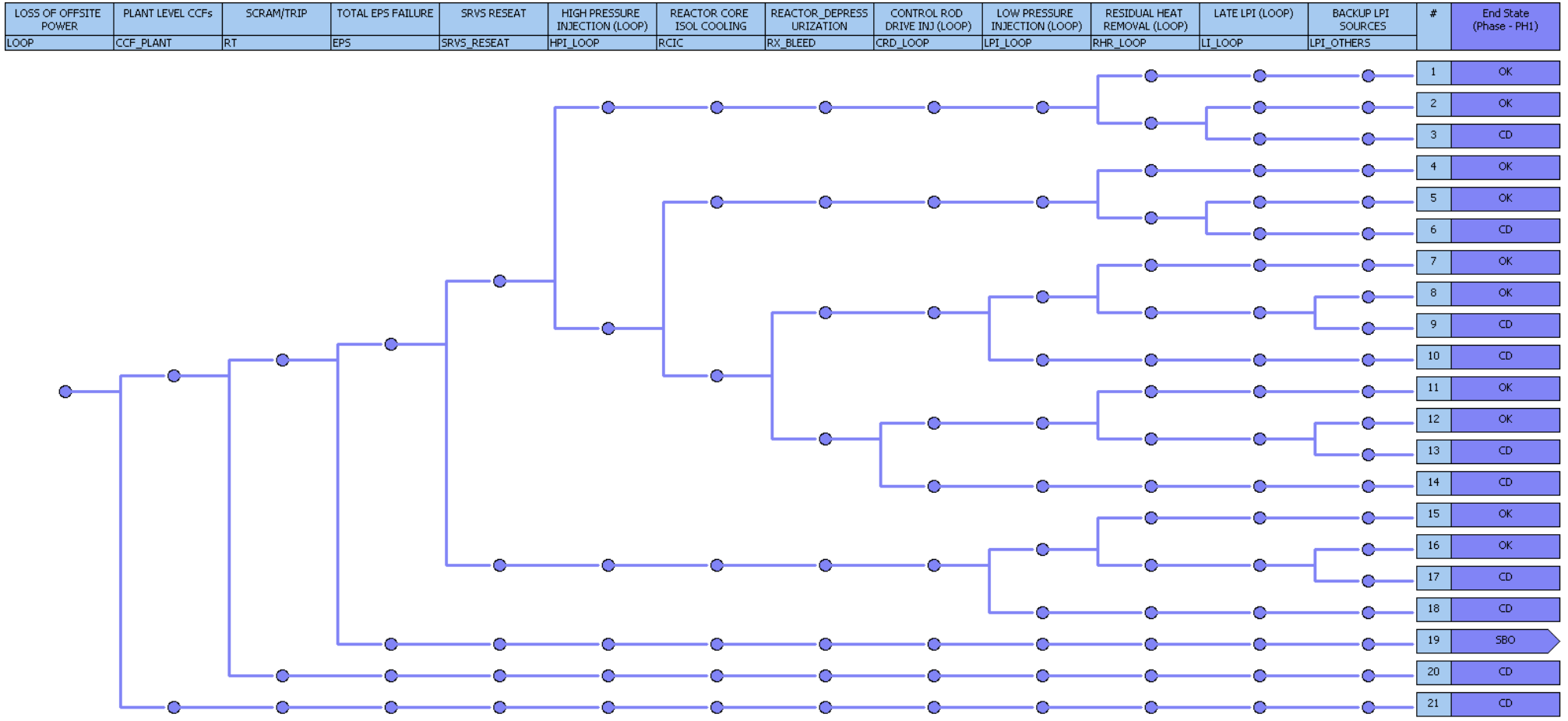


Fig. A.1. An example of a developed BWR LOOP event tree with two end-states: core damage (CD) and no core damage (OK)

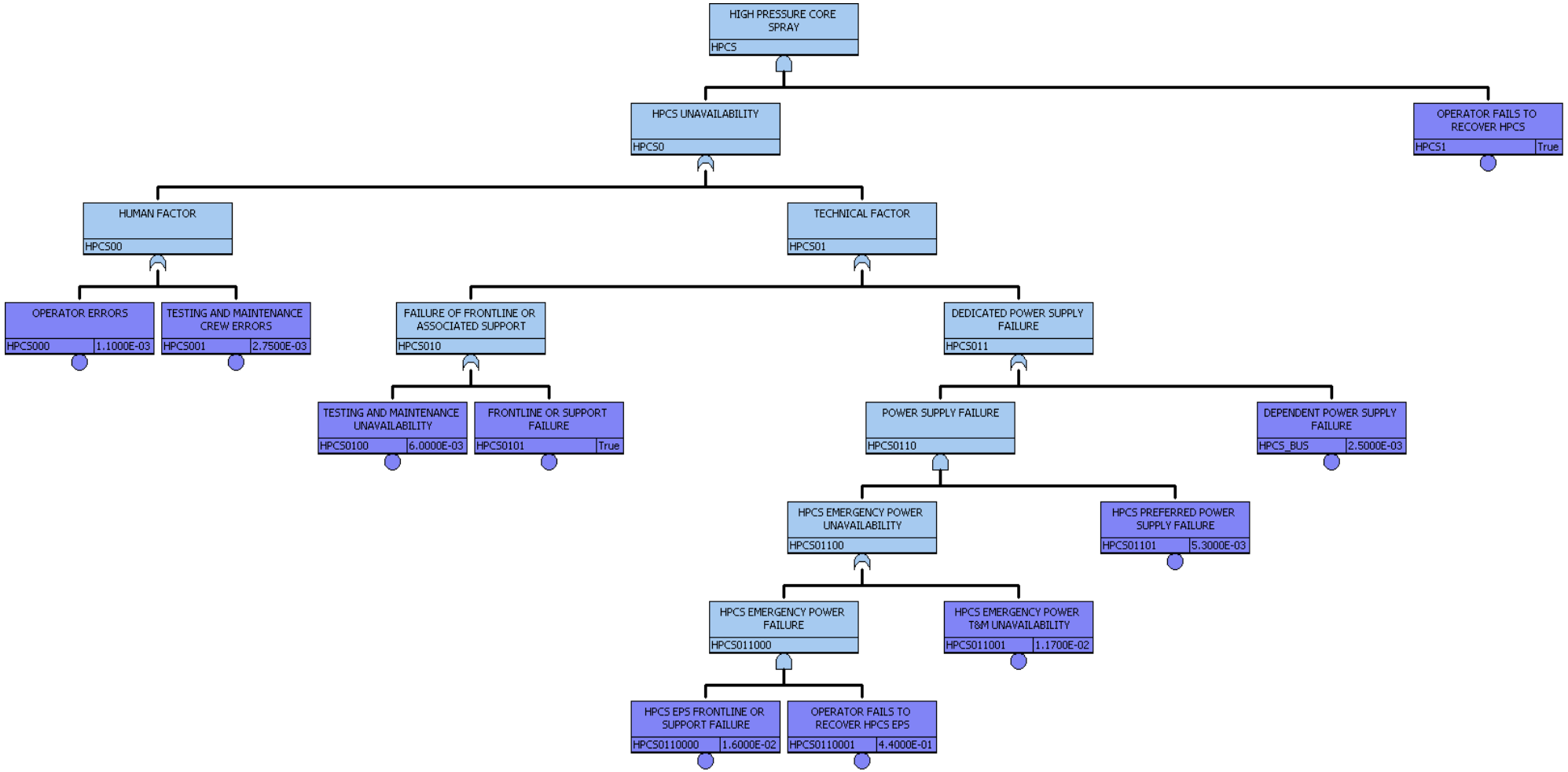


Fig. A.2. An example of a developed BWR high-pressure core spray fault tree

Table A.1. A sample of PWR basic events and their nominal values

Basic Event	**Nominal Value or Distribution**
Operator Fails to Trip the RCP Following Loss of Seal Cooling	Uniform ($2\ 10^{-2}$, $2\ 10^{-1}$) [31]
PORV Reseat Recovery Failure – Including Block Valves	Uniform ($5\ 10^{-3}$, $5\ 10^{-2}$) [31]
AFW CCF	Uniform ($1.8\ 10^{-4}$, $2.2\ 10^{-3}$)
Operator Fails to Actuate/Reconnect MFW	Uniform ($5\ 10^{-4}$, $5\ 10^{-3}$)*[31]
Operators Fail to Open Steam Dump Valves	Uniform ($2\ 10^{-4}$, $2\ 10^{-3}$)*[32]
HPIS CCF	Uniform ($1.4\ 10^{-4}$, $1.7\ 10^{-3}$)
LPIS CCF	Uniform ($1.4\ 10^{-4}$, $1.7\ 10^{-3}$)
Operator Fails to Actuate HPIS in F&B	Uniform ($2\ 10^{-3}$, $2\ 10^{-2}$) [31]
Operators Fails to Detect and Isolate Broken Steam Line	Uniform ($1\ 10^{-3}$, $1\ 10^{-2}$)*
Operators Fails to Detect and Isolate Ruptured Steam Generator	Uniform ($1\ 10^{-3}$, $1\ 10^{-2}$)*

*Experts opinion

Table A.2. A sample of BWR basic events and their nominal values

Basic Event	**Nominal Value or Distribution**
SRVs Fail to Reset	$1\ 10^{-3}$*
HPCI Frontline and Local Support Single Train UR	$5.1\ 10^{-2}$ [22]
RCIC Frontline and Local Support Single Train T&M UA	$1.1\ 10^{-2}$ [22]
ADS Failure	$3.7\ 10^{-3}$ [31]
Operator Fails to Manually Depressurize the Reactor	$7\ 10^{-1}$ [31]
Operator Fails to Align CRD	Uniform ($5\ 10^{-3}$, $5\ 10^{-2}$) [32]
LPCI CCF	Uniform ($1.4\ 10^{-4}$, $1.7\ 10^{-3}$)
Operators Fail to Align Alternative Low Pressure Injection Sources	Uniform ($3\ 10^{-3}$, $3\ 10^{-2}$)*[32]

*Experts opinion; ADS: Automatic Depressurization System

References

1. IAEA, *Probabilistic Safety Assessment*. 1992, Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY.
2. Sornette, D., Kröger, W., Wheatley, S., *New ways and needs for exploiting nuclear energy*. 2018: Springer.
3. Saleh, J., Saltmarsh, E., Favarò, F., Brevault, L., *Accident precursors, near misses, and warning signs: Critical review and formal definitions within the framework of Discrete Event Systems.* Reliability Engineering & System Safety, 2013. **114**: p. 148-154.
4. Hoertner, H., Kafka, P., Reichart, G., *The German precursor study—methodology and insights.* Reliability Engineering & System Safety, 1990. **27**(1): p. 53-76.
5. Minarick, J., *The US NRC accident sequence precursor program: Present methods and findings.* Reliability Engineering & System Safety, 1990. **27**(1): p. 23-51.
6. Ayoub, A., Kröger, W., Nusbaumer, O., Sornette, D. *Simplified/Harmonized PSA: A Generic Modeling Framework*. in *International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2019), Charleston, SC, USA*. 2019.
7. IAEA, *Probabilistic Safety Assessment: INSAG-6*, in *Safety series*. 1992: Vienna.
8. Epstein, S., Rauzy, A., *Standard model representation format for probabilistic safety assessment*. Technical report, The Open PSA Initiative, 2007-2008.
9. The Open PSA Initiative. *Retrieved from www.open-psa.org*. 2021.
10. Meléndez, E., Sánchez-Perea, M., Queral, C., Mula, J., Hernández, A., París, C. *Standardized Probabilistic Safety Assessment Models: First Results and Conclusions of a Feasibility Study*. in *13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), Seoul, Korea, 2-7 Oct*. 2016.
11. Hultkvist, G. *Common Methodology Descriptions for PSA. Retrieved from http://www.npsag.org/visa_info.asp?PostId=5&Avdelning=009&Sidrubrik=Presentation%20of%20PSA%20Results*.
12. Andersson, C., Authén, S., Holmberg, J.E. *User-friendliness and transparency in PSA modelling*. in *PSAM 10—International Probabilistic Safety Assessment & Management Conference, IAPSAM—International Association of Probabilistic Safety Assessment and Management. Seattle, Washington, USA. 7–11 June 2010*. 2010. Citeseer.
13. Friedlhuber, T., Hibti, M., Rauzy, A. *Variant management in a modular psa*. in *Proceedings of International Joint Conference PSAM*.
14. Ayoub, A., Kröger, W., Sornette, D. *Generic Probabilistic Safety Assessment Models for International Precursor Analysis Applications*. in *Proceedings of the International Youth Nuclear Congress (IYNC)*. 2020.
15. Smith, C.L., Wood, E., Knudsen, J., Ma, Z., *Overview of the SAPHIRE Probabilistic Risk Analysis Software*. 2016, Idaho National Lab.(INL), Idaho Falls, ID (United States).
16. Ayoub, A., Stankovski, A., Wheatley, S., Kröger, W., Sornette, D. *ETHZ Curated Nuclear Events Database*. 2020; Available from: http://er-nucleardb.ethz.ch/.
17. Ayoub, A., Stankovski, A., Kröger, W., Sornette, D., *The ETH Zurich curated nuclear events database: Layout, event classification, and analysis of contributing factors.* Reliability Engineering & System Safety, 2021. **213**: p. 107781.
18. Ayoub, A., Stankovski, A., Kröger, W., Sornette, D., *Precursors and startling lessons: Statistical analysis of 1250 events with safety significance from the civil nuclear sector.* Reliability Engineering & System Safety, 2021: p. 107820.
19. Okrent, D., Guarro, S., *Reflections on the study of precursors to potential severe core damage accidents.* Nuclear Safety, 1983. **24**(6): p. 836-850.
20. Keller, W., Modarres, M., *A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen.* Reliability Engineering & System Safety, 2005. **89**(3): p. 271-285.
21. Kim, J.S., Kim, M.C., *Consistency issues in quantitative safety goals of nuclear power plants in Korea.* Nuclear Engineering and Technology, 2019. **51**(7): p. 1758-1764.

22. Eide, S.A., Wierman, T.E., Gentillon, C.D., Rasmuson, D.M., Atwood, C.L., *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, U.S. Nuclear Regulatory Commission, NUREG/CR-6928, January 2007.* .
23. Joe, J.C., Shirley, R.B., Mandelli, D., Boring, R.L., Smith, C.L., *The development of dynamic human reliability analysis simulations for inclusion in risk informed safety margin characterization frameworks.* Procedia Manufacturing, 2015. **3**: p. 1305-1311.
24. Dougherty, E., *Technical Note, Human Errors of Commission Revisited: an Evaluation of the ATHEANA Approach.* Reliability Engineering and System Safety, 1998. **60**: p. 71-82.
25. Swain, A.D., Guttmann, H.E., *Handbook of human-reliability analysis with emphasis on nuclear power plant applications. Final report*. 1983, Sandia National Labs.
26. Belles, R.J., Cletcher, J.W., Copinger, D.A., Dolan, B.W., Minarick, J.W., Muhlheim, M.D., Oreilly, P.D., Weerakkody, S., Hamzehee, H., *Precursors to potential severe core damage accidents: 1997, A status report.* NUREG/CR, 1998. **4674**: p. 157.
27. Van der Borst, M., Schoonakker, H., *An overview of PSA importance measures.* Reliability Engineering & System Safety, 2001. **72**(3): p. 241-245.
28. Hirschberg, S., Parry, G.W., Carlsson, L., Mankamo, T., Mosleh, A., Vesely, W.E., *Procedures for conducting common cause failure analysis in probabilistic safety assessment.* Vienna: IAEA, 1992.
29. Chatri, H., Johanson, G., Wood, J., Akl, Y. *Recent Insights from the International Common Cause Failure Data Exchange (ICDE) Project*. in *30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15)*. 2020.
30. Čepin, M., *Probability of restoring power to the transmission power system and the time to restore power.* Reliability Engineering & System Safety, 2020. **193**: p. 106595.
31. Forester, J.A., Mitchell, D.B., Whitehead, D.W., *Precursors to potential severe core damage accidents. A status report, 1982--1983*. 1997, Nuclear Regulatory Commission, Washington, DC (United States).
32. Cox, D.F., Cletcher, J.W., Copinger, D.A., Cross-Dial, A.E., Morris, R.H., Vanden Heuvel, L.N., Dolan, B.W., Jansen, J.M., Minarick, J.W., Lau, W., *Precursors to potential severe core damage accidents: 1992, A status report. Volume 17, Main report and Appendix A*. 1993, Nuclear Regulatory Commission, Washington, DC (United States).
33. USNRC, *Severe Accident Risks: An Assessment of Five US Commercial Nuclear Power Plants.* NUREG-1150, 1989.
34. Werner, W.F., Hirano, M., Kondo, S., Johanson, G., Lanore, J.M., Murphy, J.A., Schmocker, U., *Results and insights from level-1 probabilistic safety assessments for nuclear power plants in France, Germany, Japan, Sweden, Switzerland and the United States.* Reliability Engineering & System Safety, 1995. **48**(3): p. 165-179.
35. Watanabe, H., Sancaktar, S., Dennis, S., *Generic PWR PRA Model (ML19008A133)*. 2018.
36. Turski, E., Sancaktar, S., Dennis, S., *Generic BWR PRA Model (ML19008A134)*. 2018.
37. Johnson, J.W., Rasmuson, D.M., *The US NRC's accident sequence precursor program: an overview and development of a Bayesian approach to estimate core damage frequency using precursor information.* Reliability Engineering & System Safety, 1996. **53**(2): p. 205-216.
38. Borcsok, J., Schaefer, S., Ugljesa, E. *Estimation and evaluation of common cause failures*. in *Second International Conference on Systems (ICONS'07)*. 2007. IEEE.

Chapter 5

Comprehensive quantitative large-scale assessment of nuclear power risks

How much should nuclear contribute to the energy portfolio needed to ensure a sustainable Earth environment for mankind? With the threats of global climate change and the emphasis on clean energy, nuclear opponents prominently raise the spectre of nuclear catastrophes. However, the dread of nuclear, often associated with singular catastrophic events such as Chernobyl or Fukushima and amplified by nuclear weapons terror, has limited quantitative scientific foundation, given the paucity of data. Here, we fill this gap by offering the first comprehensive statistical study of the operational risks in the civil nuclear sector. Using what is by far the largest recently constructed open database on accident precursors, and using our in-house generic probabilistic safety analysis (PSA) models for precursor analyses, we provide the first quantification of the severity of precursors to nuclear plant core damage, which takes the universal shape of a Pareto distribution. We also identify a special runaway Dragon Kings regime beyond the Pareto domain for the largest events. With respect to risk assessment, our main finding is that risk is dominated by exogenous factors (95%). We calculate that, by focusing on these factors, the frequency of accidents of the Fukushima scale can be brought down to about $6\ 10^{-6}$ *per reactor-year (less than one severe radioactive release per 300 years of operation of the whole nuclear fleet). Our results also demonstrate the need for a global international cooperation focused on the construction of full blockchains of the cascades of accident precursors in order to create an even safer civil nuclear industry.*

Based on **Ayoub, A.** & Sornette, D. (2021). Comprehensive quantitative large-scale assessment of nuclear power risks. *Nature Energy.* Under Review.

1. Introduction

Large scale disasters, whether in natural or complex technical systems, are rare, which makes the statistical estimation of their risks unreliable or even biased [1]. Realizing that the much more numerous smaller accidents and incidents shed light on their larger siblings, it has been proposed that their use can provide a better risk assessment and firmer estimates of accident probabilities [2]. Similar to natural catastrophes, a power law frequency-severity relationship is expected – yet needs to be empirically tested using a suitable measure for severity.

The use of operating experience and near-accident data has progressively gained popularity in critical industries. Khakzad et al. [3] used accident precursor data and hierarchical Bayesian models to analyse the risks of offshore blowouts. Shengli Liu and Yongtu Liang [4] applied extreme value theory on a database containing records of hazardous liquid pipeline incident and accidents to model the tail behaviour of extreme events and their expected probabilities. In the nuclear industry, the US Nuclear Regulatory Commission started the Accident Sequence Precursor Program to analyse accidents precursors, suggest risk focus areas, and estimate core damage frequencies [5]. Lina Escobar Rangel and François Lévêque [6] used a time-varying mean Poisson model on a small dataset of events rated with the International Nuclear and Radiological Event Scale (INES), to estimate the frequency of core meltdown before and after Fukushima. Wheatley et al. [7] performed a statistical analysis of nuclear

operational risks using a dataset of 170+ incidents and accidents, with cost and radiation as severity labels. These developments have been all hindered by the small size of available data sets.

Continuing in the same direction and seeking a more comprehensive and technical nuclear risk assessment, with collaborators, we have compiled a database of around 1250 events (accidents, precursors, and important incidents) from the global civil nuclear fleet and spanning the long operational history of the human nuclear era [8, 9] Each event was systematically analysed by multiple nuclear-safety experts, and was labelled with many descriptive features and risk annotations. With a dataset of this scale, we are now in a unique position to empirically quantify the frequency of core damage (CD) and large release (LR) of radioactive substance, and get good estimates of nuclear accidents occurrence rates.

Even though it can be tricky to investigate the overall risk of a heterogeneous fleet (different plant designs and reactor technologies), the approach is valid as long as one does not draw inference beyond an "average reactor". To validate this procedure, we have also developed our own generic and adaptive PSA models for pressurized and boiling water reactors (PWRs and BWRs) [10] that allow us to quantify precursors' risk with the same ruler, remove assessment biases, and get rid of plant-specific PSA differences and scope gaps. We have utilized these models to perform a first-of-a-kind large scale precursor analysis of all PWR and BWR events in our database (~900 events), calculating how far is an event from developing to an accident, i.e. we calculate the probability $P(CD|p_i)$ of core damage or $P(LR|p_i)$ of large release for every precursor p_i.

We demonstrate that the frequency vs severity plot for precursors follow a perfect Pareto distribution (using the INES scores, being an approximate logarithmic measures of costs or of release), and identify a clear runaway Dragon King regime [11] with the two infamous disasters (Chernobyl and Fukushima). Moreover, we show that the severity distribution (using precursor analysis measures) appears to have changed following the Three Mile Island (TMI) accident, shifting to a lighter Pareto tail, nevertheless, with exogenously-born Dragon Kings living beyond, and fitting within the pre-TMI risk profile. Furthermore, core damage and large release frequencies (CDF and LRF) are estimated for the whole operational history, as well as for the current fleet, using different empirical estimators. Interestingly, the precursor-based estimators validated our PSA results for internal initiators.

Finally, facing the question of what should be the optimal energy portfolio for the clean production of energy, and realizing the many advantages that nuclear power can have [12, 13], we argue that the nuclear industry still has the opportunity to regain public trust, and play an important role in a clean energy mix if it managed to tame its risks convincingly. Our analysis confirms that risks can be brought down by 95%, with $\widehat{LRF} \approx 6\ 10^{-6}\ per\ ry$ (reactor-year), if the industry is made to focus on addressing exogeneities (dominating the risk). This calls for a global cooperation and establishment of an international risk register, namely, an accident precursors-blockchain.

2. Runaway disasters

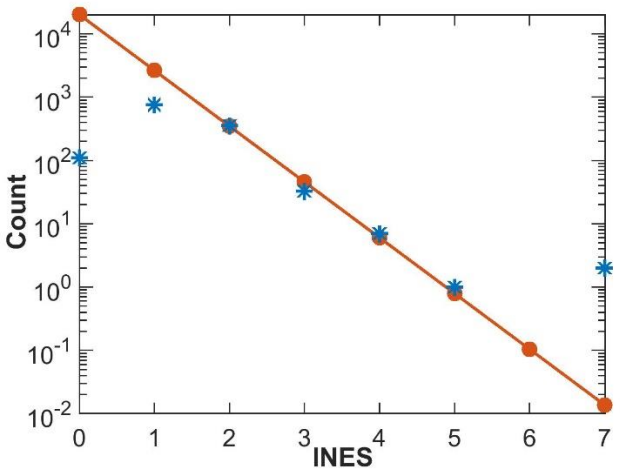
We base our first quantitative study on our recently introduced Core-Only INES score [8] to assess the severity of an event from a core damage engineering point of view, in contrast to the standard IAEA INES ratings where the focus is radiation exposure [14]. The Core-Only INES score is given per event rather than per reactor unit, i.e. if an event affected a multi-unit site, it still gets a single Core-Only INES rating.

INES 0 events have no core safety relevance, INES 1 represent minor anomalies, INES 2 and 3 correspond to incidents with serious core relevance, INES 4 is given for events which witnessed local fuel damage, INES 5 is for core damage events, INES 6 and 7 cover events beyond core damage —

having significant large releases and widespread effects. Applying this approach to our database gives a dataset of 1256 systematic Core-Only INES rated events distributed as shown in Fig. 1.

INES	Count	INES 2-5 fit: $f = Cp^{INES}$
0	109	20077
1	750	2642
2	354	348
3	33	45.7
4	7	6.02
5	1	0.8
6	0	0.1
7	2	0.013

(a)



(b)

Fig. 1 | The distribution of Core-Only INES scores. In (a), from left to right, are the INES ratings, the count (number) of events in our database associated with every INES, and the best fit INES counts given by $f = Cp^{INES}$ with C = 20077, and p = 0.13. In (b), the blue stars * are the empirical INES counts given in the second column of table (a), the solid orange line is the exponential fit to the INES counts, and the orange dots are the values for the exponential fit at each INES value.

The INES count distribution is well described by the exponential distribution for values between 2 to 5 (following a perfect straight line in a linear-log plot). One can observe a deviation for INES values 0 and 1, easily explained by and expected from censorship (i.e., missing events in our catalogue). Indeed, many INES 0 and 1 are missing in the dataset since the utilized ETHZ database is mainly concerned with events of safety relevance and potential core damage precursors. Since the INES scale is constructed as a logarithmic measure of severity (each increase in score reflects an order of magnitude increase in severity [14]), the exponential fit corresponds to a Pareto (power law) distribution in severity. Furthermore, the two most severe accidents in the nuclear history having an INES 7 rating (Chernobyl and Fukushima) lay above the extrapolation of the estimated exponential (Pareto) distribution by more than two orders of magnitude. These outlying events are “Dragon Kings” [15, 11] , in the sense that they are not generated by the same process as their smaller siblings, and tend to be more frequent than predicted by extrapolation. Intuitively, this can be associated with the fact that, once an event surpasses a certain threshold (overcoming a number of safety barriers in a complex system), it can become uncontrollable, causing disproportionately more damage than typical events. Interestingly, the fitted exponential law predicts the occurrence of serious INES 4 events and even INES 5 core damage accidents, suggesting that a core damage event of the TMI scale is not so special and can be expected to happen typically once within the observations’ history, i.e. in around 60 years of civil nuclear operation and with all 600+ ever operated reactors.

3. A change of regime in the risk profile after TMI

To further quantify risks, we use our calculated precursor severity measures for PWR and BWR events (a total of 901 entries) [8-10]. Every event is given a conditional core damage probability (CCDP) value or a measure of the change in CDP (ΔCDP) depending on whether it contained an initiating event or not, respectively. We divide the precursors into pre- and post- TMI events to study if a change in the

risk profile can be detected due to the post-TMI industry response, which is known to have involved a total investment of more than 100 billion USD in worldwide nuclear plants retrofitting [15]. Fig. 2 shows the empirical complementary cumulative distribution functions (CCDFs) of the CCDP/ΔCDP variable for both time periods. For values of CCDP/ΔCDP larger than $\sim 10^{-4}$, the CCDFs exhibit Pareto tails, with different exponents but both smaller than 1, implying that extremes dominate average measures of risks [16]. The post-TMI industry response seems to have had the effect of reducing risks in the body of the distribution, i.e. as a whole. This change is quantified by a larger power law exponent (≈0.76) compared with that of the pre-TMI distribution (≈0.55). However, for the largest CCDP/ΔCDP values, the pre- and post-TMI distributions become undistinguishable. From the view point of the reduced exponent of the post-TMI power law distribution, the largest CCDP/ΔCDP values correspond to outliers. This is in line with the often reported observation that the obsessive attitude in the control of complex technical systems of trying to suppress small events can actually backfire, either by increasing the risk of extreme events [11, 17] or not modifying them while contributing to complacency. A remarkable fact is that all these outlying post-TMI events are born from a similar origin and are usually associated with exogenous factors and hazards (they include the multi-site Fukushima Tohoku Earthquake events – 2011, multi-unit Kola tornado – 1993, Armenian plant fire – 1982).

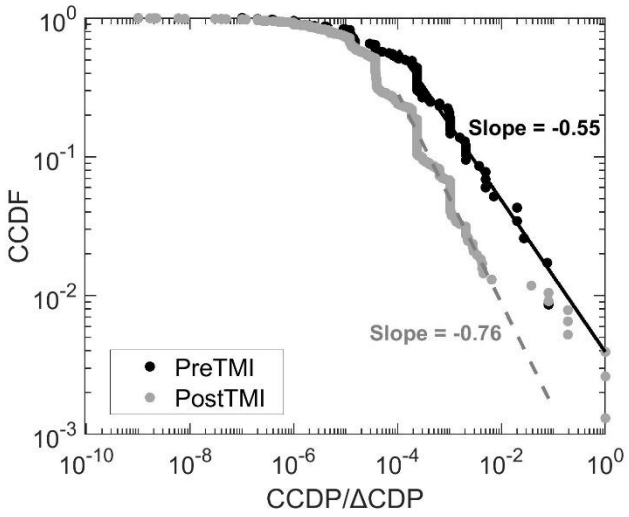


Fig. 2 | The distribution of precursors' severity. The precursors' severity measures (CCDP/ΔCDPs) are plotted according to their CCDFs for the pre- and post- TMI periods (in black and grey respectively). The solid black and the dashed grey lines are the linear fits of the pre- and post- TMI tails, estimating the slopes, i.e. parameter $-\alpha$ of a Pareto CCDF given by $F(S) = (S/S_{min})^{-\alpha}$, where S is the severity measure (e.g. CCDP/ΔCDPs).

4. The frequency of nuclear accidents

Given the nature of nuclear accidents, it is a reasonable assumption that their temporal distribution follows a stationary Poisson process, i.e. there is no dependence between successive accidents, and the distribution of waiting times between one and the next is exponential with rate λ. The sufficient statistics (best estimator) for λ is given by $\frac{n}{T}$, where n is the number of observed accidents and T is the total observation period. With 19,000 operational reactor-years (ry) and 5 severe core damage accidents (three at Fukushima, 1 at TMI, and 1 at Chernobyl), one can estimate a $\widehat{CDF} \approx 2.6\ 10^{-4}\ per\ ry$. Although this estimate is mathematically valid, it is known to be not so accurate [1, 18] (small sample and large variance) and does not allow for the study of crucial details such as the performance over time [19]. Moreover, major accidents occurred in reactors that do not represent the

current fleet (Chernobyl's RBMKs), and have shown to be outlying with respect to the expected operational experience (Fig. 1).

Different schemes are needed to assess the empirical nuclear risks using more robust estimators based on operational experience and accident precursors data from the global fleet.

4.1. INES-based estimator:

The INES model discussed above can also be used to estimate nuclear operational risk. However, a mapping is first needed to link the qualitative INES scores to the risk measures of interest, CDF and LRF. INES 5 and above can be a good proxy for core damage events in the classical meaning (INES 4 ratings are given for events with local fuel damage/melt). Moreover, INES 6 and 7 cover events beyond core damage — having significant large releases and widespread effects, therefore, can be used to estimate LRF.

Each INES count represents the mean occurrence of such event over all nuclear plants and throughout the plants' operational history (i.e. rates of independent Poisson random variables). Therefore, with around 10k plant.years:

$\widehat{CDF} \approx \frac{1}{10k\ plant.years} \sum_{INES=5}^{7} Cp^{INES}$; with $C = 20077\ and\ p = 0.13$ as shown in Fig. 1.

giving $\widehat{CDF} \approx 9\ 10^{-5}/plant.years$. Similarly LRF can be estimated using INES 6 and 7 rates, $\widehat{LRF} \approx 10^{-5}/plant.years$. Note that the fitted exponential model eliminates the effect of the Dragon Kings by construction.

4.2. Precursor-based estimators:

Using the law of total probability, for a set of N pairwise disjoint and exhaustive precursors $\{p_i : i = 1,2,3, \dots N\}$, the expected number of core damages observed at all operating reactors is given by [20-22]:

$$\widehat{E[CD]} = \widehat{CDF} = \sum_{i=1}^{N} P(CD|\,p_i) * frequency\ (p_i) \quad (1)$$

The sum in equation (1) requires the knowledge of a mathematically exhaustive set of precursors, which is not possible in practice. However, one can still obtain a good estimate using a representative set of precursors $\boldsymbol{S}$ satisfying the following properties:

1- $\boldsymbol{S}$ must contain the most important and safety significant events (i.e. events having high $P(CD|p_i)$ – dominating the sum),
2- $\boldsymbol{S}$ must be large and unbiased by construction, so that the frequency of a certain precursor can be well approximated by its number of occurrence within $\boldsymbol{S}$, in T reactor-years.

Equation (1) can then be approximated as:

$$\widehat{CDF} \approx \frac{1}{T} \sum_{\boldsymbol{S}} P(CD|\,p_i) \quad (2)$$

The ETHZ nuclear events database satisfies the above two properties. The conditional probabilities $P(CD|p_i)$ of its ~900 LWR precursors are estimated using the generic PSA models [10]. $\widehat{LRFs}$ are estimated using the same formula, and the results for both estimators with $T = 14{,}500$ LWR-years are shown in Table 1.

Table 1 | Empirical CDF and LRF precursor-based estimates

	From internal events only	Total	w/o Fukushima Daiichi
$\widehat{CDF}\ (per\ ry)$	9.8 10^{-5} (7.8 10^{-5}, 1.5 10^{-4})	3.6 10^{-4} (3 10^{-4}, 5.2 10^{-4})	1.5 10^{-4} (9.6 10^{-5}, 3.1 10^{-4})
$\widehat{LRF}\ (per\ ry)$	9.8 10^{-6} (3.2 10^{-6}, 2.9 10^{-5})	2.2 10^{-4} (2.1 10^{-4}, 2.5 10^{-4})	1.5 10^{-5} (5 10^{-6}, 4.5 10^{-5})

The first column shows the CDF and LRF estimates based on internally triggered precursors only – similar to the logic of internal-events CDF calculations in PSA. The second column shows the total CDF and LRF estimates (from both internal and external triggers). The third column shows the total CDF and LRF estimates without Fukushima Daiichi's contribution. The values in parenthesis represent the 5th and the 95th percentiles of the estimates, calculated from the uncertainties in each $P(CD|p_i)$ calculation due to the PSA parameters and basic events uncertainties (using large Latin hypercube samples).

Without the contribution of the Fukushima Daiichi accident, the precursor-based estimates of CDF and LRF are very close to the INES-based estimates which exclude the effect of the Dragon Kings in its exponential fit, even though the two methods are independent and use totally different risk metrics, different ensemble, and different estimation techniques.

The estimates in table 1 are static and aggregate the whole experience in one number, hence, information about local temporal behaviours are lost. Therefore, the same calculation approach can be used to construct their temporal evolution as shown in the main frames of Fig. 3a,b (solid black line) along with its 90% uncertainty bounds (dashed black lines). Low $\widehat{CDF}$ ($\widehat{LRF}$) values in the first years can be explained by censorship and limited reporting during the early phase of nuclear operation. The remarkable increase between 1975-1980 captures serious precursors (Browns Ferry-1 fire of 1975, and Rancho Seco steam generator dry-out in 1978), and the TMI-2 1979 core meltdown. After TMI, the steady decreasing trend with almost one order of magnitude drop can be explained by the industry retrofitting response and the famous "TMI Action Plan". The Tohoku Earthquake associated events (3 core meltdowns and 3 precursors at the Fukushima Daiichi and Daini nuclear plants respectively) are at the origin of the large $\widehat{CDF}$ ($\widehat{LRF}$) jump in 2011. The dashed red lines in both main frames show the evolution of the remaining $\widehat{CDF}$($\widehat{LRF}$) after taking out the beyond-design Fukushima Daiichi's contribution (yet conservatively keeping Daini's).

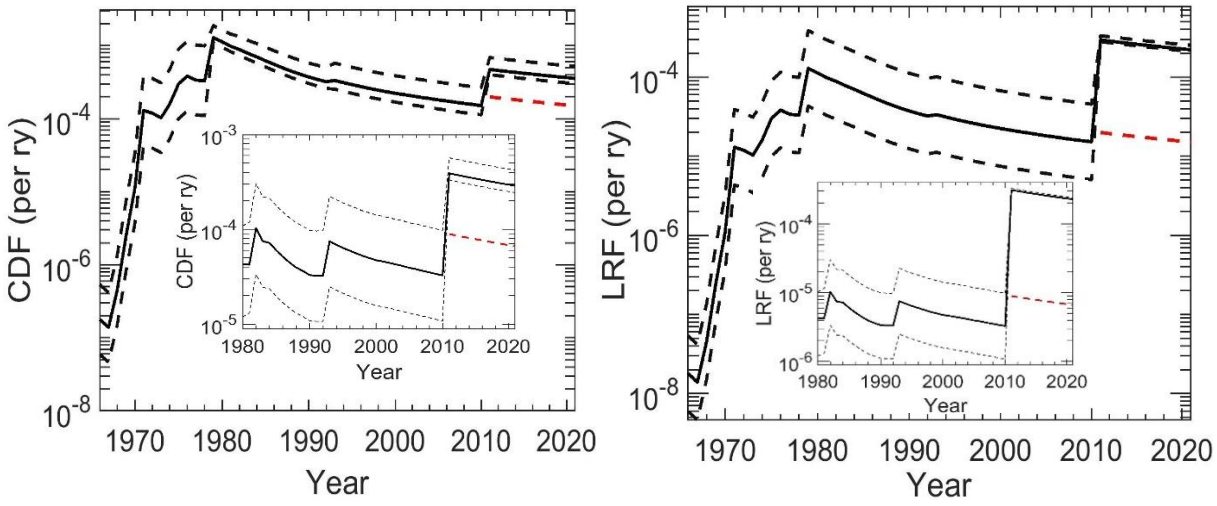


Fig. 3 | Running $\boldsymbol{CDF}$ and $\boldsymbol{LRF}$ estimates. In (a), the main frame shows the temporal evolution of $\widehat{CDF}$ (solid black line) along with its 90% uncertainty bound (dashed black lines) calculated using thousands of Latin hypercube samples of the PSA uncertain parameters. The inset shows the running rate estimates from 1980 onwards (post-TMI) with its 90% uncertainty bound (dashed black lines). The dashed red line in both the main and the inset frame show the results without Fukushima Daiichi's contribution. In (b), the same analysis and results are shown for $\widehat{LRF}$.

To have a more accurate estimation of the operational risks of the current fleet, with incorporated backfits, generational updates (Gen II, II+ reactors, and newer), and removing the effect of early days' censorship, we perform a new calculation starting at TMI as year 0 and running forward. The results are shown in the lower inset of Fig. 3 (solid black line) along with the 90% uncertainty bounds (dashed black lines), calculating an aggregate $\widehat{CDF} \approx 2.8\ 10^{-4}\ per\ ry$ by 2021, with $(2.4\ 10^{-4}, 4.2\ 10^{-4})$ 90% uncertainty band. Here again, removing the Fukushima Daiichi's contribution will lead to lower estimates (dashed red line in the inset figures), with a $\widehat{CDF}$ and $\widehat{LRF}$ of about $6.6\ 10^{-5}\ per\ ry$ $(2.2\ 10^{-5}, 2\ 10^{-4})$ and $6.6\ 10^{-6}\ per\ ry$ $(2.2\ 10^{-6}, 2\ 10^{-5})$ by 2021 respectively.

5. Conclusions and policy implications

The records of operational experience and the occurrence of near misses are not only frustrating occurrences, but are opportunities to learn the vulnerabilities of a system. In this study, the risk of nuclear power was assessed using the largest available open database on accident precursors. The empirical frequency of core damage and large release are estimated to be around $2\ 10^{-4}\ per\ ry$ for the current fleet, i.e. for a fleet of 450+ reactors, an accident of the Fukushima-scale is expected to happen every 11 years! This scary estimate is in complete disagreement with theoretical PSA results – stating CDF estimates of the current fleet in the order of $10^{-5}\ per\ ry$ [15, 23], and even lower for LRFs [24]. What should be expected instead is that the results of precursor analyses and precursor-based estimates should serve as a good benchmark for PSA completeness and fidelity. This fact is mathematically demonstrated in equation (1), suggesting that for a sufficiently large and representative sample of precursors, and for a given PSA model used in the precursor analyses, the precursor-based CDF/LRF estimates should converge to their respective PSA-calculated quantities. As a testimony of this fact, the CDF and LRF estimates of our generic PSA models covering only internal events [10] were quantitatively retrieved through the "internal events only" precursor-based

estimates shown in the first column of Table 1 (in the range of 10^{-5} and 10^{-6} $per\ ry$ for $\widehat{CDF}$ and $\widehat{LRF}$ respectively). These results serve both as a sanity check for the quality of our PSA models, as well as an explanation for the reasons behind the realized discrepancy between typical industrial PSA results and the empirical estimates. The results suggest that external events seem not to be well taken into account in the current PSAs (potential of underestimation), hence causing the observed inconsistency between theoretical (underestimated) and empirical estimates.

Furthermore, we have shown that nuclear risk is driven by exogenous factors giving birth to Dragon King extremes. Our analysis suggests that the nuclear industry can tame risks and regain public trust if it focuses its efforts to address and prepare for these exogeneities and learn from previous mistakes; the risks can be brought down by 95%!, with $\widehat{LRF} \approx 6\ 10^{-6}\ per\ ry$.

In conclusion, our results demonstrate the value of large open database from which essential lessons can be learned from recording and sharing of nuclear operational experience. We call for a global cooperation and the establishment of an international risk register, accident precursors-blockchain, where every plant reports all its precursors and operating events, and all the blockchain participants (nuclear power plants, regulators, concerned international organizations, concerned scientists) have access to this data. With more data, analysis by country, reactor class, technology, or vendor will become possible. The blockchain should address the issue of incentives (or penalties) for sharing (or concealment). Nevertheless, the main incentive should remain that all parties can learn from each others' experience, and avoid repeating mistakes, at a time where the industry can fly as a whole or fall as a whole. This call is not nuclear specific, but should be expanded to all critical industries.

Methods

Data description. This analysis utilizes The ETHZ Curated Nuclear Events Database [25], which contains events compiled from multisource data from the operational experience of civil nuclear power plants. The main source of data (events) are annual reports from national nuclear regulators. Other sources include published IAEA INES events, operating experience databases, open access official reports, academic publications, and serious newspaper articles. All events have a reference.

Data availability

The ETHZ Curated Nuclear Events Database can be accessed and downloaded from http://er-nucleardb.ethz.ch/. For reactor year's calculations, we relied on the IAEA PRIS data (https://pris.iaea.org/pris/) and have our calculation files in the supplementary information.

Code availability

All the SAPHIRE PSA models that were used to calculate the CCDP and the ΔCDP values for the 901 LWR events can be found at Mendeley Data (http://dx.doi.org/10.17632/y9wfgyk6nz.1#folder-d062efaf-c881-46aa-b7c1-73be535bf5c0).

Acknowledgements

The authors would like to thank Prof. Dr. Wolfgang Kröger for all the interesting discussions and comments throughout the project. The authors would also like to thank Keyi Ma for the support in some background calculations.

Competing Interests statement

The author declares no competing interests.

References

1. Şengör, A., *Evaluating nuclear accidents.* Nature, 1988. **335**(6189): p. 391-391.
2. Hsü, K., *Nuclear risk evaluation.* Nature, 1987. **328**(6125): p. 22-22.
3. Khakzad, N., Khan, F., Paltrinieri, N., *On the application of near accident data to risk analysis of major accidents.* Reliability Engineering & System Safety, 2014. **126**: p. 116-125.
4. Liu, S., Liang, Y., *Statistics of catastrophic hazardous liquid pipeline accidents.* Reliability Engineering & System Safety, 2021. **208**: p. 107389.
5. Johnson, J.W., Rasmuson, D.M., *The US NRC's accident sequence precursor program: an overview and development of a Bayesian approach to estimate core damage frequency using precursor information.* Reliability Engineering & System Safety, 1996. **53**(2): p. 205-216.
6. Rangel, L.E., Lévêque, F., *How Fukushima Dai-ichi core meltdown changed the probability of nuclear accidents?* Safety Science, 2014. **64**: p. 90-98.
7. Wheatley, S., Sovacool, B., Sornette, D., *Of disasters and dragon kings: a statistical analysis of nuclear power incidents and accidents.* Risk analysis, 2017. **37**(1): p. 99-115.
8. Ayoub, A., Stankovski, A., Kröger, W., Sornette, D., *The ETH Zurich curated nuclear events database: Layout, event classification, and analysis of contributing factors.* Reliability Engineering & System Safety, 2021. **213**: p. 107781.
9. Ayoub, A., Stankovski, A., Kröger, W., Sornette, D., *Precursors and startling lessons: Statistical analysis of 1250 events with safety significance from the civil nuclear sector.* Reliability Engineering & System Safety, 2021: p. 107820.
10. Ayoub, A., Kröger, W., Sornette, D., *Generic and adaptive probabilistic safety assessment models: Precursor analysis and multi-purpose utilization.* Nuclear Engineering and Technology. Under Review, 2021.
11. Sornette, D., Ouillon, G., *Dragon-kings: Mechanisms, statistical methods and empirical evidence.* The European Physical Journal Special Topics, 2012. **205**(1): p. 1-26.
12. Huang, L., Liu, Y., *Balanced news for long-term growth.* Nature Energy, 2020. **5**(7): p. 500-501.
13. Severnini, E., *Impacts of nuclear plant shutdown on coal-fired power generation and infant health in the Tennessee Valley in the 1980s.* Nature Energy, 2017. **2**(4): p. 1-9.
14. *INTERNATIONAL ATOMIC ENERGY AGENCY, INES: The International Nuclear and Radiological Event Scale User's Manual*. 2013, Vienna: IAEA.
15. Sornette, D., Kröger, W., Wheatley, S., *New ways and needs for exploiting nuclear energy*. 2018: Springer, Heidelberg.
16. Sornette, D., *Critical phenomena in natural sciences: chaos, fractals, selforganization and disorder: concepts and tools*. 2nd ed. 2006: Springer Science & Business Media, Heidelberg.
17. Sornette, D., *Dragon-kings, black swans and the prediction of crises.* International Journal of Terraspace Science and Engineering, 2009. **2(1):1–18.**
18. Bier, V.M., *Statistical methods for the use of accident precursor data in estimating the frequency of rare events.* Reliability Engineering & System Safety, 1993. **41**(3): p. 267-280.
19. Wheatley, S., Kröger, W., Sornette, D. *Comprehensive Nuclear Events Data Base: Safety and cost perspectives*. in *Proc. ESREL*. 2017.
20. Minarick, J., *The US NRC accident sequence precursor program: Present methods and findings.* Reliability Engineering & System Safety, 1990. **27**(1): p. 23-51.
21. Apostolakis, G., Mosleh, A., *Expert opinion and statistical evidence: an application to reactor core melt frequency.* Nuclear Science and Engineering, 1979. **70**(2): p. 135-149.
22. Bier, V.M., Yi, W., *The performance of precursor-based estimators for rare event frequencies.* Reliability Engineering & System Safety, 1995. **50**(3): p. 241-251.
23. Gaertner, J., Canavan, K., True, D., *Safety and operational benefits of risk-informed initiatives.* EPRI White Paper, 2008.
24. World Nuclear Association, *Advanced Nuclear Power Reactors*. April 2014; Available from: http://www.world-nuclear.org/info/Nuclear-Fuel-Cycle/Power-Reactors/AdvancedNuclear-Power-Reactors/.

25. Ayoub, A., Stankovski, A., Wheatley, S., Kröger, W., Sornette, D., *ETHZ Curated Nuclear Events Database*. 2020: Retrieved from http://er-nucleardb.ethz.ch/.

Chapter 6

Risk Information transmission: Obstacles and practical solutions

When investigating past disasters, it soon becomes clear that before the disaster, some employees of the affected organization were aware of dangerous conditions that had the potential to escalate to a critical level. But for a variety of reasons, information about these risky conditions were not delivered to decision-makers. Consequently, the organization continued to move towards catastrophe, unaware of the possible threat - despite the fact that some of its employees clearly understood the likelihood of an impending disaster. In this chapter, we present our work on risk information transmission within critical infrastructure companies. Here, we only introduce the problem and the research methodology; the comprehensive study, details, and results can be found in our two Springer books cited in this chapter, which will be published by early 2022. The first book is focused on case studies of major disasters caused by intra-organizational silence and failure in upward feedback about observed risks before and during these disasters. The second book proposes practical solutions to the problem of risk information concealment mainly based on the professional opinions of 100 practitioners managing critical infrastructures around the world.

Based on:

- Chernov, D., **Ayoub, A.**, Sansavini, G., & Sornette, D., (2022). Averting disaster before it strikes: How to ensure your subordinates warn you while there is still time to act. *Springer.* Handbook to be published.
- Chernov, D., Sornette, D., Sansavini, G., & **Ayoub, A.**, (2022). Don't tell the boss: How poor communication on risks within organizations causes major catastrophes. Springer. Book to be published.

1. Introduction

Management theory postulates that executives control subordinates by means of information [1, 2]. They obtain information from different sources, process it, make a decision, and inform subordinates about it. Therefore the quality and the free flow of information reaching executives about the real situation inside and outside an organization affects their decisions, and ultimately the organization's response to any changes in the internal and external environment. Receiving appropriate feedback from subordinates about real conditions at the bottom of the corporate hierarchy is crucial for the effectiveness, and ultimately the survival, of an organization. It enables the timely detection of dangerous deviations in the operation of equipment, faulty production, violation of corporate rules, criminal action by employees, etc. But in reality, feedback from subordinates to superiors is usually distorted because of ill-advised organizational rules, principles and incentives, along with the natural human tendency for people to try and present themselves in a positive light, hiding their mistakes and faults. Unfortunately, this tendency can have disastrous consequences in the context of critical infrastructures and public health, just as it does in other fields of management.

To respond effectively to a disaster, executives need to have credible information about the preliminary causes of the incident, the extent of damage and the resources available to them, and agree on a clear vision of how to solve the crisis. If this information is honestly, directly, and promptly communicated to all interested parties, their questions about the details of an accident can be answered and the consequences can be promptly allayed.

A similar consensus about communication with external and internal stakeholders during a risk management process was expounded in the ISO 31000 report "Risk management — Principles and guidelines" published in November 2009. The report stipulates that for risk management to be effective, an organization should at all levels comply with several principles, one of which is that risk management "*is based on the best available information. The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgment. However, decision- makers should inform themselves of, and should take into account, any limitations of the data… Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects*" [3]. The standard does not set out practical solutions for improving the quality of internal risk transmission, but only outlines what better communication should achieve: "*The organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that: key components of the risk management framework, and any subsequent modifications, are communicated appropriately; there is adequate internal reporting on the framework, its effectiveness and the outcomes; relevant information derived from the application of risk management is available at appropriate levels and times; and there are processes for consultation with internal stakeholders. These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information*" [3].

Looking into major industrial accidents, we have identified different kinds of risk information concealment practices — both internally between members of an organization at different levels, and externally between the organization and external audiences — preceding and contributing to the disasters. We have also found practices of internal and external risk concealment in the financial sector, in state governance during natural disasters, and in the retail production and service industries.

Through the deep analysis of past disasters and of ongoing risky cases, our research sought to understand the obstacles that prevent the transmission of truthful, relevant, accurate and understandable risk information within organizations, and between organizations and governments or other external audiences. Our investigation concluded that when human beings distort information about risks before or during a disaster, their behavior is generally not determined by personal factors, but mainly by the existence of a flawed organizational environment that promotes secrecy and discourages honesty. We found that most of the factors obstructing the free transmission of risk information have been consistently present across many major disasters, which have occurred throughout the world, in different sectors, and in different historical periods according to quite similar scenarios.

Furthermore, we leveraged the experience of executives and top managers of worldwide leading critical infrastructure companies by seeking their professional opinion on how to overcome the identified causes of risk concealment during the operation of critical facilities. To this aim, we carried 100 professional in-depth interviews with high-level representatives (e.g. production or chief executive/technical officers, heads of safety departments, and Health, Safety and Environmental directors), to establish recommendations and practical solutions for the efficient and timely transmission of information about technological risks within large industrial companies. The main

targeted sectors include oil and gas, power generation and transmission, chemicals and petrochemicals, mining, and metallurgy.

2. Don't tell the boss: How poor communication on risks within organizations causes major catastrophes

In our book *"Don't tell the boss: How poor communication on risks within organizations causes major catastrophes"* [4], we analyzed 20 major disasters in details, where failures of internal and external risk communication played a dominant role in creating or aggravating a catastrophe. The aim is to analyze the factors that motivated different members of the organizations, or the involved project teams, to be hesitant in sharing risk-related information upwards, downwards or horizontally, and why their superiors preferred to ignore early warnings if they reported them. The causes of the internal risk concealment within these 20 cases were systematized and ranked by frequency of repetition. The following is the list of the 20 analyzed disasters:

1- Unreadiness of the Soviet Red Army for the Nazi invasion (USSR, 1941)
2- The great Chinese famine (China, 1958-1962)
3- Collapse of the Banqiao and Shimantan reservoir dams (China, 1975) the Machhu dam-II (India, 1979)
4- Problems with the rear cargo door of McDonnell Douglas DC-10 (USA, 1970s)
5- Challenger space shuttle accident (USA, 1986)
6- Chernobyl nuclear disaster (USSR, 1986)
7- Barings bank collapse (Singapore-UK, 1995)
8- Staphylococcus related food poisoning in Snow brand dairy products (Japan, 2000)
9- SARS outbreak (China, 2002-2003)
10- Amagasaki train derailment (Japan, 2005)
11- Sayano-Shushenskaya hydropower station disaster (Russia, 2009)
12- Upper Big Branch coalmine blowout (USA, 2010)
13- Deepwater Horizon oil spill (USA, 2010)
14- Raspadskaya coalmine blowouts (Russia, 2010)
15- Great wildfires in the European part of Russia (Russia, 2010)
16- Fukushima-Daiichi nuclear disaster (Japan, 2011)
17- The Volkswagen diesel engine emissions scandal (Germany-USA, 2000s-2010s)
18- Collapse of the Fundão tailing dam at Samarco iron ore mining site (Brazil, 2015)
19- Severnaya coalmine blowouts (Russia, 2016)
20- African swine fever epidemic in China (China, since 2018)

Furthermore, we made a literature review of other research on the challenges of voice and silence in organizations, citing some of the results which help to explain why people hesitate to communicate bad news to others, and why members of some organizations prefer to keep quiet about unpleasant facts or potential risks in communication with superiors and colleagues. Additionally, we present the results of a survey that we conducted with 52 middle managers providing government services to the public; we classify government administrative services, although they fall into the service sector, as part of the critical infrastructure of any state. We summarize the interviewees' responses of the reasons why information is concealed or distorted by employees in government administrative services. Finally, we utilized the information gained from 100 interviews with top managers of worldwide leading critical infrastructure companies, to understand why employees are reluctant to disclose risks when dealing with managers, why managers are reluctant to receive risk information, and who is primarily responsible for creating an internal climate where it is not acceptable to talk about

problems. On the basis of their answers, we outlined the top reasons why leaders don't want to hear about the problems in their companies, and why employees are reluctant to disclose risks when dealing with managers.

In summary, this book studies the obstacles which prevent the free and timely transmission of risk-related information within organizations or project teams. It aims to answer two questions: what is the problem with intra-organizational communication about risk, and why does this problem exist?

3. Averting disaster before it strikes: How to ensure your subordinates warn you while there is still time to act

In our handbook “Averting disaster before it strikes: how to ensure your subordinates warn you while there is still time to act” [5], we aim to establish recommendations and practical solutions for the efficient and timely transmission of information about technological risks within large industrial companies. The handbook serves several goals:

1- to demonstrate the critical importance of the free transmission of objective risk information within companies operating critical infrastructure,
2- to establish why risk-related information is sometimes distorted during communication between employees and management in critical infrastructure companies,
3- to provide critical infrastructure executives with practical and effective recommendations and tools, which will allow them to receive early warnings from subordinates before disasters happen.

This handbook sets out what top management needs to do to improve the flow of accurate risk-related information within critical infrastructure companies. The proposed recommendations are based on the opinions of 100 leader-practitioners of various ranks (top management, technical managers and safety managers), managing critical infrastructure companies in Western Europe, Russia, North America, the Middle East, Africa, and Australia. Interviewees were drawn from the following industries: oil and gas, power generation and distribution, metallurgy, chemicals and petrochemicals, mining and other industries. We believe that the opinion of leaders and practitioners across different industries is the most valuable input to the development of practical recommendations, as it guards against proposing theoretically plausible solutions that turn out to be difficult to apply in the practice of running a large industrial company.

The handbook focuses only on the problems of risk information transmission within a critical infrastructure organization, without touching on how risk information is communicated between the organization and its numerous external contractors and partners. The main audiences of the handbook are: executives of companies from critical industries; internal managers responsible for governance, risk management and compliance; heads of departments responsible for the operation of critical infrastructure; representatives of the global insurance industry — from companies which could begin to implement the recommendations made in the handbook within the organizations of their clients, to regulators of the insurance industry in different countries and editors of influential professional media; representatives of the global risk management community from different sectors and spheres — from corporate practitioners in uncritical industries to scientists and editors of professional websites and scientific journals; and professionals and scientists focused on general management issues, organizational studies and decision-making.

References

1. Hedberg, B., *How organizations learn and unlearn.* Handbook of organizational design (1), 1981: p. 3-27.
2. Mullins, L.J., *Management and organisational behaviour*. 2007: Pearson education.
3. ISO., *ISO 31000: 2009. Risk Management-Principles and guidelines*. 2009, ISO Geneva, Switzerland.
4. Chernov, D., Sornette, D., Sansavini, G., Ayoub, A., *Don't tell the boss: How poor communication on risks within organizations causes major catastrophes*. 2021: Springer. Book to be published.
5. Chernov, D., Ayoub, A., Sansavini, G., Sornette, D. , *Averting disaster before it strikes: How to ensure your subordinates warn you while there is still time to act*. 2021, Springer. Handbook to be published.

Curriculum Vitae

Ali Ayoub

Luegislandstrasse 59, 8051 Zürich

aayoub@ethz.ch

EDUCATION

ETH Zurich: PhD, Probabilistic Risk Assessment and Precursor Analysis **(2018 - 2021)**

ETH Zurich – EPF Lausanne: MSc, Nuclear Engineering **(2016 - 2018)**

American University of Beirut (AUB):

- BE in Mechanical Engineering (with Distinction) **(2012 - 2016)**
- BS in Applied Mathematics (with Distinction) **(2012 - 2016)**

RESEARCH INTERESTS

Risk Analysis, Probabilistic Safety Assessment, Nuclear Safety, Probability Theory, Precursor Analysis, Uncertainty Quantification and Sensitivity Analysis, Safety Culture, Nuclear Policy.

RESEARCH EXPERIENCE

ETH Zurich

PhD Researcher (2018 - 2021) - Supervisors: Prof. Didier Sornette and Prof. Wolfgang Kroeger:

- Developed the largest open nuclear events database focusing on worldwide nuclear precursors (http://er-nucleardb.ethz.ch).
- Developed generic, standardized, and modular PRA models for PWRs and BWRs, for efficient precursor analysis application.
- Performed large-scale precursor analyses (~1000 events) to generate empirical nuclear risk estimates and provide a framework for precursor's simulation and accident's prediction.
- Studied the problem of risk information concealment within critical infrastructure companies, and proposed solutions to improve intra-organizational risk communication and safety culture (two Springer Books).

MS Researcher (2017 - 2018):

- Carried a detailed uncertainty and sensitivity analyses for nuclear waste repositories performance assessment. Analysis covers reaction chemistry and large geology scales.
- Built a thermodynamic model of wet type natural draft cooling towers to perform a cost-efficiency thermodynamic analysis in a changing climate.

Leibstadt Nuclear Power Plant (2017)

- Developed and implemented a fast and robust Bayesian update tool/algorithm for components failure rates estimation in nuclear power plants.

Paul Scherrer Institute (2015, 2017)

- Developed event sequences for LOCAs, station blackout, main blower failure, and steam generator tube rupture internal initiating events for the High Temperature Gas Cooled Reactor-Pebble Bed Module (HTR-PM).

- Worked with the modeling and simulation group on implementing and verifying the Lagrangian particle tracking (LPT) approach in an in-house code (PSI-BOIL).

American University of Beirut (2016)

- Developed a methodology for Inverse Lagrangian particle tracking in stochastic flow fields.

AWARDS

- Best Reviewer Award at the International Youth Nuclear Congress **(IYNC 2020)**
- The George Apostolakis Early-Researcher Award in Risk Assessment **(PSAM 14, 2018)**
- Best paper Award Winner at the AUB FEA Student & Alumni Conference **(2016)**
- AUB Faculty of Engineering and Architecture: Dean's Honor List **(2012 - 2016)**

LIST OF PUBLICATIONS

Author and coauthor of **two working books**, **six published and three submitted journal papers**, and **four conference papers** in refereed international conference proceedings.

Books:

1. Chernov, D., **Ayoub**, A., Sansavini, G., Sornette, D., *Averting disaster before it strikes: how to ensure your subordinates warn you while there is still time to act*. 2022: Springer. Handbook to be published.
2. Chernov, D., Sornette, D., Sansavini, G., **Ayoub**, A., *Don't tell the boss: How poor communication on risks within organizations causes major catastrophes*. 2022: Springer. Book to be published.

Journals and conference proceedings:

1. **Ayoub, A.** and Sornette, D., *Comprehensive quantitative large-scale assessment of nuclear power risks*. Nature Energy, 2021. Under Review.
2. **Ayoub, A.,** Kröger, W., Sornette, D., *Generic and adaptive probabilistic safety assessment models: Precursor analysis and multi-purpose utilization*. Nuclear Engineering and Technology, 2021. Under Review.
3. Kröger, W. and **Ayoub**, A., *Autonomous Driving: A Survey with Focus on Reliability and Risk Issues*. Environment Systems and Decisions. 2021. Under Review.
4. **Ayoub, A.**, Stankovski, A., Kröger, W., Sornette, D., *The ETH Zurich Curated Nuclear Events Database: Layout, Event Classification, and Analysis of Contributing Factors*. Reliability Engineering & System Safety, May. 2021.
5. **Ayoub, A.**, Stankovski, A., Kröger, W., Sornette, D., *Precursors and Startling Lessons: Statistical Analysis of 1250 Events with Safety Significance from the Civil Nuclear Sector*. Reliability Engineering & System Safety, May. 2021.
6. **Ayoub, A.**, Stankovski, A., Kröger, W., Sornette, D., *Status of the ETHZ Curated Nuclear Events Database*. ESREL2020-PSAM15, 2020.
7. Kröger, W., Sornette, D., **Ayoub, A.,** *Towards Safer and More Sustainable Ways for Exploiting Nuclear Power*. World Journal of Nuclear Science and Technology 10.03 : 91. 2020.

8. **Ayoub, A.**, Pfingsten, W., Podofillini, L., Sansavini, G., *Uncertainty and Sensitivity Analysis of the Chemistry of Cesium Sorption in Deep Geological Repositories*. Applied Geochemistry, 104607. 2020.
9. **Ayoub, A.**, Kröger, W., Sornette, D., *Generic Probabilistic Safety Assessment Models for International Precursor Analysis Applications*. International Youth Nuclear Congress (IYNC). Sydney, Australia, Mar. 2020.
10. **Ayoub, A.**, Ariu, V., Nusbaumer, O., *A fast and robust Bayesian update of components failure rates in a nuclear power plant*. Progress in Nuclear Energy 118 : 103067. 2020.
11. **Ayoub, A.**, Kröger, W., Nusbaumer, O., Sornette, D., *Simplified/Harmonized PSA: A Generic Modeling Framework.* Probabilistic Safety Assessment conference (PSA 2019), April 2019.
12. **Ayoub, A.**, Gjorgiev, B., Sansavini, G., *Cooling towers performance in a changing climate: Techno-economic modeling and design optimization*. Energy 160 : 1133-1143. 2018.
13. **Ayoub, A.**, Ariu, V., Nusbaumer, O., *Improved Bayesian Update Method for Components Failure Rates*. Probabilistic Safety Assessment & Management conference (PSAM 14), Sep. 2018.

ACADEMIC ACTIVITIES

- Chair of the 2020 PSA Event Analysis Technical Meeting, Zurich, November 16-17, (**2020)**.
- Supervisor of several Masters and Bachelor students (Nuclear Safety, PSA, Autonomous driving safety, Statistics; **2018 - present**).
- Teaching assistant in several Grad/Undergrad courses on Risk, Statistics, and Mathematics **(2015 - present)**.
- Member of the European Commission ESReDA "Risk, knowledge, management" project group **(2020 - 2023 mandate)**.
- President of the AUB Math society **(2015 - 2016)**.

EXTRACURRICULARS

- Valedictorian of the American University of Beirut 147th undergraduate commencement ceremony **(2016)**.
- Founder of the American University of Beirut Electoral Law **(2016)**.
- Member of the AUB University Student-Faculty Committee **(2015 - 2016)**.
- Students' Delegate for the ETHZ-EPFL Nuclear Engineering Master's Program **(2016 - 2017)**.
- Students' representative on the "AUB Award for Excellence in Teaching Selection Committee".
- Second place winner at the World Health Organization (WHO) competition about youth, among all school representatives in Lebanon **(2008 - 2009)**.
- Co-organizer of several public civil nuclear power awareness events in Switzerland; particularly the "Stand Up for Nuclear" events **(2016 - 2020)**.

SKILLS

Language Skills

- Arabic (mother language), English (bilingual proficiency), German (intermediate), French (basic)

Computer Skills:

- MATLAB, SAPHIRE, C++, MCNP, Serpent, Ruby, LabVIEW, AutoCAD, Simulink