The ETH Zurich Curated Nuclear Events Database: Layout, Event Classification, and Analysis of Contributing Factors

Journal Article

Author(s):
Ayoub, Ali; Stankovski, Andrej; Kröger, Wolfgang; Sornette, Didier

Publication date:
2021-09

Permanent link:
https://doi.org/10.3929/ethz-b-000485196

Originally published in:
Reliability Engineering & System Safety 213, https://doi.org/10.1016/j.ress.2021.107781

Reliability Engineering and System Safety 213 (2021) 107781

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

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

Ali Ayoub[a,b,*,1], Andrej Stankovski[a,1], Wolfgang Kröger[a,b], Didier Sornette[a,b,c]

[a] Chair of Entrepreneurial Risks, D-MTEC, ETH Zürich, Switzerland
[b] ETH Risk Center, ETH Zürich, Switzerland
[c] Institute of Risk Analysis, Prediction and Management (Risks-X), Southern University of Science and Technology (SUSTech), Shenzhen, China

ARTICLE INFO

Keywords:
Nuclear accidents
Operational experience
Database
PSA
Safety
Risk analysis
Statistical analysis

ABSTRACT

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.

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

* Corresponding author.
E-mail address: aayoub@ethz.ch (A. Ayoub).

[1] These authors had equal contribution to this work.

https://doi.org/10.1016/j.ress.2021.107781
Received 21 January 2021; Received in revised form 16 April 2021; Accepted 4 May 2021
Available online 15 May 2021

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

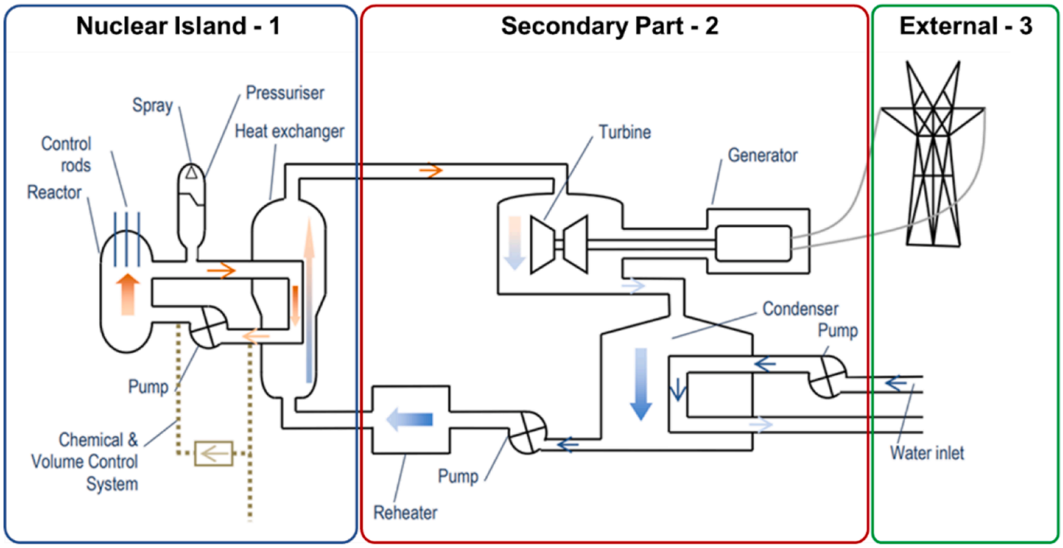

Fig. 1. Definition of plant boundaries for a pressurized water reactor (PWR) [27].

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.).

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.

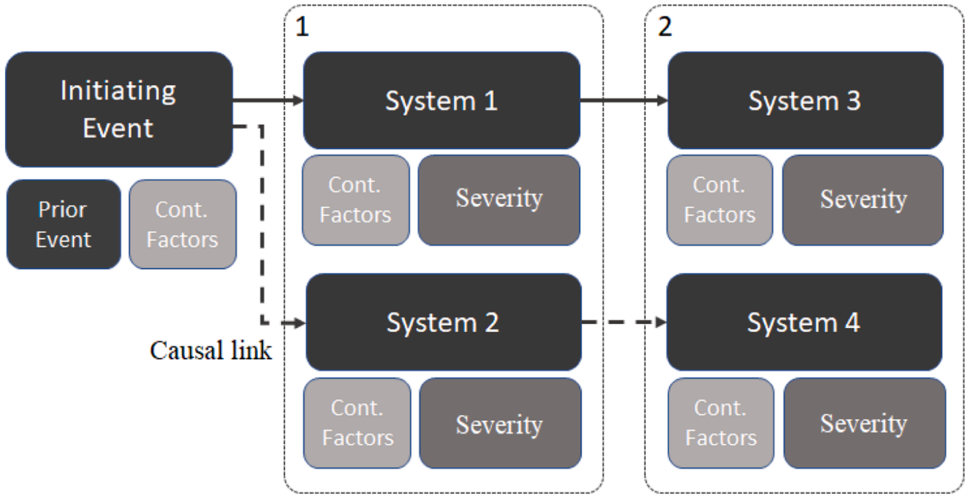

Fig. 2. Illustration of the failure sequences feature.

- 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.

The failure sequence shows all the involved events and systems

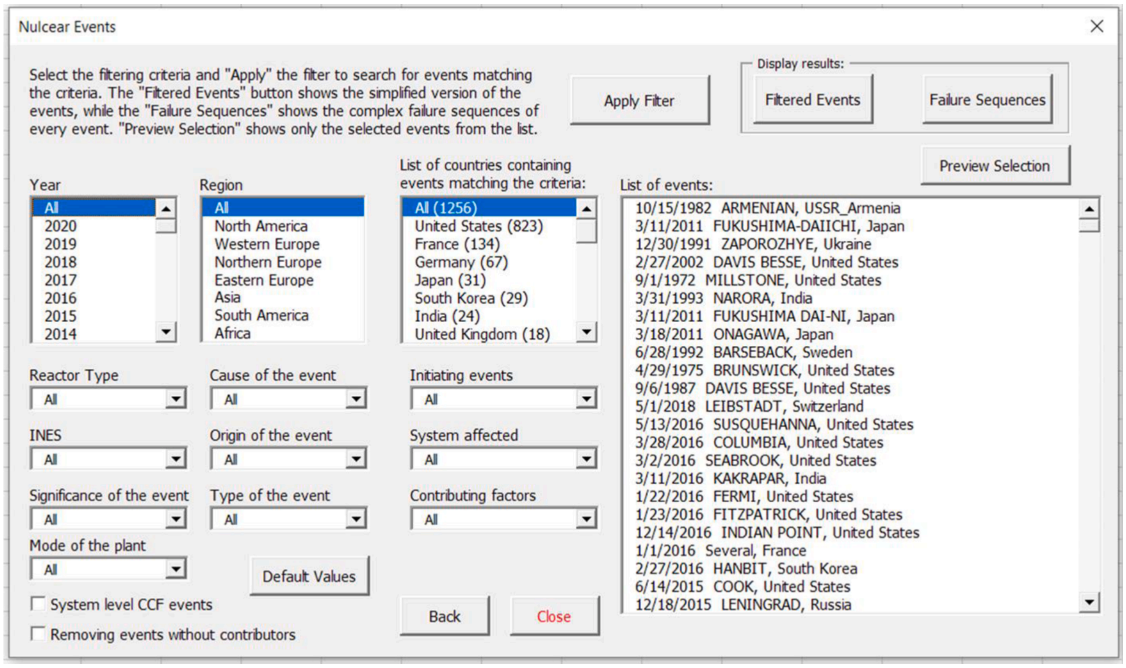

Fig. 3. Graphical user interface (GUI) of the ETHZ Curated Nuclear Events database showing filtering criteria and display options.

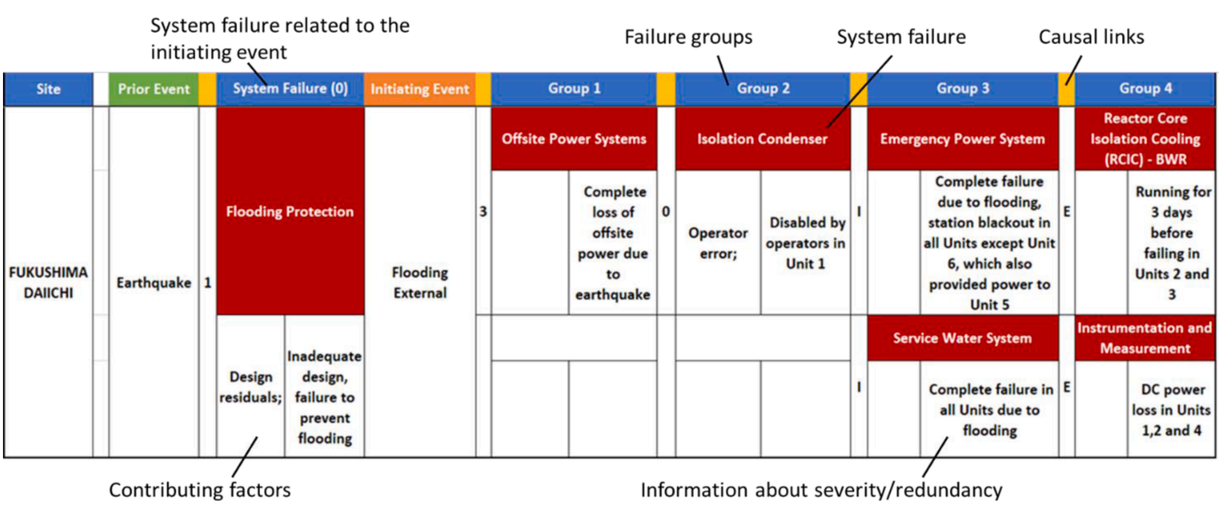

Fig. 4. Demonstration of the failure sequences using the Fukushima Daiichi 2011 nuclear accident.

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. 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

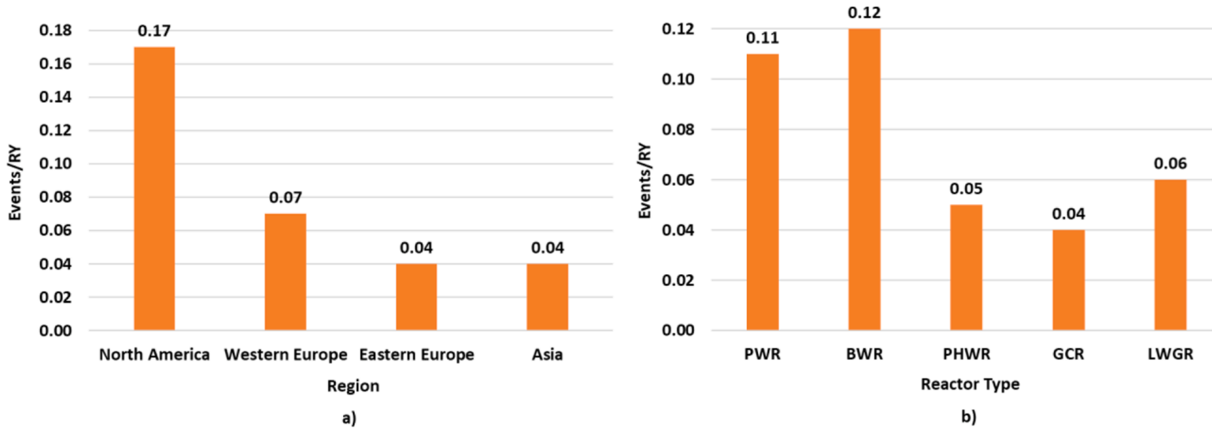

Fig. 5. Rates of events per reactor year, based on the: a) region and b) reactor type.

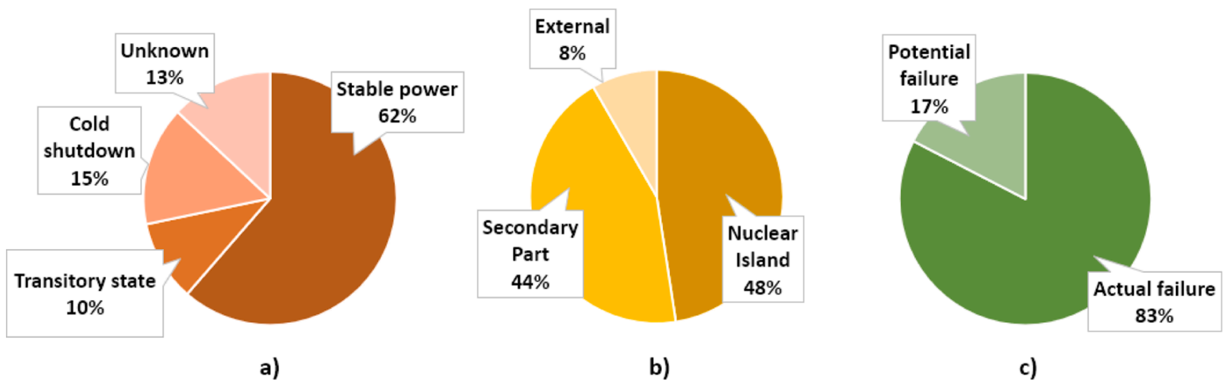

Fig 6. Breakdown of the number of events based on the: a) operating mode of the reactor; b) origin of the event; c) type of failure.

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].

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[2] 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.

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.

From Fig. 6 (a), it can be concluded that the majority of events occurred while the reactor was operating at stable power (62%).

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

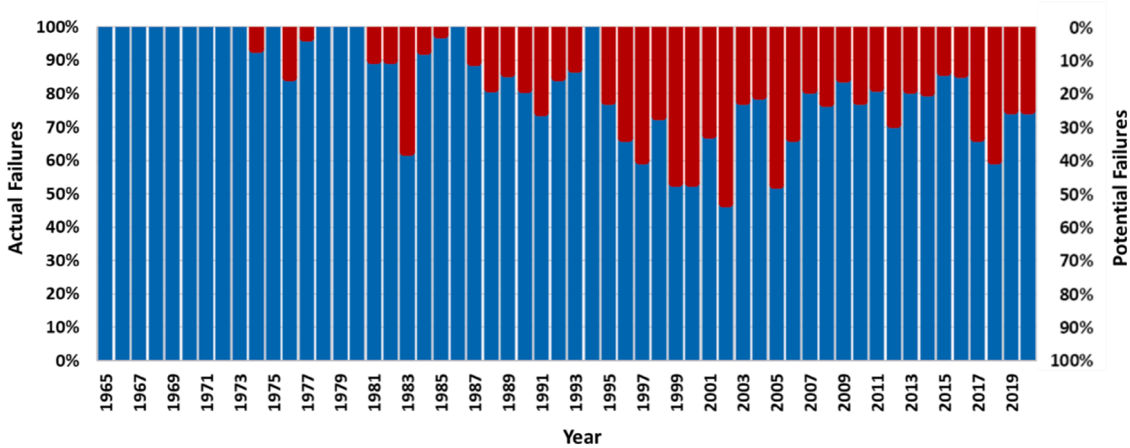

Fig. 7. Share of actual (blue) and potential (red) failures of the total events per year.

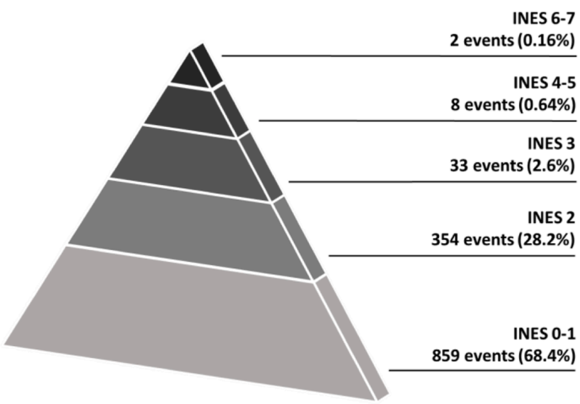

Fig. 8. Number of events based on their Core Only INES score.

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.

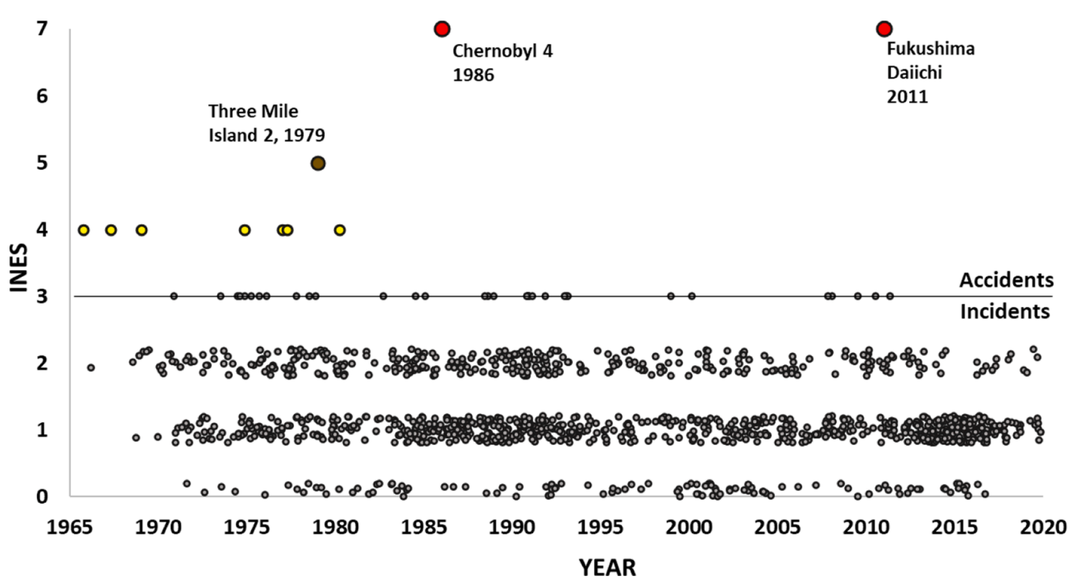

Fig. 9. Distribution of events based on their Core Only INES score per year of occurrence. For visibility, points are spread around their INES and year values.

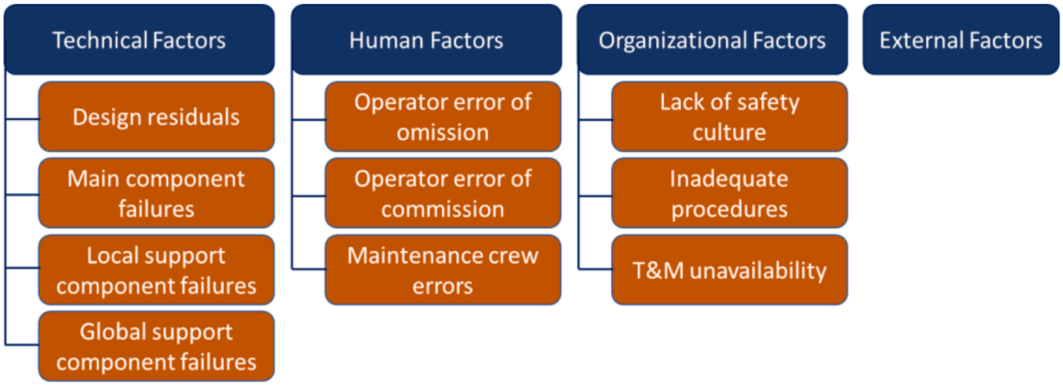

Fig. 10. Macro-classification of contributing groups. T&M means testing and maintenance.

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].

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.

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.

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%

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.

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

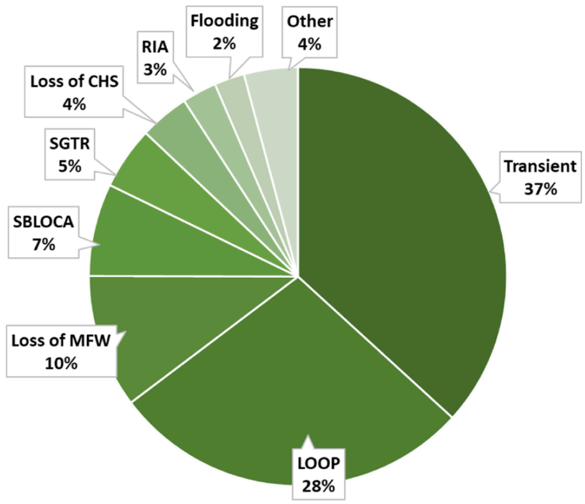

Fig. 11. Rate of occurrence of individual initiating events out of the total number of observed initiating events in the database. Meaning behind the abbreviations: LOOP – loss of offsite power; MFW – main feedwater; SBLOCA – small break loss-of-coolant accident; SGTR – steam generator tube rupture;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

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.

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%),

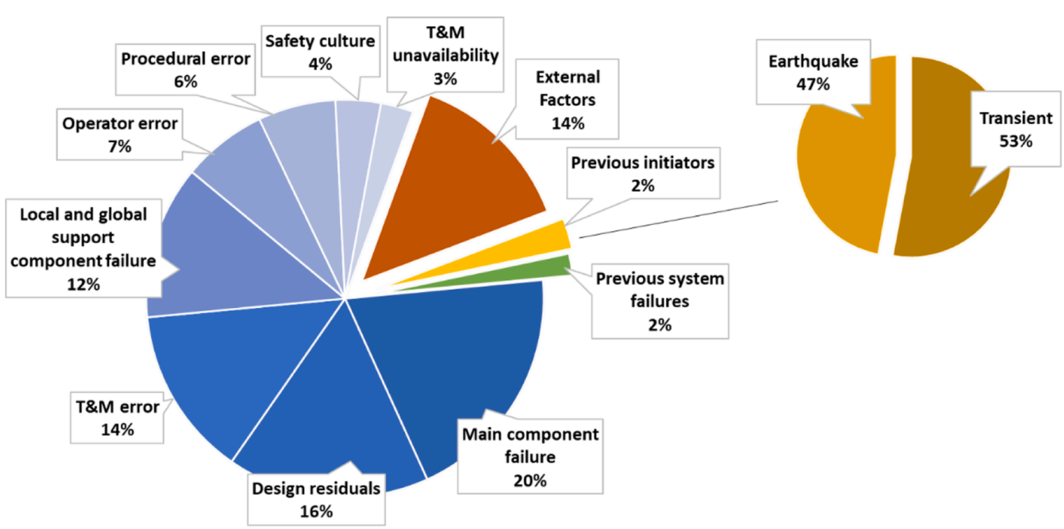

Fig. 12. Leading causes for the occurrence of initiating events. Meaning behind the abbreviation: T&M – testing and maintenance.

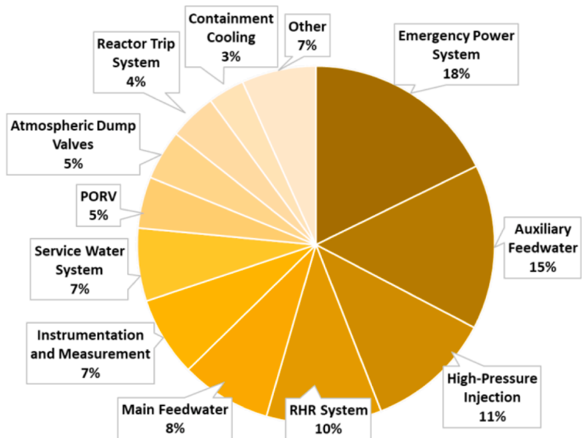

Fig. 13. Rate of occurrence of individual safety system failures out of the total number of observed safety system failures in PWRs. Meaning behind the abbreviation: PORV – pilot operated relief valve; RHR – residual heat removal.

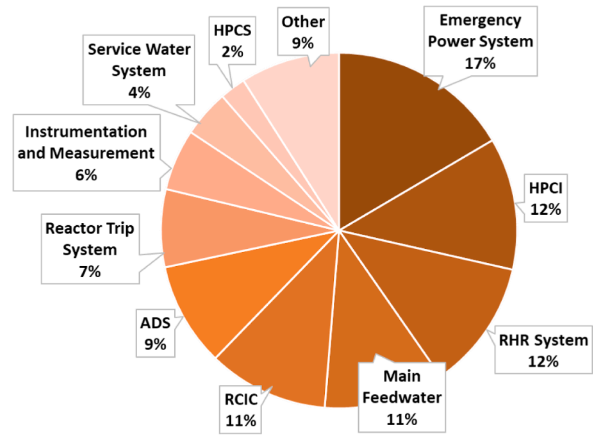

Fig. 15. Rate of occurrence of individual safety system failures out of the total number of observed safety system failures in BWRs. Meaning behind the abbreviations: RCIC – reactor core isolation cooling; HPCI – high pressure coolant injection; ADS – automatic depressurization system; HPCS – high pressure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

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).

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.

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

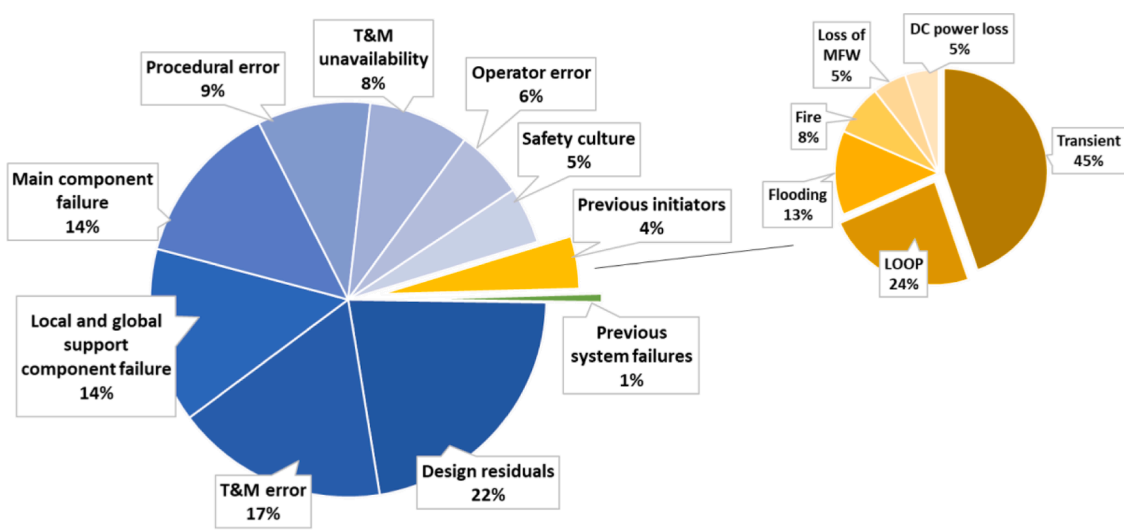

Fig. 14. Leading causes for the occurrence of safety systems failures in PWRs. Meaning behind the abbreviations: T&M – testing and maintenance; MFW – main feedwater; LOOP – loss of offsite power, DC – direct current.

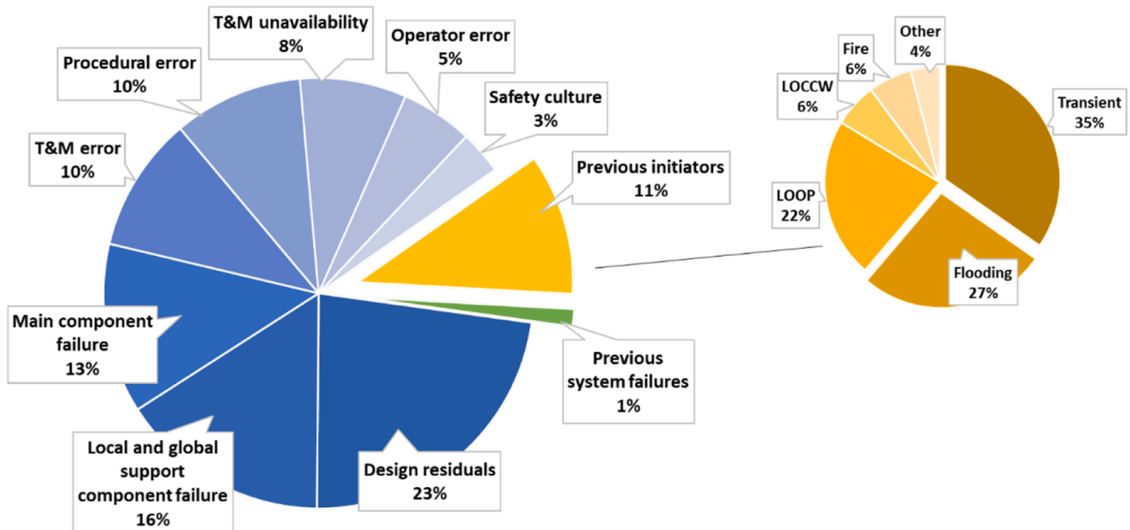

Fig. 16. Leading causes for the occurrence of safety systems failures in BWRs. Meaning behind the abbreviations: T&M – testing and maintenance; LOOP – loss of offsite power; LOCCW – loss of component cooling water.

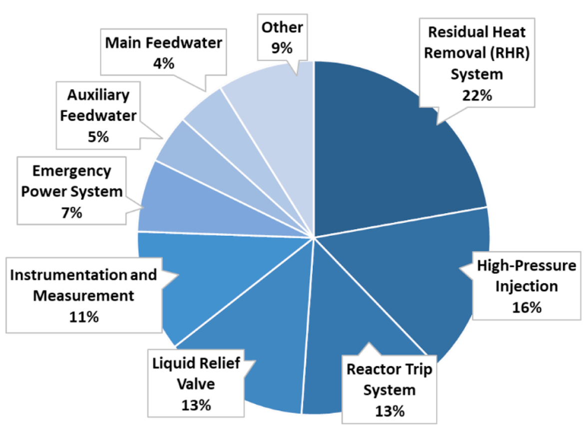

Fig. 17. Rate of occurrence of individual safety system failures out of the total number of observed safety system failures in PHWRs.

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.

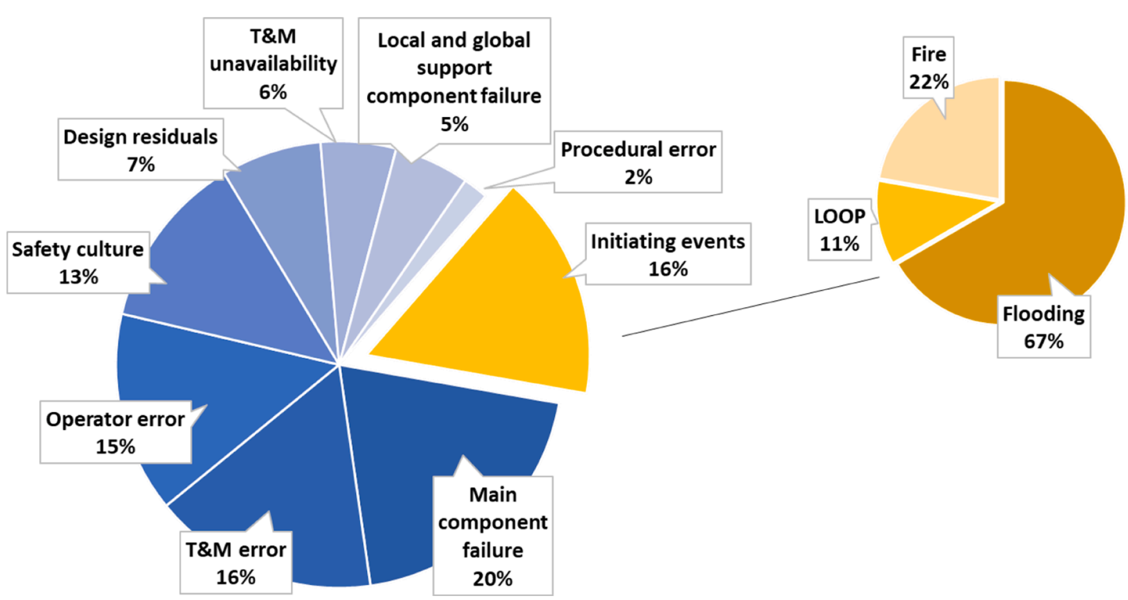

Fig. 18. Leading causes for the occurrence of safety systems failures in PHWRs. Meaning behind the abbreviations: T&M – testing and maintenance; LOOP – loss of offsite power.

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%.

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).

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%.

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.

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].

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

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.

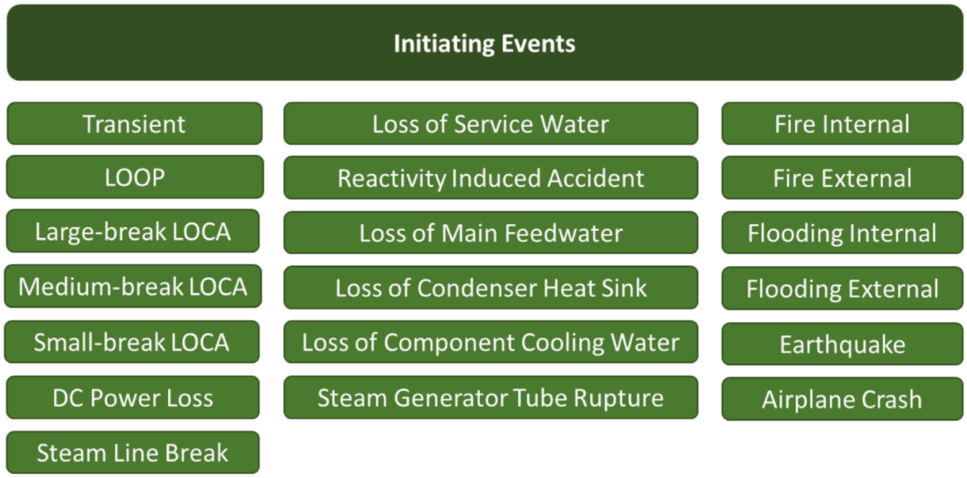

Fig. A.1. Considered initiating events in the database. Abbreviations: LOOP – loss of offsite power; LOCA – loss-of-coolant-accident.

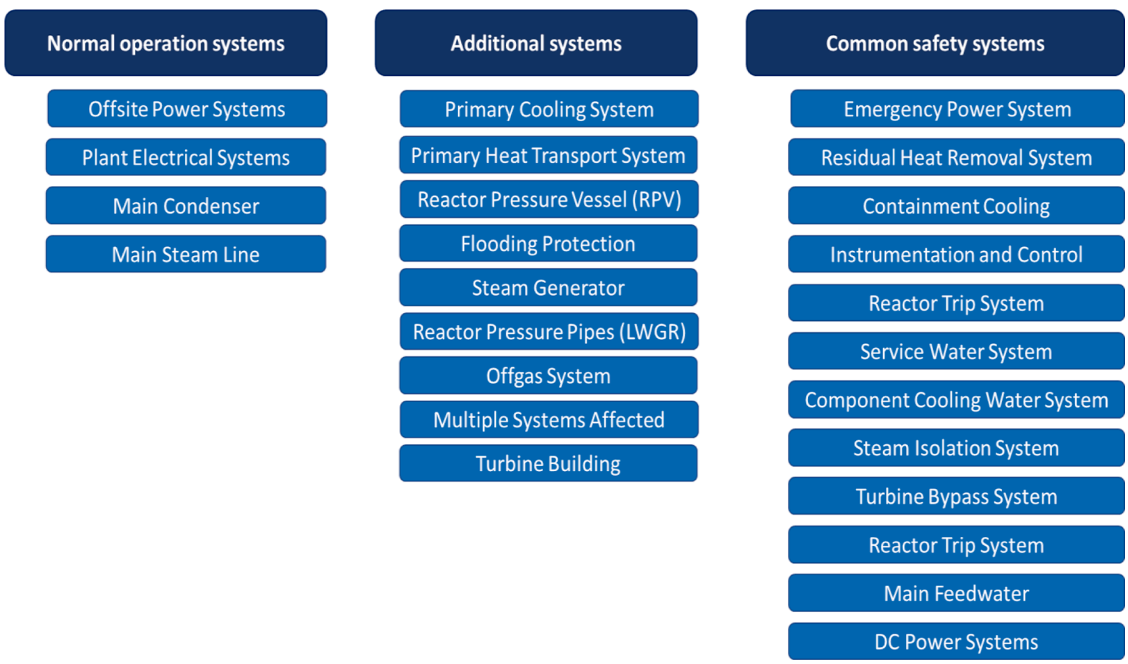

Fig. A.2. Considered common systems encompassing all reactor types in the database.

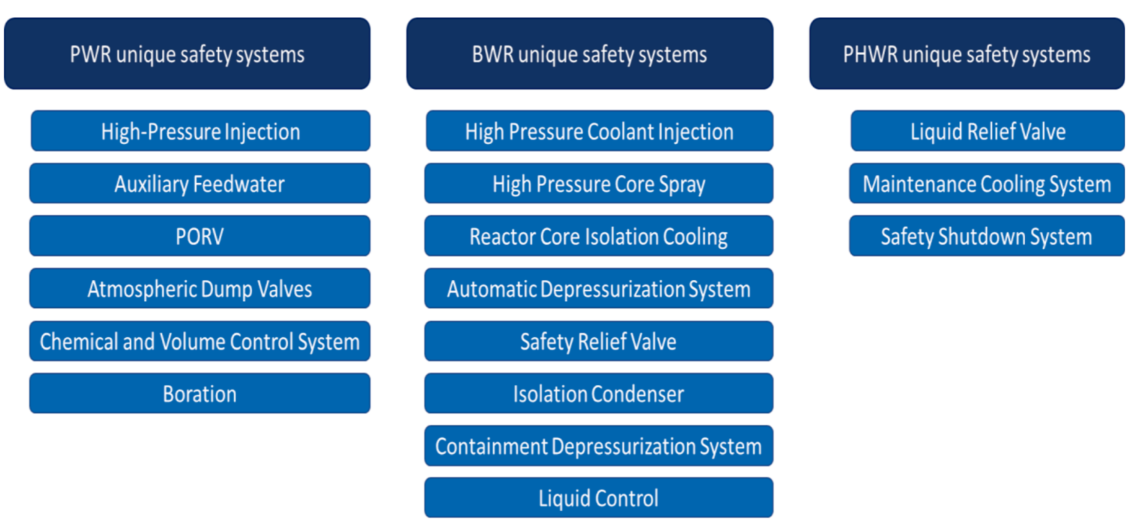

Fig. A.3. Considered systems specific for the most common reactor types in the database.

References

[1] Gordon RPE. The contribution of human factors to accidents in the offshore oil industry. Reliab Eng Syst Saf 1998;61(1):95–108.
[2] Chernov D, Sornette D. Man-made catastrophes and risk information concealment. Springer; 2016.
[3] Chernov D, Sornette D. Critical risks of different economic sectors. Springer; 2020.
[4] Gnoni MG, Saleh JH. Near-miss management systems and observability-in-depth: handling safety incidents and accident precursors in light of safety principles. Saf Sci 2017;91:154–67.
[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. Ann Nucl Energy 2019;130:192–9.
[6] Moura R, Beer Michael, Patelli Edoardo, Lewis John, Knoll Franz. Learning from major accidents to improve system design. Saf Sci 2016;84:37–45.
[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. Saf Sci 2017;99:58–70.
[8] Hauge S, Hokstad Per, Håbrekke Solfrid, Lundteigen Mary Ann. Common cause failures in safety-instrumented systems: using field experience from the petroleum industry. Reliab Eng Syst Saf 2016;151:34–45.
[9] Preischl W, Hellmich M. Human error probabilities from operational experience of German nuclear power plants. Reliab Eng Syst Saf 2013;109:150–9.
[10] Preischl W, Hellmich M. Human error probabilities from operational experience of German nuclear power plants, Part II. Reliab Eng Syst Saf 2016;148:44–56.
[11] Park J, Kim Y, Jung W. Calculating nominal human error probabilities from the operation experience of domestic nuclear power plants. Reliab Eng Syst Saf 2018;170:215–25.
[12] Kröger W. Securing the operation of socially critical systems from an engineering perspective: new challenges, enhanced tools and novel concepts. Eur J Secur Res 2017;2(1):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 JW, Rasmuson DM. The US NRC's accident sequence precursor program: an overview and development of a Bayesian approach to estimate core damage frequency using precursor information. Reliab Eng Syst Saf 1996;53(2):205–16.
[21] Ayoub A, Stankovski Andrej, Wheatley Spencer, Kröger Wolfgang, Sornette Didier. ETHZ Curated Nuclear Events Database. 2020. retrieved from http://er-nucleardb.ethz.ch/.
[22] 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.
[23] Mosleh A. PRA: a perspective on strengths, current limitations, and possible improvements. Nucl Eng Technol 2014;46(1):1–10.
[24] Ayoub A, Nusbaumer Olivier, Kröger Wolfgang, Sornette. Didier *Simplified/Harmonized PSA: a generic modeling framework*. In: International Topical Meeting on Probabilistic Safety Assessment and Analysis(PSA 2019). American Nuclear Society (ANS); 2019.
[25] Ayoub A, Kröger Wolfgang, Sornette Didier. Generic Probabilistic Safety Assessment Models for International Precursor Analysis Applications. In: International Youth Nuclear Congress (IYNC); 2020.
[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. Paris, France: NEA, OECD; 2011.
[28] U.S.NRC. Accident Sequence Precursor (ASP) Program - Summary Description. Washington, DC; 2008.
[29] Sornette D, Kröger W, Wheatley S. New Ways and Needs for Exploiting Nuclear Energy. Springer; 2018.
[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. Nucl Regulatory Commission 2007. NUREG/CR-6928.
[31] Poloski J, Marksberry D, Atwood U. Rates of initiating events at us nuclear power plants. Washington (DC): US Nuclear Regulatory Commission; 1999. NUREG/CR-5750.
[32] Morrow SL, Koves GK, Barnes VE. Exploring the relationship between safety culture and safety performance in US nuclear power operations. Saf Sci 2014;69:37–47.
[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. Saf Sci 2013;53:82–95.
[34] Kinnersley S, Roelen A. The contribution of design to accidents. Saf Sci 2007;45(1-2):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. Saf Sci 2019;118:288–97.
[36] Ayoub A, Stankovski Andrej, Kröger Wolfgang, 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.