Automated Integration and Network-Based Analysis of Hazard Impacts within Probabilistic Safety Analysis (PSA) Models

GRS - 565

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Automated Integration and Network-Based Analysis of Hazard Impacts within Probabilistic Safety Analysis (PSA) Models

Nadine Berner

July 2020

Remark:

This report refers to the research project RS1556 which has been funded by the German Federal Ministry for Economic affairs and Energy (BMWi).

The work was performed by Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH.

The author is responsible for the content of this report.

GRS - 565
ISBN 978-3-947685-50-9

Key Words

Agent-based Concept, Automated Integration, Complex System, Hazard Impact,
Multi-dimensional Network, Multiplex Network, Network Analysis, Probabilistic Risk Assessment (PRA),
Probabilistic Safety Analysis (PSA), Topological Modification

Kurzfassung

Die umfassende systematische Berücksichtigung einer Vielzahl real zu unterstellender übergreifender Einwirkungen (Englisch als Hazards bezeichnet) – einschließlich der Einwirkungskombinationen abhängiger wie unabhängiger Einwirkungen – führt zu einer wesentlichen systematischen Erweiterung bisheriger probabilistischer Sicherheitsanalysen (PSA) für komplexe technische Systeme (z. B. eines Kernkraftwerks). Die Berücksichtigung von Auswirkungen solcher Einwirkungen stellt insofern eine große Herausforderung dar, da selbst die Auswirkungen einer einzelnen übergreifenden Einwirkung komplex und spezifisch für das jeweilige Anlagensystem sein können.

Um ausgewählte übergreifende Einwirkungen auf ein komplexes Anlagensystem abzubilden, wird ein allgemeiner Ansatz verfolgt, der auf der Identifizierung relevanter, voneinander abhängiger Raumbereiche (sogenannter Compartments), die von der zu berücksichtigenden Einwirkung unterschiedlich betroffen sind, basiert. Eine PSA für übergreifende Einwirkungen, die auch als Hazards PSA bezeichnet wird, lässt sich dabei möglichst effizient mittels einer automatisierten Integration der abgeleiteten relevanten Raumbereiche (als Hazard Compartments, kurz HCs, bezeichnet) in die Fehlerbäume für die von der Einwirkung betroffenen sicherheitsrelevanten Bauteile, Systeme und Komponenten erstellen. Zu diesem Zweck hat die GRS die agentenbasierte Software pyRiskRobot entwickelt, mit welcher komplexe und aufwendige topologische Operationen effizient durchgeführt werden können, so dass übergreifende Einwirkungen zuverlässig in PSA-Anlagenmodelle der Stufe 1 integriert werden können.

Da die Abhängigkeiten der HCs selbst höchst komplex sind, wurde ein netzwerkbasierter Analyseansatz für HCs erarbeitet, um die Auswirkungen einer übergreifenden Einwirkung noch vor Integration in das PSA-Anlagenmodell zu organisieren, visualisieren und analysieren. Das breite Spektrum deskriptiver Netzwerkmaße ermöglicht es, wichtige Netzwerkelemente (d. h. HCs) zu identifizieren und mehrere Netzwerke (d. h. Auswirkungen verschiedener Hazards) auf lokaler und globaler Ebene zu vergleichen. Der netzwerkbasierte Ansatz wurde im Rahmen der HC-Abhängigkeitsanalyse für einen anlageninternen Brand in einer Referenzanlage erprobt. Basierend darauf wurden mögliche Strategien zur Anpassung und Erweiterung des untersuchten HC-Netzwerkes für weitere übergreifende Einwirkungen, wie beispielsweise anlagenexterne Überflutungsereignisse, diskutiert.

Das Konzept der netzwerkbasierten Analyse einzelner HC-Abhängigkeiten lässt sich auf einen mehrdimensionalen netzwerkbasierten Ansatz zur einheitlichen Untersuchung mehrerer Hazards als Schichten eines Multiplexnetzwerks erweitern. Dieser Ansatz dient als zusätzlicher, ergänzender Analyseschritt, um die Abhängigkeiten der HCs vor ihrer Integration in ein PSA-Anlagemodell der Stufe 1 zu untersuchen. Darüber hinaus liefert der Ansatz die methodischen Grundlagen, um Korrelationen zwischen verschiedenen übergreifenden Einwirkungen zu berücksichtigen, die über die grundlegende Annahme unabhängiger Ereignisse infolge übergreifender Einwirkungen deutlich hinausgehen.

Abstract

A comprehensive and systematic consideration of multiple hazards in terms of induced hazards and credible combinations of related as well as independent hazards represents an important enhancement of a probabilistic safety analysis (PSA) for a complex technical system, such as a nuclear power plant. The consideration of impacts by hazards is challenging since even the impact of any individual hazard is complex and specific with respect to the given plant system.

A general approach to map a specific hazard impact pattern to a complex plant system offers the identification of relevant, mutually dependent compartments being differently affected by the given hazard. An appropriate hazards PSA can be efficiently performed, e. g. by automatically integrating the hazard compartments (HCs) derived in the fault trees of the affected systems, structures and components (SSCs) important to safety. For this purpose, GRS has developed the agent-based software pyRiskRobot for efficiently performing complex and laborious topological operations in order to reliably integrate hazard impacts in Level 1 PSA plant models.

The HC dependency patterns are complex themselves. Therefore, a network-based analysis approach of HCs has been developed to organise, visualise and analyse the hazard impact characteristics prior to the integration in the PSA plant model. The broad spectrum of descriptive network measures allows to identify important network elements (i. e. HCs) and to compare multiple networks (i. e. hazard impact patterns) on a local and global scale. The network-based approach has been validated for the plant internal hazard fire in an exemplary nuclear power plant and, the potential strategies to adapt the reference network to other hazards, such as an external flooding, have been discussed.

The concept of network-based analysis of individual HC dependency patterns has been extended towards a multidimensional network-based approach for jointly investigating multiple hazard impacts as layers of a multiplex network. The approach can be used as an auxiliary, complementary analytical step to study hazard impact patterns prior to their integration in a Level 1 PSA plant model. Moreover, the approach yields the methodological base to consider correlations between different hazards beyond the common basic assumption of independent events resulting from hazards.

Acknowledgements

The author wants to thank Matthias Utschick (formerly GRS) and Gurgen Kanetsyan (Nuclear and Radiation Safety Center, Armenia) for valuable insights and fruitful discussions about the practical and conceptional challenges faced during the enhancement process of PSA models towards HPSA models. Moreover, the author thanks Manorma Kumar (Lloyd's Register, Sweden) and Anders Olsson (Lloyd's Register, Sweden) for interesting discussions about strategies for addressing combinations of multiple hazard impacts in the frame of Level 1 PSA framework. The author also wants to express her thanks to Josef Scheuer (GRS) for critical and important discussions on network applications from the perspective of an information and computer scientist.

The author wants to acknowledge the support provided by the German Federal Ministry for Economics and Energy ("Bundesministerium für Wirtschaft und Energie", BMWi) for funding the development of PSA methods and tools by GRS in the frame of the research and development project RS1556.

Contents

1 Introduction

Based on the operating experience from nuclear facilities worldwide, evidence has increased that the consideration of impacts from hazards on a nuclear installation is of fundamental importance for enhancing safety assessments of such complex technical systems, particularly for probabilistic safety analysis (PSA). For instance, the nuclear accidents Fukushima Dai-ichi in Japan in March 2011 resulted from the combination of two causally related external hazards, an earthquake with a consequential tsunami. The consequences of this hazard combination, especially a flooding of the site by the tsunami, exceeded the design basis of the nuclear power plant (NPP) units. The nuclear accidents highlighted several challenging issues, such as cascading events, cliff-edge effects and multi-unit plants, with respect to the application of common PSA concepts for such low-probability but high-consequences external events /FOE 20/. In recent years, scientific and technical approaches for the characterisation of external natural extreme events and the evaluation of their consequences on the safety of complex technical plant systems have been reviewed, discussed and improvement strategies elaborated amongst others by the collaborative international projects funded by the European Commission (EC) ASAMPSA_E (*A*dvanced *S*afety *A*ssessment *M*ethodologies: *E*xtended *PSA*), carried out between 2013 and 2016 /EC 20/ and NARSIS (*N*ew Approach to *R*eactor *S*afety *I*mprovement*s*), which is ongoing since 2017 and intended to end in 2021 /NAR 20/.

One of the major insights from these international projects emphasises the need for extending the scope of PSA in order to appropriately consider the entire spectrum of individual (single) internal and external hazards as well as all types of hazard combinations in a systematic manner. The resulting PSA approach extended for the hazard impacts is commonly referred to as a hazards PSA (HPSA). Another important insight is that in order to appropriately assess the robustness of the plant behaviour under hazard impacts, the risk aggregation on the site-level has to be taken into account. The aspect of risk aggregation requires that all reactor units and radioactive sources collocated on a common site need to be considered in the comprehensive safety analysis /NEA 20/. The resulting multi-unit and multi-source PSA approach is commonly referred to as a site-level PSA.

The key insights mentioned above necessitate efficient, dynamic and reliable PSA modelling strategies allowing to adapt existing Level 1 PSA plant models for addressing additional, often complex issues in the analyses significant for the overall plant behaviour

and especially for items important to safety. For instance, the integration of hazard impacts in the PSA of a NPP representing a highly complex plant system can be accomplished by extending the existing Level 1 PSA plant model by all hazard related effects on the availability of the respective systems, structures and components (SSCs) of the plant.

The approach for conducting such a HPSA is a challenging task due to the complexity of the given plant system and of the hazard specific impact patterns. In general, a HPSA requires a vast amount of modifications of the PSA plant model. To enable the analyst to efficiently and systematically integrate a specific hazard impact in an existing Level 1 PSA plant model, GRS has developed the software tool (py)RiskRobot as an approach for modifying complex fault tree (FT) topologies in an automated and traceable manner, introduced in /HER 12/ as RiskRobot and extended in /BER 17a/ to its current python-based version pyRiskRobot. Besides the automated integration of hazard impacts through extensive FT modification, the modelling concept also enables the analyst to generate Level 1 PSA plant models on the site-level considering multiple collocated reactor and non-reactor nuclear facilities by the automated duplication of exemplary reactor units at a given reference site within existing PSA plant models.

Performing a HPSA requires a comprehensive understanding of the acquired information about the impact on the plant system for a hazard to be considered. The hazard related information covers the SSCs potentially affected by the hazard impact, the specific impact effects from the hazard on SSCs and the potential hazard dependencies during the impact on the whole plant system. Due to the complexity of the hazard impact data, it is of high interest to investigate the properties and dependencies of the hazard impact as mapped to the plant system, e. g. in terms of derived hazard compartments (HC) each containing assigned SSCs equally affected by the given hazard. HCs are generally modelled as a large set of disjunct entities with mutual interrelations of potential directional dependencies. Therefore, HCs can be effectively organised, intuitively visualised and statistically analysed as a complex network with respect to a single hazard impact /BER 19/ or as a multiplex network with respect to multiple hazard impacts /BER 20/. The broad spectrum of descriptive network measures allows to identify important network elements, e. g. individual HCs, and to compare multiple networks, e. g. representing a different hazard impact on the same plant building, on a local and global network scale. In order to support the modelling tasks that arise in the context of hazard impacts, an additional module to the pyRiskRobot tool has been developed by GRS, to perform the

network-based visualisation and analysis of complex HC dependencies as a prior and facilitating step to the modelling of a HPSA.

In the following, an overview on the general PSA framework and strategies to integrate hazard impacts in the PSA plant model through HCs is provided in Chapter 2. In Chapter 3 the agent-based concept of pyRiskRobot is presented allowing to flexibly perform complex and time-consuming modelling tasks in PSA plant models in an automated manner. In Chapter 4 the representation of HCs as complex networks and strategies to analyse, characterise and compare HC networks are discussed. The extension of the approach to comprehensively represent, compare and combine multiple hazard impacts, i. e. multiple sets of HCs, through multidimensional complex networks is introduced in Chapter 5. The report is concluded with a summary of the methodological findings and the discussion of potential applications in Chapter 6.

2 Hazard Probabilistic Safety Analysis

An important enhancement of the probabilistic safety analysis (PSA) of a complex technical system, such as a nuclear power plant (NPP), provides the consideration of multiple hazards in terms of induced hazards and credible combinations of related as well as independent hazards (cf. /IAE 20/). It is of interest to investigate and quantify the potential effect on the risk metrics of an NPP plant system due to the hazard impact. Note, in the following an NPP plant system is simply referred to as plant system throughout this report.

An appropriate probabilistic safety analysis for hazards (a so-called hazards PSA, HPSA) can be realised based on a comprehensive database containing the information required to characterise the hazard impact on the plant system (described e. g. in /LIN 07/, /TUE 15a/, /ROE 17/, and /ROE 18/). The impact on the plant facility can be characterised by a corresponding group of initiating events (IEs) induced by hazards and the hazard(s) induced failures of SSCs as explained in /TUE 14/, /TUE 15/ and /ROE 17/. By integrating the relevant hazard impact patterns in a Level 1 PSA plant model comprehensive risk measures can be computed by considering a specific hazard impact for accident sequences modelled in the respective event tree (ET) of interest.

To provide a self-contained overview on the extension strategy of PSA plant models towards HPSA approaches, the conceptional understanding of PSA plant models and the integration of hazard impacts are outlined in the following. To put this methodological HPSA approach into perspective other approaches for considering hazards and hazard combinations in a Level 1 PSA are discussed.

2.1 Probabilistic Safety Analysis Models

Probabilistic risk assessment (PRA) is conducted by performing a comprehensive, systematically structured, and logical analysis approach specialised on identifying and assessing risks in complex technological systems for the purpose of improving their safety related performance. The general outcome of a PSA for complex engineered plant systems yields the quantitative risk estimation of entering undesired system states for specific scenarios of interest, referred to as IEs. In the context of NPPs, an undesired plant state of interest may be the damage of the nuclear fuel with the possibility of a release of a certain amount of radioactivity to the environment. The corresponding final states of a Level 1 PSA are core and/or fuel damage states. The respective frequencies are core and/or fuel damage frequency. The development of the Level 1 PSA plant model is

based on the logical representation of the technical system behaviour including the failure or unavailability of SSCs important to safety. The logical models constructed in the frame of probabilistic risk assessment require to investigate in detail the occurrence and consequences of relatively rare IEs, for which the likelihood of event occurrences is generally inferred from theoretical modelling approaches. In this context, the main assumption is that the failure or unavailability can sufficiently well be characterised by random variables, quantified based on past observations which are considered as realisation of an underlying random process /KIR 99/.

To provide a more detailed conceptual understanding of PSA plant models, the basic modelling components and analytical steps of the PSA plant model are illustrated in Fig. 2.1. A Level 1 PSA plant model consists of ETs modelling the response of the system to an IE of interest (e. g., a major component failure, or a station black-out) as an accident sequence potentially leading to undesired damage states of systems and components (e. g., core or fuel damage). Various fault trees (FTs) representing in more detail the unavailability of SSCs are embedded in the ET allowing to derive the transition probabilities between the sequence branches of the event sequences modelled. The combination of ETs and FTs assigned to the specific sequence transitions allows to comprehensively derive global risk metrics and importance measures of the complex technical plant system.

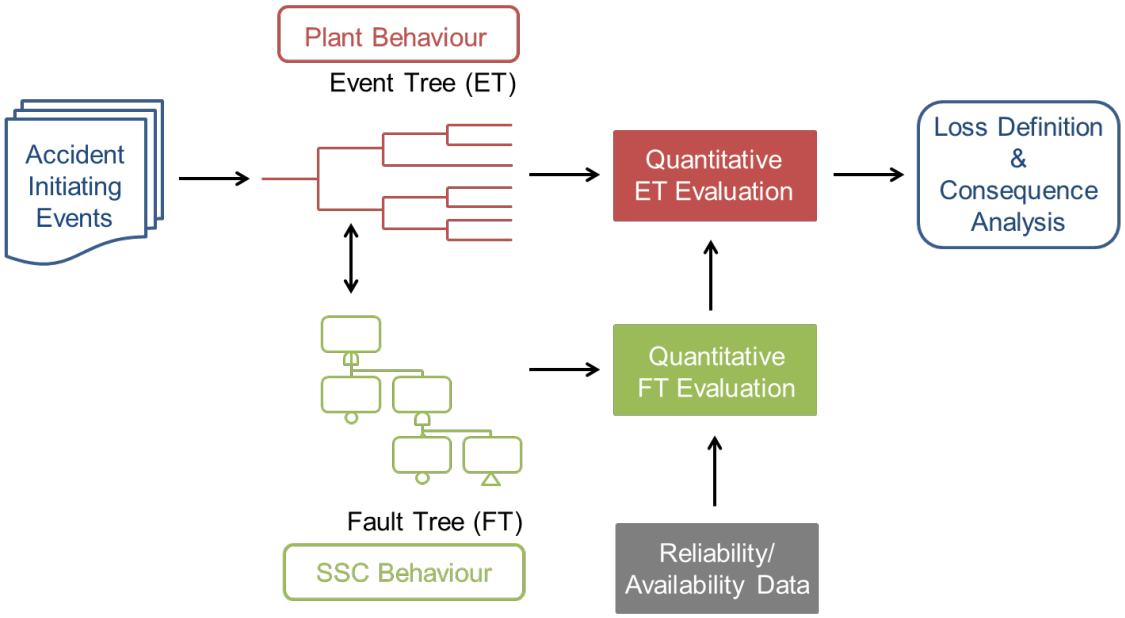


Fig. 2.1 Main analysis steps of a Level 1 PSA plant model based on /KIR 99/

The term risk metric refers to probabilistic performance measures indicated by the frequency or probability of expected consequences of a specific magnitude. Typical PSA results therefore include the contributions of sequences to targeted risk metrics and of failure causes to the targeted risk /STA 11/. In the nuclear context, the risk may be indicated by an estimated frequency, such as the core damage frequency.

Thus, the PSA plant model allows to consider the complete plant behaviour from a scenario-based perspective, i. e. an event sequence modelled as an ET, at a degree of complexity defined by the accomplished modelling depth, i. e. in which detail the FTs for SSCs are implemented and what causes for their unavailability are taken into account. An important strength of a probabilistic analysis approach is the integrative and quantitative concept which allows a ranking of issues and results as well as explicit consideration and treatment of all types of given uncertainties. In general, the integration of additional aspects in the PSA plant model can be done either by introducing a new scenario, i. e. assuming a further IE with an associated ET, or by integrating new causes to the unavailability of SSCs, i. e. to the associated FTs. The latter can be an additional basic event (BE) of the FT or a complete sub-FT indicating a more complicated cause resulting from multiple BEs.

2.2 Modelling Hazard Impacts

A hazard impact can represent an additional aspect to be considered within a PSA. The hazard impact on a plant system can be characterised by a corresponding group of IEs resulting from hazards and hazard induced failures of SSCs /TUE 14/ and /TUE 15/. The affected system functions modelled as FTs within the Level 1 PSA plant model can be systematically modified in accordance to these additional failure causes and failure dependencies. By modifying the PSA topology of either ETs or FTs, an existing PSA plant model can be extended considering the hazard specific impact patterns. The required modifications are derived from a hazard database containing the information relevant to characterise the hazard impact on a given plant system, as described e. g. in /LIN 07/. A systematic approach to map a hazard impact on a plant system can be accomplished by compiling information about

- those SSCs identified to be unavailable due to the impact resulting from the specific hazard,
- hazard related failure dependencies in case of failures induced by hazards, and

- IEs induced by hazards as deduced from the expected plant response to the hazard impact.

Besides the time-consuming task of compiling hazard impact data, one important challenge arises from applying the multitude of required changes on the corresponding PSA plant model. Here, only those modifications will be considered that comprise the extension of FTs with additional BEs or with topological similar sub-FTs as illustrated in Fig. 2.2. Hence, in the following the term HPSA solely refers to the aspect of hazard induced failures of SSCs by modifying the respective FT topologies. The need to apply this vast amount of modelling tasks initially motivated the development of (py)RiskRobot as a software tool to automatically modify topological structures within existing Level 1 PSA plant models as addressed in detail in Chapter 3.

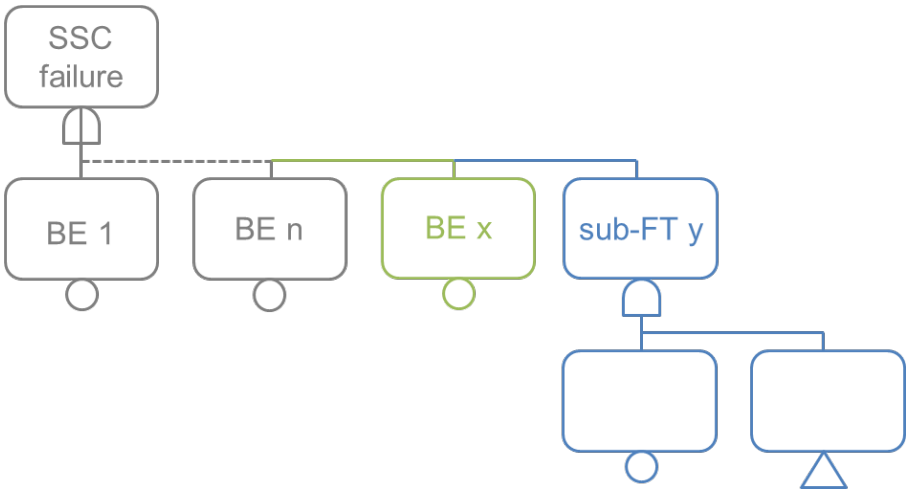


Fig. 2.2 Basic types of FT extensions through an additional BE (green) or additional sub-FT (blue) to the unavailability of a given SSC

2.2.1 Discretisation of Hazard Impacts in Hazard Compartments

A general approach to map a specific hazard impact on a complex plant system offers the identification of relevant compartments being differently affected by the hazard. To each compartment a set of SSCs important to safety is assigned within the given Level 1 PSA plant model. The assumption for such a hazard compartment (HC) is based on the idea that all SSCs assigned to this HC are jointly and equally affected in the same manner by the impact from the considered hazard. In case a given SSC behaves differently from others assigned to the same HC, a new HC needs to be generated to derive a consistent modelling of the additional failure causes of the SSC for assuring a meaningful analysis. Hence, all SSCs important to safety affected by a given hazard can be assigned

to a disjunct set of HCs with potential mutual interrelations of potential directional dependencies as illustrated in Fig. 2.3. The dependencies between HCs indicate the magnitude and directionality of the hazard impact propagation between such compartments. Consequently, the hazard impact can be integrated in a PSA plant model by extending the FTs of the SSC failures with additional, optional causes for each hazard being considered.

The partitioning of the plant system into HCs may vary for different hazards and cannot be applied to the entire spectrum of individual and combined hazards. For instance, the compartments representative for a fire hazard may significantly differ from those for a hydrological (e. g. internal flooding) hazard. The building partitioning into fire compartments (definition see /IAE 20/) in case of a fire hazard may be strongly affected by potential fire propagation between the compartments. In contrary, in case of a hydrological hazard the geodetic height may be a key concern in the partitioning process for generating flooding compartments. Consequently, a set of compartments derived for a specific hazard is in general defined particularly with respect to the impact by the respective hazard or hazard combination.

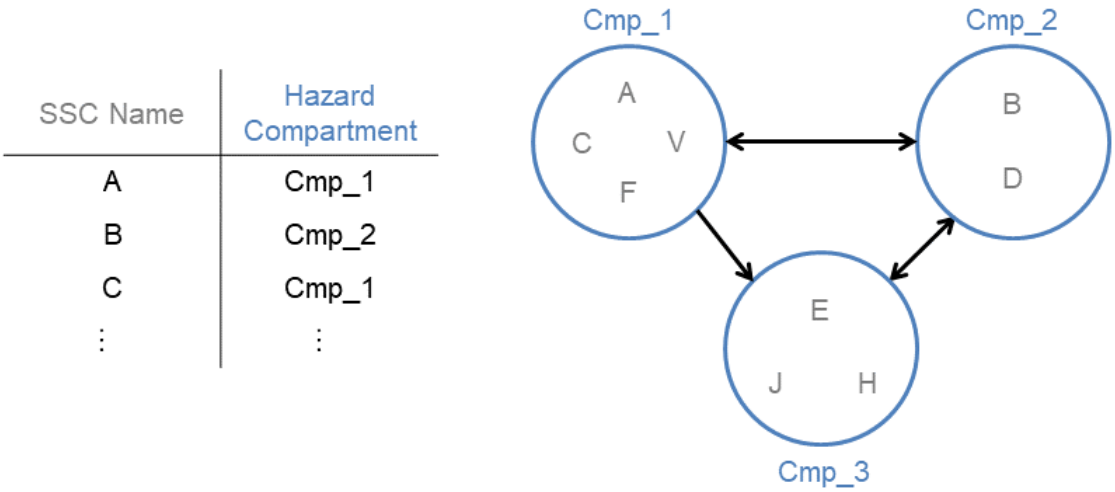


Fig. 2.3 Mapping SSCs affected differently by a hazard impact to disjunct hazard compartments, with mutual interrelations of directional dependencies

The most basic assumption for a HC is to consider all SSCs assigned to a specific HC as failed due the hazard impact independent of any other HC. For instance, all SSCs assigned to a given HC fail jointly as soon as an internal fire occurs in the specific HC as analysed in /HER 15/. By assuming fire propagation between the HCs a mutual dependency is introduced in the HC mapping indicating the possibility of fire propagation between neighbouring HCs and the possible paths of the fire propagation by directed links

between these HCs as illustrated in Fig. 2.3 and analysed in /BER 16/. The graphical representation of these complex hazard impact information indicates that it is useful to understand the compartment dependency patterns of a specific hazard impact as network graphs as described in Chapter 4.

2.2.2 Integration of Hazard Impacts

The integration of a hazard impact in an existing Level 1 PSA plant model can therefore be accomplished by mapping the HCs as additional failure causes to each FT of the assigned SSCs. Depending on the hazard and the considered hazard modelling depth, the extension of the respective Level 1 PSA plant model towards a HPSA model is a laborious modelling task. The resulting multitude of required FT modifications emphasises the need for automatization of redundant and systematic topological modifications as provided, e. g. via the agent-based software pyRiskRobot developed by GRS. The automated hazard integration in FT topologies using pyRiskRobot has been studied for fire propagation in case of a plant internal fire in /BER 16/ and for multiple external flooding scenarios in /BER 17/ (cf. Chapter 3).

2.3 Combination of Hazard Impacts

Besides the individually induced single hazards, the consideration of multiple hazards in terms of credible combinations of related as well as independent hazards (cf. /IAE 20/) remains an important modelling challenge. In principle, combinations of independent hazards can be accomplished by the rigorous automated integration of all hazard impacts relevant to a given plant system. However, the modelling complexity of the PSA plant model is challenged by the vast amount of FT modifications required. To attenuate the resulting increase in modelling complexity, the International Atomic Energy Agency (IAEA) has developed the fault sequence analysis method (FSA) as a systematic approach to investigate the impact of extreme events for a wide range and credible combinations of independent hazards /KUZ 11/. The approach has been extended to the Extreme Event Analyzer (EEA) based on the PSA Software RiskSpectrum® /KUM 16/. However, the FSA approach relies on an at least partly adapted HPSA model and captures only combinations of events occurring by chance independently of each other simultaneously (that is one during the mission time of the other) jointly impacting the plant system.

Basically, the FSA approach analyses combinations of unrelated events occurring independently of each other at the same time and jointly impacting a plant system. The approach cannot explicitly consider related hazards since it requires a comprehensive understanding of the hazard interrelations and the corresponding invasive modifications of the FT topologies within the Level 1 PSA. The extended FSA approach EEA is directly applied on a HPSA model in order to dynamically associate susceptibility values indicating the occurrence and magnitude of a specific hazard impact. Consequently, the approach indirectly relies on an efficient strategy for modifying FTs in order to integrate the various hazard impacts of interest in an existing PSA plant model. Given an efficient modelling strategy and the hazard impact data necessary to integrate and specify different hazard impacts, the challenge of PSA model complexity basically remains unchanged. Thus, the automated and flexible FT modification depicts a key proficiency in enhancing Level 1 PSA plant models towards models for HPSA. Moreover, the network-based analysis of HC dependency patterns prior to the automated integration of the hazard impact offers a promising approach to address combinations of the multiple hazard impacts within a Level 1 PSA as discussed in Chapter 5.

3 Automated Integration of Hazard Impacts

The GRS experience gained from conducting as well as reviewing Level 1 PSA for German NPPs carried out e. g. in the frame of periodic safety reviews has identified important aspects for enhancing risk assessment methods. These aspects are related to extensions of the PSA plant model with respect to a systematic risk aggregation from the variety of hazards as well as to the level of detail needed in the PSA plant model. This is particularly important for a systematic consideration of the complete spectrum of events from site and plant specific individual as well as combined hazards for all plant operational states. Moreover, such an aggregation of risks needs also to consider various multi-unit and/or multi-source aspects (cf. /NEA 20/). Similar insights were derived from the GRS precursor analyses of the operating experience from German NPPs and from related international activities in the field of risk-based precursor analysis /BAB 09/ and /BAB 16/.

The appropriate consideration of a hazard impact on an NPP with the aim to enhance the Level 1 PSA plant model towards a HPSA model requires a multitude of FT modifications. To efficiently and systematically integrate a specific hazard impact in existing PSA plant models, GRS has developed the software tool pyRiskRobot as an approach to modify complex FT topologies in an automated and traceable manner /BER 17a/. The set of basic modelling operations derived fosters more complex and advanced modelling strategies. For instance, by automatically duplicating complete FT topologies across multiple transfer gates, plant sub-systems characterised by high redundancy and multiple interconnections can be directly reproduced within a Level 1 PSA plant model.

In the following, the modelling tool pyRiskRobot is outlined in more detail based on its current implementation in tandem with the PSA software RiskSpectrum®. The interpretation of pyRiskRobot as an agent-based concept is discussed to emphasise the intended design as a general application programming interface (API) irrespective of the employed PSA software. In order to understand how the set of basic modelling operations developed fosters a broad spectrum of FT modelling options, the basic as well as advanced FT operations are described.

3.1 Implementation Strategy of pyRiskRobot

Regardless of the specific implementation of a PSA plant model via a particular PSA software, certain aspects need to be considered with respect to the aim of an automated and reproducible modification approach. These general requirements arise mainly from

the fact that a realistic Level 1 PSA plant model comprises a vast amount of information about each component and its manifold assignments within the model's FT topologies. As discussed in /HER 12/, the design of an automated modification approach should provide the following functionalities:

- trace modifications by date and user identification number (ID),
- process plain data assigned with topological information, i. e. extend FTs for individual BEs or sub-FTs,
- perform combinatory tasks, e. g. labelling or permutation, and
- compare complete PSA plant models in order to identify the applied changes.

All aspects aim on reducing the manual work by the development of an appropriate computational approach such that the modifications are less prone to manual errors. Hence, the ability to automatically compare complete PSA plant models in order to monitor the applied changes is of paramount importance. For this purpose, the GRS tool CmpFT (Compare FTs, introduced in /HER 11/) provides an efficient approach for visualizing each modification relative to the original PSA plant model. The remaining aspects listed above were already addressed by the modelling tool (py)RiskRobot, introduced in /HER 12/ as a ruby-based version RiskRobot and extended in /BER 17a/ to its current python-based version pyRiskRobot. To understand the interplay of pyRiskRobot and the electronic PSA plant model employed, the basic components and general workflow of a pyRiskRobot application are described based on Fig. 3.1.

In the current version of pyRiskRobot, the implementation in the Level 1 PSA plant model is realised by the PSA software RiskSpectrum® (green in Fig. 3.1). The model development and the analysis process are performed by the PSA analyst solely within the graphical user interface (GUI) provided. The information content of a Level 1 PSA plant model, consisting basically of plain data (i. e. BEs assigned with properties) and the topological information (i. e. the relational mapping of BEs within a conjoint FT structure embedded in an ET structure) need to be stored appropriately and efficiently. In case of RiskSpectrum® the information is organised, stored and accessed through a Microsoft® SQL Server (MSSQL) database (arrow (1) in Fig. 3.1). In general, the PSA software also allows to import and export suitable data content, e. g. lists of BE or FT labels with potential meta-information, to be further processed within the PSA plant model (arrow (2) in Fig. 3.1).

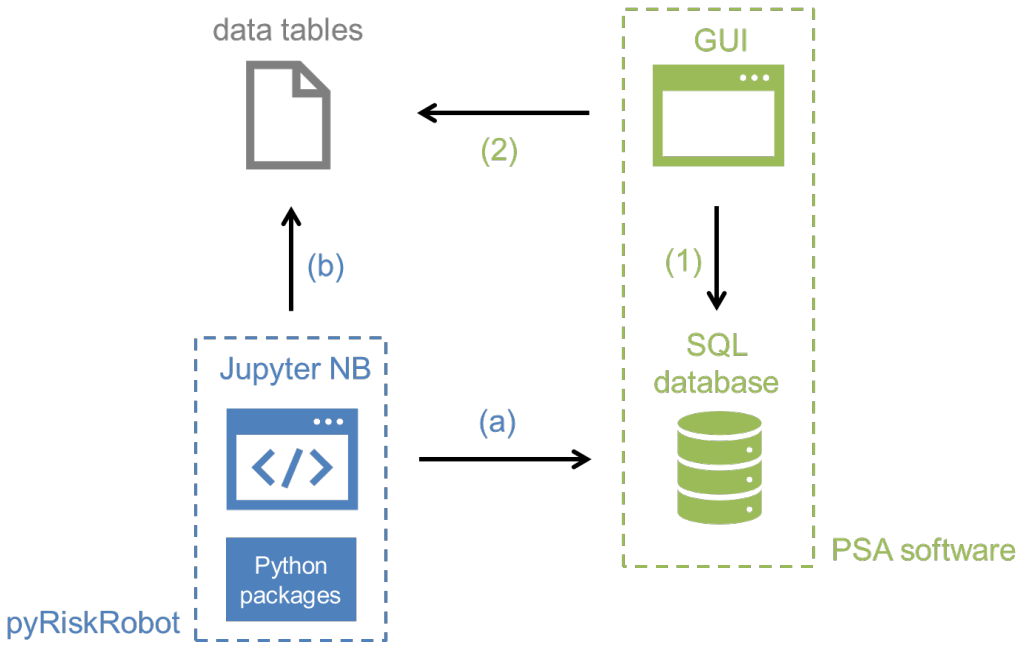


Fig. 3.1 Basic scheme and components of a pyRiskRobot application (blue) to a PSA plant model (green), given additional data for the modelling process (grey)

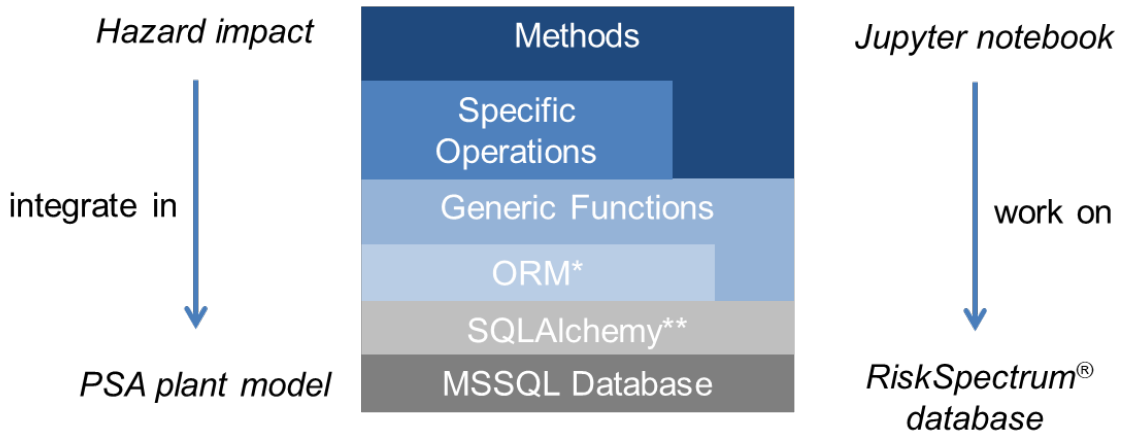
To accomplish the automated modification of FT topologies, pyRiskRobot directly operates on the SQL database, i. e. the PSA plant model, of the PSA Software employed. The application of pyRiskRobot is mainly performed by Jupyter notebooks (NB) based on imported python packages containing the developed method packages and implemented utilities of the pyRiskRobot approach (blue in Fig. 3.1). By using the python library SQLAlchemy /BAY 12/ pyRiskRobot establishes a connection to the MSSQL database of the corresponding Level 1 PSA plant model (arrow (a) in Fig. 3.1.). For tracing the entire modifications applied to the database, each session and change performed is carried out under the username *pyRiskRobot*. Moreover, the review and approval information of all PSA data thereby modified is deleted. Dependent on the modelling task, pyRiskRobot also allows to import and export data from other sources, e. g. lists of BE or FT labels with potential meta-information from e. g. MS EXCEL® files, via utilities based on the python library PyTables /PYT 20/ to be further processed within the Jupyter NB environment (arrow (b) in Fig. 3.1.).

3.2 Agent-Based Concept of pyRiskRobot

The guiding principle in the development of pyRiskRobot is the design of a software agent that acts for a user in a relationship of agency. Software agents (simply referred to as agents) are commonly known as bots, derived from the term robot. Note that the

name pyRiskRobot already encompasses the connotation of an agent-based approach to perform FT modifications in an automated manner on behalf of the PSA modeler aiming to evaluate risks of a complex technical system. In this context, the term ‘agent-based concept’ characterises a complex software entity capable of acting with a certain degree of autonomy in order to accomplish tasks on behalf of the analyst.

The pursued implementation strategy of pyRiskRobot is intended to develop a general application programming interface (API) irrespective of the PSA software employed as the necessary prerequisite for an agent-based concept (cf. arrow (b) in Fig. 3.1.). Based on object-oriented programming the general methodological functionalities are consequently separated from the access to and operation on the SQL database. The main abstraction layers used for the implementation of pyRiskRobot are shown in Fig. 3.2 and mirror the strategy to separate the FT modification methods (referred to as topological operations) from the database specific operations. For instance, all SQL commands necessary to connect, disconnect and copy the database of a PSA plant model remain enclosed in the MSSQLDB class. Hence, pyRiskRobot is designed to be used in electronic PSA plant models of different software, given a stable and dynamic interface to the PSA database employed.



*object relational mapping

**SQL commands

Fig. 3.2 Software layer diagram of pyRiskRobot for the automated integration of hazard impacts in a Level 1 PSA plant model, i. e. for performing modelling operations on the PSA software database

Based on the python library SQLAlchemy, object relational mapping (ORM) is used as data mapping pattern, such that classes can be mapped to the database in multiple ways. Consequently, the object model and database scheme are rigorously decoupled and can be further developed. By reformulating the object relational mapping of the database within the ORM class, the basic components used to jointly describe a FT can be derived as obvious class objects: events, FT nodes and FTs. For tracing the modifications applied within the database the class object 'User' is derived. Thus, the basic functionalities of requesting, adding and removing BE and FT objects from the database are formulated within the ORM class as object relations by means of python objects. Based on the API developed, the topological operations to generate, modify or duplicate components of FTs or sub-FTs can now be defined by classes representing the spectrum of basic operations utilizable by pyRiskRobot.

3.2.1 Generalised Tree Graphs

Prior to the description of the possible topological operations of pyRiskRobot, the formulation of a generic tree graph is introduced in Fig. 3.3. The aim is to provide a consistent and generic terminology capable to express all aspects of topological operations made available and applicable by pyRiskRobot.

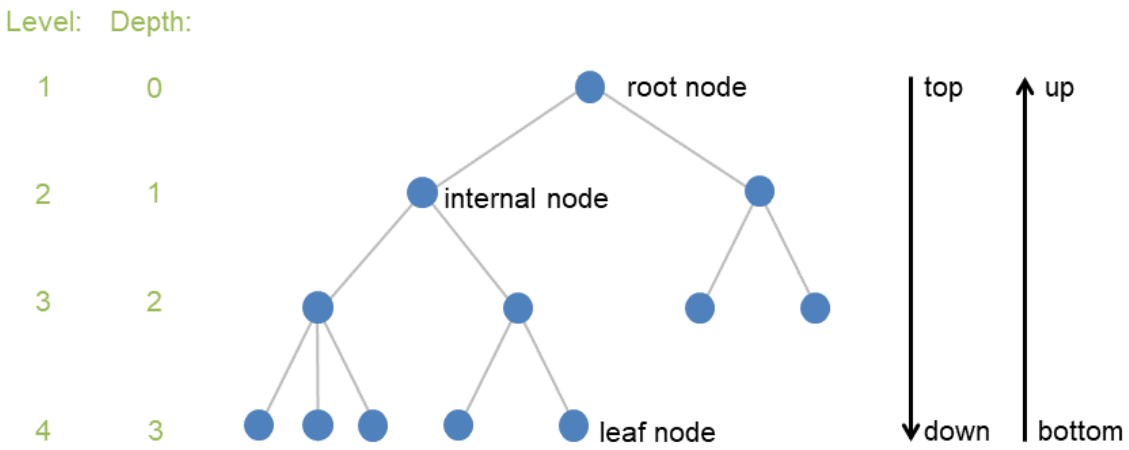


Fig. 3.3 Generic tree graph composed of the basic element nodes (blue circles) and edges (grey lines) indicating the directions top-down, i. e. from root to leaves, and bottom-up, i. e. from leaves to root

In general terms, a FT depicts a specific type of a tree topology corresponding to an acyclic, directed graph, where any two nodes are connected by one and only one edge. Based on a generic tree graph, the FT elements BEs and gates are interpreted as nodes (blue circles in Fig. 3.3) and the relative arrangement and logic combination of FT ele-

ments are interpreted as edges (grey lines in Fig. 3.3). All elements and their explicit arrangement jointly determine the topology of the tree. Since the graph is directed one distinguishes between the two directions top-down and bottom-up. The top element of a contiguous tree graph is referred to as the root node, whereas the bottom elements are referred to as leaf nodes. The depth of a tree graph indicates the maximum number of edges between a leaf node and the root node. Similar to the property depth, the property level can be defined as an indicator for the distance of a considered node to the root node. The simplified interpretation can be further generalised by means of a tree of FTs, that is a tree graph with each node representing a complete FT graph.

3.2.2 Basic Operations on Fault Trees

Based on the pyRiskRobot API developed, a set of basic topological operations can be performed directly within the PSA database, i. e. within the PSA plant model, as illustrated in Fig. 3.4. The modelling tasks can be directly scripted within a Jupyter NB and iteratively applied to the PSA plant model. Another more sustainable strategy offers preparing complex redundant modelling tasks as conjoint topological features that can be jointly processed by pyRiskRobot. Both strategies require labelling schemes assigned to each modelling task or feature group. In order to ensure a stable and efficient workflow of the automated FT modelling, regular consistency checks between the modelling tasks and the Level 1 PSA plant model are required. Potential inconsistencies can occur due to non-unique labelling schemes or non-logical assignment of element types (i. e. BE or gate types). By providing pyRiskRobot with a continuously growing set of strategies on how to behave in case of specific inconsistencies, the realisation of pyRiskRobot as an agent-based concept can be gradually pursued during the ongoing development process.

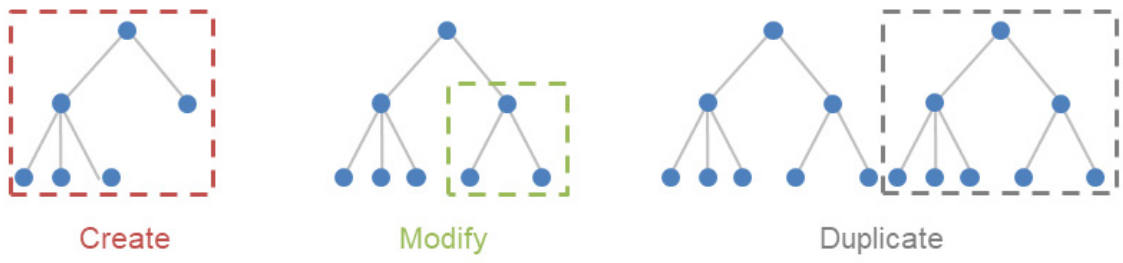


Fig. 3.4 Set of basic topological operations on FTs provided by pyRiskRobot

Generation of New Fault Trees

The generation of new FTs can in principle be carried out independently from the remaining Level 1 PSA plant model, given that the employed FT and FT element labels are not conflicting with entries elsewhere in the PSA plant model. In case existing element types and labels are consistently used during the generation process, the generated FT can be constructed with elements from other FTs. Moreover, the top element of the FT generated may be referenced through a transfer gate to a leaf node of one or multiple different FTs. Thus, the generated FTs can be integrated in the existing PSA plant model topology.

Note, special caution is needed in case of inconsistent labelling schemes. Since a SQL database does not provide any active counter measures for avoiding inconsistent labelling of its entries, the inconsistency generally leads to an irreversible corruption of the database.

Modification of Existing Fault Trees

The modification of existing FTs requires a consistent labelling scheme for the newly created elements or efficient re-labelling scheme for rearranged elements. An existing FT can be extended for sub-topologies by integrating new BEs based on existing gates, by combining new BEs via new gates, or by relating new FTs referenced via valid transfer gates. The successive FT extension by multiple pyRiskRobot sessions corroborates the need for flexible, dynamic and descriptive (re)labelling schemes. For instance, it is often reasonable to extend FTs for an individual hazard aspect justifying the practice of an auto-generated labelling scheme based on plain task counters without further description. In case pyRiskRobot is repeatedly applied to the PSA plant model for extending FTs for multiple hazards, it is important that the labelling schemes applied are unambiguous to avoid deleting already existing hazard impact modifications. An application example for the extensive modification of existing FTs by means of pyRiskRobot has been studied for the automated integration of a plant internal fire in an exemplary NPP /BER 16/ propagating.

Duplication of Given Fault Trees

The duplication of a given (sub-)FT is carried out based on a harbour FT provided and a respective anchor FT element. Given the initial anchor element for the duplication operation, pyRiskRobot can autonomously recompose the relevant descendent FT topology

from the anchor element top-down to all according leaf elements of the FT directly from the database. Based on a predefined integration strategy pyRiskRobot re-creates and re-integrates the according FT topology in the Level 1 PSA plant model. The definition of a generic and automated labelling scheme for the re-created elements according to the labels of the original topology can be complicated and in general scales with the complexity of the considered FT topology. In case of duplicating a newly created topology, the interplay between pyRiskRobot and the PSA software can be beneficially combined. The GUI of the PSA software can be used to generate a reference (sub-)FT in compliance with an adequately designed labelling scheme and pyRiskRobot can be used to recompose the reference topology directly from the SQL database. An application example for a nested duplication of FT topologies via pyRiskRobot has been studied for the automated integration of multiple external flooding scenarios in the Level 1 PSA plant model for a German reference NPP /BER 17/.

By combination, the basic topological operations derived foster a broad spectrum of FT modelling options that can be organised as more complex topological features. The preparation of a topological feature is reasonable in case it represents a redundant modelling task reoccurring during the modelling process. Due to the increasing complexity of combined topological operations it is of great importance to provide pyRiskRobot with an indicator for the progress of a modelling task in order to accomplish a suitable interruption property. An interruption property aims to stop the execution of the operation at an intermediate stage of the modelling process, meanwhile avoiding the corruption of the database. Given an interruption property and indicators for the accomplished modelling progress, pyRiskRobot can in principle resume the modelling process even after an interruption and proceed with the remaining tasks of the topological operation. The development of an interruption property in combination with preventive security checks aims to increase the autonomous behaviour of pyRiskRobot towards an agent-based concept.

3.2.3 Interactive Operations Across Multiple Fault Trees

Besides the organisation and preparation of topological features, the flexibility of the pyRiskRobot API enables to interactively and dynamically perform more advanced modelling tasks across multiple FTs. For instance, for extending an existing Level 1 PSA plant model towards a multiple reactor unit (multi-unit) PSA plant model, it may be reasonable to duplicate a complete redundant train already implemented within the PSA topology. Based on a root FT identified, the complete interrelated topology consisting of

all descendent FTs can be principally derived from an autonomous top-down search of pyRiskRobot. The result of such a top-down search is presented as a tree of descendent FTs in Fig. 3.5. As explained previously, in the tree of FTs each node refers to a complete FT consisting of multiple FT elements. For clarity, note that not the FT labels are shown at each tree node, but the automatically generated FT numbers inherently allocated at construction within the SQL database are used as identifiers. To visualise and analyse graph topologies, such as tree graphs, pyRiskRobot has been extended by a graph analysis module based on the python package NetworkX /HAG 08/.

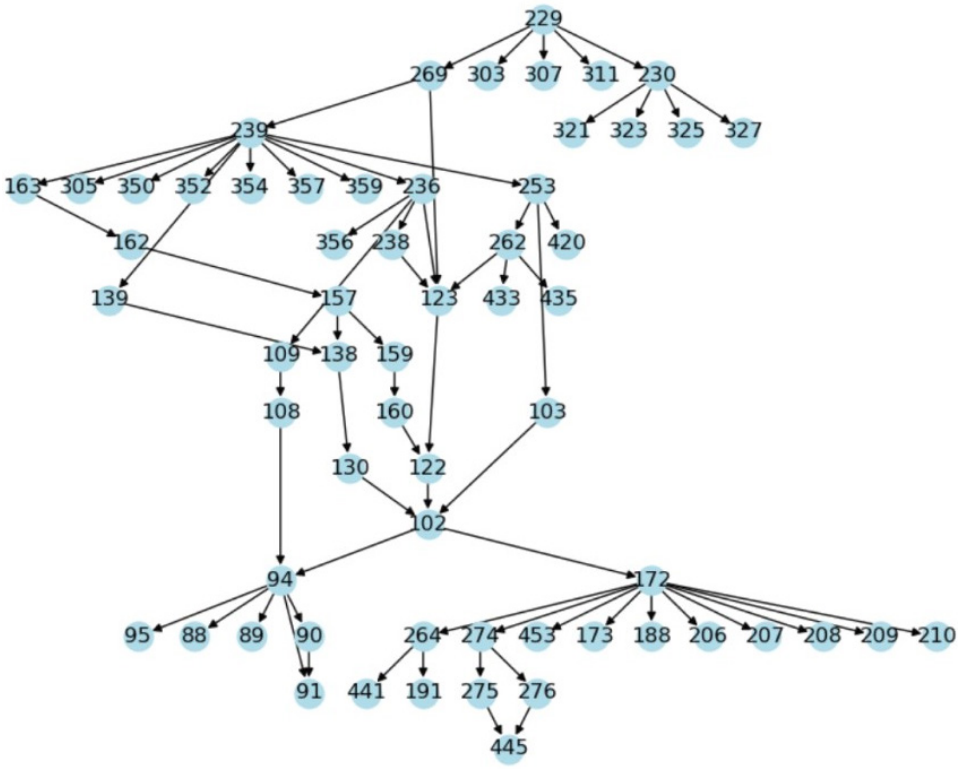


Fig. 3.5 Automatically recomposed tree of FTs representing the interrelated topology of descending FTs from the root FT (229) as derived by pyRiskRobot from a given PSA plant model

As in the top-down search for all descendent FTs, pyRiskRobot can in principle re-create all FTs and re-integrate them accordingly via valid transfer gates within one duplication operation. However, this straight-forward concept fails in the context of continuously developed and advanced PSA plant models, commonly implemented by several PSA analysts. The labelling of continuously, manually developed PSA plant models is often not sufficiently consistent within individual FTs and particularly not across interconnected FTs. Hence, the labels within a FT cannot be mapped to a systematic labelling scheme. The amount and complexity of the descendent FT makes it neither suitable nor accepta-

ble to apply a brute-force auto-generated re-labelling scheme, with the consequence of losing the descriptive meta-information provided in the labels and text boxes of each FT element. Another issue arises due to potentially large tree depths as defined in Fig. 3.3. For instance, Fig. 3.5 shows a relatively small tree of FTs of depth 13 which hampers the continuous execution of the duplication process by pyRiskRobot. Due to the amount and complexity of the jointly processed modelling task, the risk of run time errors in pyRiskRobot increases requiring a suitable strategy to decompose the topological operation into smaller and less complex modelling tasks.

	229	230	269	303	307	311
0	P-JNA20-NK	P-JNA20-NK100	V-JNA20-NK	XJNA20AP001-STN	XJNA20BC002-KWA	XJNA20AP001-BVR2
1	P-JNA20-NK	P-JNA20-NK100	V-JNA20-NK	XJNA20AP001-STN	XJNA20BC002-KWA	XJNA20AP001-BVR2
2	@P-JNA20-NK10	JNA20AA001RÜ	ET-BMB	JNA20AP001-STN	@XJNA10/20BC2KWA60	JNA20AP001-FN
3	@P-JNA20-NK21	@P-JNA20-NK114	@V-JNA.0-NK15	@XJNA10/20AP1STN60	&JNABC002KWA4V4	@XJNA10/2AP1BVR260
4	@P-JNA20-NK24	JNA22AA001RÜ	P-KAA20-NK	&JNAAP001STN4V4	@XJNA10/20BC2KWA70	&JNAAP1BV R24V4
5	P-JNA20-NK100	JNA22AA001SNM	NaN	@XJNA10/20AP1STN70	&JNABC002KWA123	@XJNA10/2AP1BVR270
6	V-JNA20-NK	JNG21AA001RÜ	NaN	&JNAAP001STN123	&JNABC002KWA124	&JNAAP1BV R2123
7	JNP20AA001RÜ	JNG22AA001RÜ	NaN	&JNAAP001STN124	&JNABC002KWA234	&JNAAP1BV R2124
8	@P-JNA20-NK33	@P-JNA20-NK124	NaN	&JNAAP001STN234	@XJNA10/20BC2KWA80	&JNAAP1BV R2234
9	@P-JNA20-NK34	JNA20AP002STN	NaN	@XJNA10/20AP1STN80	&JNABC002KWA12	@XJNA10/2AP1BVR280
10	JNP20AA002RÜ	@P-JNA20-NK134	NaN	&JNAAP001STN12	&JNABC002KWA23	&JNAAP1BV R212
11	@P-JNA20-NK43	JNA24AA001RÜ	NaN	&JNAAP001STN23	&JNABC002KWA24	&JNAAP1BV R223
12	@P-JNA20-NK44	JNA24AA002RÜ	NaN	&JNAAP001STN24	NaN	&JNAAP1BV R224
13	JNA20AA003-SNU	@P-JNA20-NK144	NaN	NaN	NaN	NaN
14	JNA20AA003RÜ	JNA20AA050-SN	NaN	NaN	NaN	NaN
15	@P-JNA20-NK53	JNA20AA050RÜ	NaN	NaN	NaN	NaN
16	@P-JNA20-NK54	P-MESSUNG<8BAR R2	NaN	NaN	NaN	NaN
17	JNA20AA017RÜ	@P-JNA20-NK154	NaN	NaN	NaN	NaN
18	KAA24CF001<150KG	JNA20AA005RÜ	NaN	NaN	NaN	NaN
19	@P-JNA20-NK64	JNA20AA006RÜ	NaN	NaN	NaN	NaN
20	XJNA20AP001-STN	JNA20AA051RÜ	NaN	NaN	NaN	NaN
21	XJNA20BC002-KWA	@P-JNA20-NK164	NaN	NaN	NaN	NaN
22	XJNA20AP001-BVR2	XJNA22AA002ÖNM	NaN	NaN	NaN	NaN
23	NaN	JNA22AA002RÜ	NaN	NaN	NaN	NaN
24	NaN	JNA22AA004RÜ	NaN	NaN	NaN	NaN
25	NaN	@P-JNA20-NK174	NaN	NaN	NaN	NaN
26	NaN	XJNA22AA004ÖN	NaN	NaN	NaN	NaN
27	NaN	XJNA22AA005ÖN	NaN	NaN	NaN	NaN
28	NaN	JNA22AA005RÜ	NaN	NaN	NaN	NaN
29	NaN	XJNA22AA003ÖN	NaN	NaN	NaN	NaN

Fig. 3.6 Label list of all FT elements for each FT of tree levels 1 (root FT) and 2 (first descendent FTs) of the tree graph in Fig. 3.5 as provided by pyRiskRobot

Note, the table presented in Fig. 3.6 is the direct output of the pyRiskRobot query within the Jupyter NB. The handling of structured data within the Jupyter NB is developed

based on generic data frames provided by the data science python package pandas /PAN 20/. The NaN entries (i. e. numeric data type *Not a Number*) shown in Fig. 3.6. are simply used to fill the data frame to obtain data arrays (i. e. table columns) of similar size. Given the automatically derived tabular data formatting, the original FT element labels can be directly inspected as well as the relabelling schemes developed can be directly applied and tested within the Jupyter NB. Thus, a suitable relabelling scheme can be developed per tree level or at least per FT. In case an automated relabelling scheme is not feasible to accomplish alternative labels can be individually provided for the respective FT elements.

Since in general not all FT elements need to be duplicated, a practical convention determines that a FT element will only be duplicated if a new label is provided, i. e. either automatically generated or individually specified. Otherwise, the original FT element is re-integrated within the duplicated FT topology. Provided a consistent and complete relabelling scheme, pyRiskRobot iteratively duplicates level by level all FTs. By introducing an interruption property, pyRiskRobot is able to pause, proceed and terminate the topological operation at each transfer gate of a FT. The behaviour of pyRiskRobot derived can be controlled from outside through rules that enforce the interruption of the current modelling task at the FT margins or accept the proceeding of the current modelling task beyond the FT margins.

The implemented interruption property is particularly useful for the robust (in the sense of the database access) and dynamic (in the sense of the modelling process) application of pyRiskRobot in the context of interactive Jupyter NBs. The interruption property in combination with progress indicators of the topological operation and preventive security checks further increases the ability of pyRiskRobot to solve increasingly complex modelling tasks directly and without a predetermined execution order. Thus, the autonomous behaviour of pyRiskRobot is further developed towards an agent-based concept.

4 Network-Based Analysis of Hazard Impacts

Extending Level 1 PSA plant models towards HPSA models can be efficiently accomplished based on the automated execution of topological operations via the agent-based software pyRiskRobot (cf. Chapter 3). Even if the required FT modifications involve laborious and complex modelling tasks, the automated integration allows to map the HCs as additional hazard induced failure causes to each FT of the assigned SSCs (cf. Chapter 2.2). The automated hazard integration in FT topologies using pyRiskRobot has been demonstrated for the propagation of a plant internal fire in /BER 16/ and for multiple external flooding scenarios in /BER 17/. However, the HC data characterising the hazard impact on the complex technical system is often complex itself and potentially contains mutual, directed and weighted dependency patterns. For a comprehensive understanding of the mapped hazard impact and for developing strategies to optimally incorporate multiple hazard impacts in the PSA, the investigation of the structure and properties of the mapped HC dependencies promises valuable insights prior to their integration in the Level 1 PSA plant model.

Network graphs offer an intuitive approach to organise, visualise and analyse manifold relations between multiple objects. By representing HCs and their mutual dependencies as networks, the encoded hazard specific impact patterns can be analysed for statistical global and local network properties. The use of such network measures in the PSA context has already been discussed in /HIB 16/ and /RIF 18/ by associating centrality measures of complex networks describing a considered accident scenario to the risk increase factor calculated by a corresponding PSA plant model. For clarity, it is important to distinguish between the major goals of network analysis /NEW 10/:

- characterisation of the network structure,
- modelling of the network structure, and
- studying the effects of the network structure on the system behaviour.

The first two aspects basically refer to the aim of mapping an ET to a complex network to derive network measures directly comparable to the risk metrics of a corresponding PSA plant model. Different to this partial network substitution of a PSA plant model, the network-based analysis of hazard impacts aims at modelling and characterising the network structure of HCs to objectively compare different HC networks and to potentially

reduce an HC network due to statistical features prior to their eventual integration in a PSA plant model.

In this chapter, the representation of hazard impact data through network graphs is outlined as introduced in /BER 19/. The formulation of network graphs and the definition of descriptive measures are explained based on a network analysis of the hazard impact by a plant internal fire on an exemplary NPP. For developing a network-based approach as a prior and facilitating step to generate HPSA models, potential strategies to consider, compare and combine multiple hazards by multiple network representations are discussed.

4.1 Hazard Compartment Dependencies as Network Graphs

Based on the systematic partitioning of the plant system into hazard specific compartments as described in Chapter 2.2.1, the plant specific hazard impact on SSCs important to safety can be mapped to a set of disjunct compartments with mutual dependency patterns between HCs identified. Since the acquirement of the hazard impact information is a protracted process eventually performed by different experts from systems technology, the comprehensive understanding of the hazard impact patterns derived is an important aspect to be considered by the PSA modeler and analyst. A detailed investigation of the structure and properties of the HCs dependencies mapped yields an important in-depth understanding of the hazard impact assumed and modelled for the integration in the Level 1 PSA plant model. The analytical goal is to organise and investigate hazard impact patterns for a complex technical system prior to the mapping to the functional requirements of the safety sub-systems. An intuitive representation of a set and structure of HCs can be achieved by re-formulating the set of HCs and their pairwise dependencies in terms of a network graph as shown in Fig. 4.1.

Hence, the HCs are represented by the nodes of the network and the links connecting them indicate dependency patterns between the compartments, e. g. fire propagation direction and probability. Each hazard impact may be characterised by specific properties, attributes and dependency patterns (directed and/or weighted) based on the available knowledge and information on the considered hazard and technical (sub-) system.

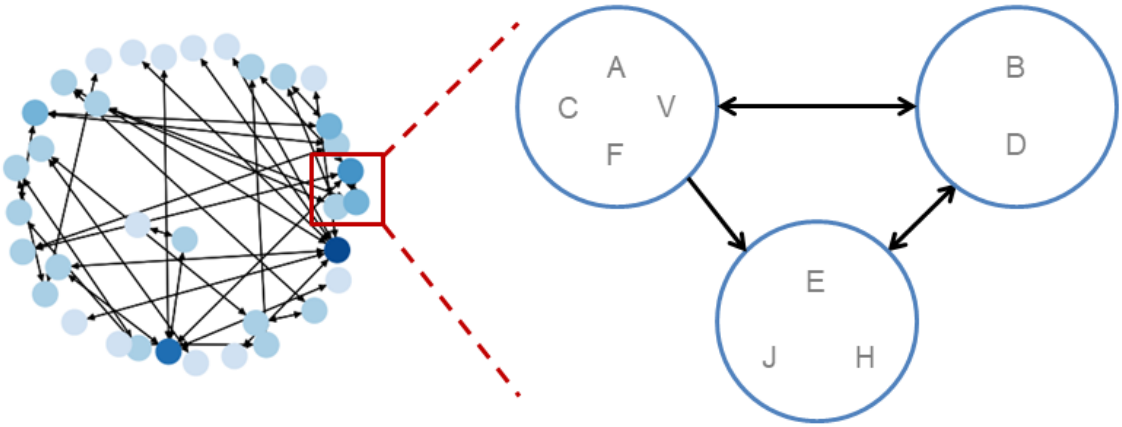


Fig. 4.1 Representation of hazard compartments (HC, blue circles) and their mutual dependencies (black arrows) as a network graph with capital letters indicating the assigned SSCs equally affected by the hazard (cf. Fig. 2.3)

The methodological framework of network graphs offers strategies and techniques to intuitively visualise pairwise, weighted and directed dependencies between HCs and to statistically analyse the HC data for local and global network measures. The network representation approach has been implemented as an additional analysis module in the pyRiskRobot software. The implementation is based on the Python package NetworkX introduced in /HAG 08/ providing the basic methods for the generation, manipulation, and study of the structure, dynamics, and functions of complex networks. In combination with the utilities based on the python package PyTables /PYT 20/ and pandas /PAN 20/ for accessing and processing data tables of different formats, the network analysis module of pyRiskRobot aims to support experts from systems technology in compiling the hazard impact data as well as PSA analysts in conducting a HPSA. Due to the interactive visualisation, investigation and analysis of the HC networks derived within the Jupyter NB environment, the approach can also assist the experts to detect discrepancies or missing data in hazard impact compilations.

4.2 Complex Network Graphs

To capture all hypothetic dependency aspects of a HC set, a realistic graph depicts a directed, weighted network as illustrated for an artificial set of correlated nodes in Fig. 4.2. For clarity, note that different to a tree graph (defined in Chapter 3.2.1) a network graph may contain multiple edges with different properties and directionality between two nodes. Here, the focus is on complex network graphs with potentially bidirec-

tional, weighted edges between two nodes. The aspect of multiple edges between two nodes will be addressed by multidimensional network graphs in Chapter 5.

The term *'complex network'* refers in the context of one HC set to the complexity of the HCs and assigned dependencies, i. e. the number of nodes and edges in the network derived. In graph theory, the term '*complexity'* generally describes various, often more sophisticated aspects of network topologies as discussed e. g. in /KIM 08/ that are beyond the scope of this work. The approach of representing HCs as network graphs primarily aims to investigate the hazard specific, mutual dependencies between identified compartments through visualisation and statistical analysis in order to unravel characteristic patterns of the hazard impact. Hence, the approach yields an exploratory data analysis method to describe the structural properties of the network. From another perspective a constructed network representation can be used to model the dynamics between HCs as a physical process to specify the mutual hazard impact dependencies between compartments, e. g. to estimate transition probabilities. All these aspects corroborate the universal relevance of network-based approaches.

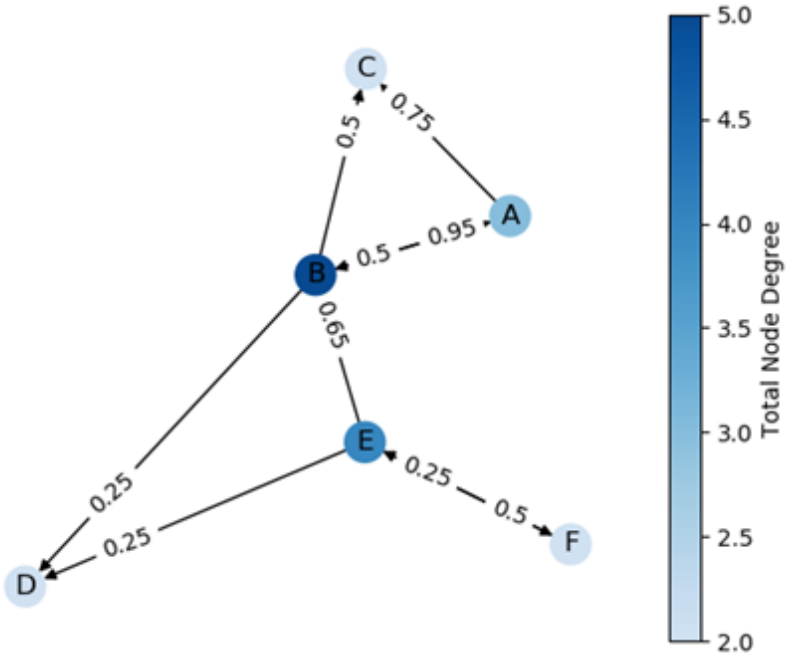


Fig. 4.2 Graphical representation of a directed, weighted network with nodes (A-F) coloured according to the respective total node degree and edges labelled with the assigned weights shifted towards the according direction

The basic definition of a network in terms of a graph G is given by the following formula:

$$G \coloneqq G(V, E, f) \tag{4.1}$$

with $v \in V$ as the set of N nodes (or vertices), $e \in E$ as the set of links (or edges) and $f: E \to V$ as a function mapping each link to an unordered pair of nodes. For directed networks the edges are ordered pairs of nodes and for a weighted network each edge has an associated weight $w: E \to \in \mathbb{R}$ mapping each edge to a real number. The artificial network graph presented in Fig. 4.2. is an example of a directed (indicated by arrows at the corresponding edge ends) and weighted (indicated by numerical values shifted towards the according direction) network topology. The colour of the nodes indicates the total node degree as a local descriptive network measure defined in Eq. (4.4).

The formulation of the network in Eq. (4.1) emphasises the fact that a network can be simply described as unordered or ordered sets of nodes, i. e. edges, potentially assigned with weights. It may as well be useful to provide further information for each node, e. g. technical or physical information that might be of interest for the consideration of another hazard or the combination of hazards. Thus, as a practical implementation strategy, all available information of a HC is assigned to the representing node through a set of descriptive attributes.

4.2.1 Network Visualisation

The dependency patterns of HCs can be visualised either as a network topology (see Fig. 4.2), or as a heat map of the representation matrices, e. g. the adjacency matrix (see Fig. 4.3).
The adjacency matrix of a network is defined by the connection status a_{ij} as

$$a_{ij} = \begin{cases} 1, & \text{if } \langle v_i, v_j \rangle \text{ exits} \\ 0, & \text{otherwise} \end{cases} \tag{4.2}$$

whereas $\langle v_i, v_j \rangle$ refers to the edge between node v_i and node v_j. For weighted and directed networks each edge is assigned with a weight w_{ij} and represented by an ordered pair of nodes. Hence, the connection status is not indicated by 1, but by the according weight w_{ij} and the adjacency matrix can be non-symmetric as illustrated in Fig. 4.3.

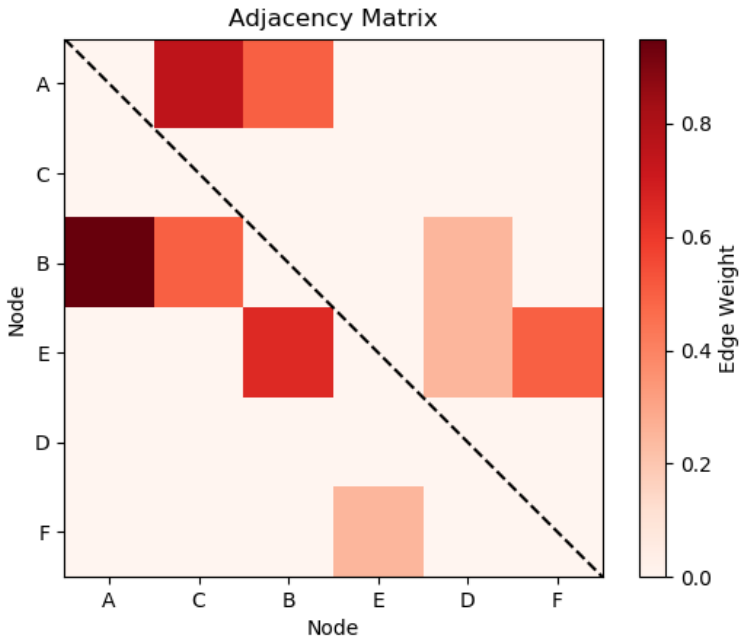


Fig. 4.3 Heat map of the adjacency matrix for the network shown in Fig. 4.2, with the colours indicating the weights of the edges between the nodes and the non-symmetric entries indicating a directed, unbalanced network topology

4.2.2 Network Analysis

To describe and characterise complex networks commonly defined basic metrics and centrality, segregation and resilience measures can be computed /NEW 10/. Thereby, the overall aim is to derive statistical and objective quantities that allow to characterise individual elements of the network and to compare different networks independent of their network size *N*. One of the main objectives in network analysis approaches is the identification of important individual nodes and important node clusters within a network topology. In general, network properties can be described by global and local network measures, each indicating a certain topological aspect, such as individual importance, information flow or connectivity. Moreover, the distributional patterns of local measures are also used to investigate the network characteristics on a global scale.

Global Network Measures

The most general characteristics of a network offers the network density and is given by the ratio of the actual existing edges to all possible edges of the network. In order to investigate structural patterns of the network the topological distance d_{ij} known as shortest path length) between two nodes v_i and v_j are defined as

$$d_{ij} = \sum_{a_{ux} \epsilon g_{i \leftrightarrow j}} a_{ux} \tag{4.3}$$

with the connection status a_{ij} given in Eq. (4.2) and the shortest path g_{jk} between the node pair. The average topological distance can be used as a global characteristic of the network. Another global perspective on the network offers the distribution of topological distances. These measures will be explained in more detail in Chapter 4.3.1.

Local Network Measures

Local measures enable the characterisation of individual elements of a network, such as the importance of a node, through centrality measures. The most basic indicating measure for the centrality of a node depicts the degree k_i of a node as the sum of all edges connected to the node v_i and is defined as

$$k_i = \sum_{j \epsilon N} a_{ij} \tag{4.4}$$

via the connection status a_{ij} given in Eq. (4.2).

The closeness C_i serves as a more descriptive centrality measure and indicates the average topological distance or shortest path length to a node v_i. The closeness is defined as

$$C_i = \frac{N-1}{\sum_{j \in N} d_{ij}}, \qquad \text{for } i \neq j \tag{4.5}$$

via the topological distance d_{ij} and normalised with respect to the number of nodes *N*, respectively the size of the network.

The betweenness B_i serves as another centrality measure and indicates the sum of fractions of all shortest paths that pass through the node v_i. The betweenness is defined as

$$B_i = \frac{1}{(N-1)(N-2)} \cdot \sum_{j,k \epsilon N} \frac{g_{jk|i}}{g_{jk}} \tag{4.6}$$

for $i \neq j,\ i \neq k$ and $j \neq k$, and with g_{jk} as the shortest paths between the nodes v_i and v_k, and $g_{jk|i}$ as the shortest paths between v_j and v_k including the node v_i. The measure is normalised via the number of node pairs excluding v_i. Note, the degree as well as the topological distance can be adapted to directed and weighted edges and thus can the centrality measures.

4.3 Network Representation of Hazard Impacts on an Exemplary Nuclear Power Plant

In order to discuss the defined network measures, a compilation comprising the dependency patterns of an internal fire hazard are represented as HC dependency networks. The database contains information for each building of an exemplary NPP. Thus, for each plant building a network of fire compartments can be derived and investigated. The compilation of this data is an important task that need be achieved by a systems technology expert understanding the complex technical system of interest. The fire compartment networks may provide valuable reference networks, whose topologies may be adapted to map the dependency patterns of another hazard to the plant system, e. g. a plant external hydrological hazard. Note that not only the topology of the dependency networks but also the compartment-component mapping may change with respect to another hazard.

4.3.1 Analysis of a Plant Internal Fire Hazard

As a comprehensive overview of the hazard network analysis results of the main global characteristics for several buildings of an exemplary NPP are summarised in Tab. 4.1.

Tab. 4.1 Characteristic quantities of the fire hazard network analysis for selected buildings of an exemplary NPP

Quantity	Building				
	B01	**B02**	**B03**	**B04**	**B05**
# nodes	342	176	99	18	35
# edges	980	444	269	36	72
density	0.008	0.014	0.028	0.118	0.061
diameter	19	20	12	10	16
$\langle d_{ij} \rangle$	9.44	7.38	5.22	4.24	5.40
$\langle k_i^{\text{in/out}} \rangle$	2.87	2.52	2.72	2.00	2.06

Without the use of interactive visualisation techniques, the presentation of large networks (i. e. $N > 50$) is not very useful. Therefore, we demonstrate the main objectives of the analysis strategy regarding hazard networks for the building B05. The network topology representing the dependency patterns between fire compartments is shown in Fig. 4.4 Each node refers to a fire compartment and is coloured based on its unweighted total degree within the network. Each directed edge refers to possible fire propagation directions and is assigned with the fire propagation probability accordingly.

Comparison of Dependency Networks

As listed in Tab. 4.1, the number of nodes and edges per network graph can be put in relation to each other via the network density indicating how many of the possible edges exist within the topology. The diameter of a network is the shortest distance between the two most distant nodes in the network. The average shortest path length $\langle d_{ij} \rangle$ indicates the efficiency of information flow in a network. The distribution of topological distances as shown in Fig. 4.5 combines both aspects and serves as a statistical description of the basic characteristics of a network.

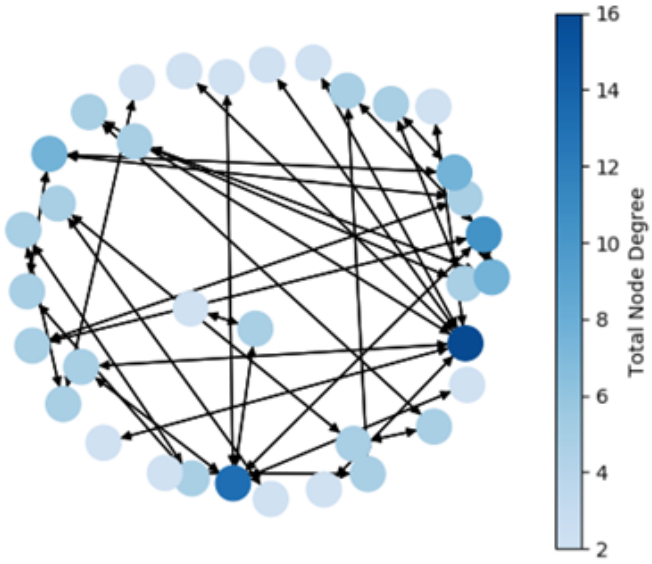


Fig. 4.4 HC dependency network for a plant internal fire in building B05 of the exemplary NPP with the node colour indicating the total degree of a fire compartment and edge arrows indicating the possible direction of the fire propagation

Identification of Important Compartments

Besides the global comparison of complete network topologies, a major concern is the identification of the most important nodes, i. e. HCs, within the network. Since the interpretation of importance within a network may change for each applicational context, a wide spectrum of centrality measures does exist trying to capture various aspects of importance. In Tab. 4.2, the commonly used measures are compared for the four highest rank nodes of the fire hazard network for building B05 of the exemplary NPP. The ranking is carried out with respect to the total degree. Note, the ranking based on other measures differs and is an indicator how differently these measures do interpret importance.

The degree k_i defined in Eq. (4.4) indicates how well a node is connected to all other nodes. The closeness C_i defined in Eq. (4.5) may also be referred to as reciprocal farness. The centrality pattern captured by this measure describes how well information flows from this node to all other nodes (aka information flow). The betweenness B_i defined in Eq. (4.6) indicates the relative number of times a node is present in the shortest paths between two other nodes. The measure indicates how well the information between two nodes flows through a specific node (known as communication flow).

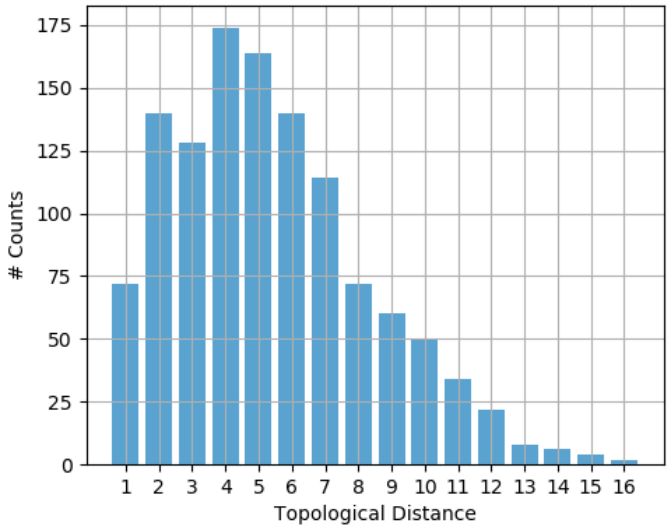


Fig. 4.5 Topological distance distribution of the fire compartment network for building B05 of the exemplary NPP shown in Fig. 4.4

Based on these differences, it can be explained that the ranking of the network nodes may vary, but it also substantiates that the spectrum of centrality measures provides a rich descriptive framework to investigate networks and compare their properties for different hazard patterns.

Tab. 4.2 Comparison of centrality measures for the HCs with the four highest degrees of the fire compartment network for building B05 of the exemplary NPP

Node v_i	Centrality Measure		
	Degree k_i	Closeness C_i	Betweenness B_i
B05-04-02	16	0.241	0.531
B05-03-01	10	0.281	0.617
B05-02-01	8	0.279	0.592
B05-02-04	6	0.252	0.294

Reduction Based on Objective Properties

Next to the importance of individual nodes, i. e. HCs, the investigation of edges, i. e. fire propagation paths, is of further interest. The network topology can be highlighted based on certain conditions, e. g., thresholds, formulated for the attributes assigned to the edges. As shown in Fig. 4.6, the edges of the hazard network can be coloured based on the weights, i. e. fire propagation probabilities, assigned to them. Thus, smaller sub-structures within the network topology can be recognised, as marked by the red rectangle in Fig. 4.6. This sub-structure encloses a group of compartments that are connected by

edges of relatively high weights, i. e. the fire propagation probability. The identification of such sub-topologies may be useful for studying localised hazard domains within the global dependency patterns. Since only a relevant impact on the system may be expected above a specific hazard threshold, it can be as well of interest to reduce the network complexity of the considered HCs accordingly.

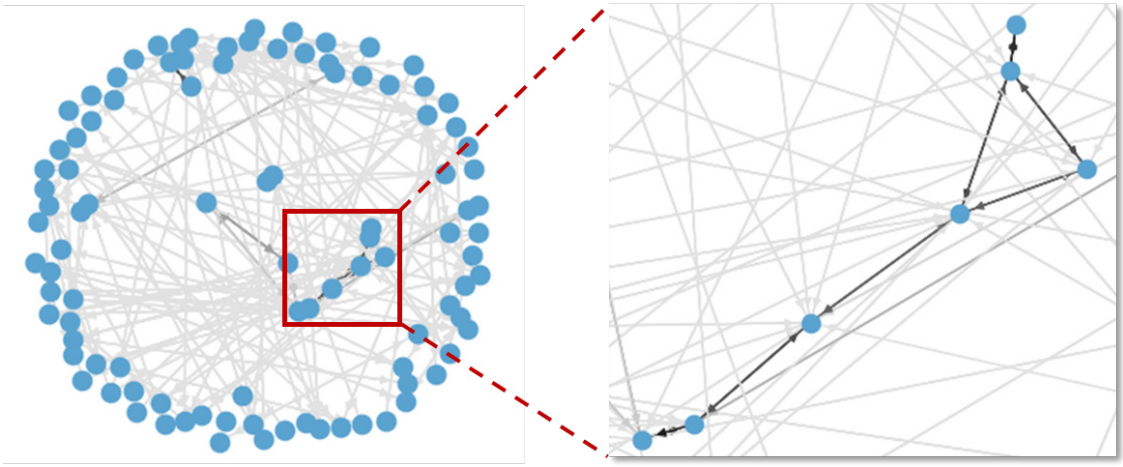


Fig. 4.6 HC dependency network of a plant internal fire for building B03 of the exemplary NPP with edges coloured with respect to assigned weights, emphasizing a sub-topology (red) of relatively high fire propagation probabilities

4.3.2 Extension to Plant External Hydrological Hazards

Even though the detailed impact on technical components of the engineered system is highly dependent on the hazard considered in particular, the insights from the analysis of the fire hazard dependency networks can be used for enhancing and extending dependency patterns for impacts by other hazards, such as an external flooding. The idea arose due to the fact that the networks capture the dependency patterns of hazard compartments, but not the direct system dependency patterns of technical system components. In addition, each hazard compartment requires a hazard specific compartment-component mapping, since different hazards affect different components in a different manner. Hence, the compilation of this information is of fundamental need to re-interpret a hazard dependency network and requires the knowledge and experience of an expert in systems technology.

However, hazard dependency networks developed for a complex technical system may serve as reference topologies guiding the partitioning of the system with respect to other hazards. The basic properties have to be identified, such as the height above ground of components important to safety in case of flooding. Therefore, the expert may decide to refine the distribution of components by further partitioning the dependency patterns into additional HCs. In consequence, the topology of the reference network may be extended or reduced as described in Chapter 5 for the transitions between the layers of a multidimensional network.

4.4 Summary and Discussion

A network-based approach has been introduced to organise, visualise and analyse complex dependency patterns of hazard impacts on complex technical systems such as NPPs. In this approach, the network is composed of HCs as nodes and of edges representing the mutual correlations of the HCs. A strategy has been proposed for reference networks allowing to represent the hazard networks from the perspective of different types of internal as well as external hazards, individual as well as combined ones, for a complex plant system. By demonstrating the network analysis applying the data compilation for a plant internal fire hazard in an exemplary NPP, the spectrum of measures allowing to investigate the network and to compare different network topologies is characterised. The network derived can serve as a reference network topology for elaborating other partitioning schemes reflecting the impact of other hazards on the same complex technical system, such as an external flooding.

The framework of networks potentially provides the flexibility to consider, compare and combine hazard dependency patterns prior to their integration in the actual PSA plant model. Moreover, the approach can be easily adapted to any changes in the complex technical system, as expected e. g. for the decommissioning phase of a NPP. Thus, the approach offers an intuitive way for mapping continuous system changes to the hazard dependency patterns and to study the effect of modifications on the overall hazard dependency patterns.

5 Multidimensional Network Approach for Multiple Hazards

Extending and enhancing Level 1 PSA plant models towards HPSA models can be efficiently accomplished based on the automated execution of topological operations by the agent-based software pyRiskRobot (cf. Chapter 3). The network-based analysis of HC dependency patterns allows to consider and compare individual independent hazard impacts prior to the integration in the actual PSA model (cf. Chapter 4). Based on these approaches, combinations of independent hazard impacts can in principle be accomplished by the rigorous automated integration of all hazard impacts relevant to a given plant system. However, the modelling complexity of the PSA plant model is challenged by the vast amount of FT modifications required. To attenuate the resulting increase in modelling complexity, the IAEA has developed the fault sequence analysis (FSA) method as a systematic approach to investigate the impact of extreme events for a wide range and credible combinations of independent hazards /KUZ 11/. The approach has been extended to the Extreme Event Analyzer (EEA) based on the PSA Software RiskSpectrum® /KUM 16/. However, the underlying FSA approach relies on a partly adapted HPSA model and captures only combinations of unrelated events occurring by chance independently of each other simultaneously jointly impacting the plant system.

In the context of previous PSA-based approaches the question arose if it is possible to analyse hazard impact patterns in detail and prior to their integration in the PSA plant model. The representation of HC dependency patterns through network graphs as discussed in /BER 19/ offers a promising methodological framework. The network-based analysis allows the individual investigation and mutual comparison of HC dependency patterns of multiple hazards based on statistical network measures. The identification of conjoint important network elements aims to foster the understanding about critical hazard impact contributors irrespective of the investigated system state or event sequence assumed within a given PSA.

The investigation of multiple hazard impacts still needs to be addressed, particularly with respect to credible combinations of related as well as independent hazards. In the following, a generic network-based approach is proposed that aims to reformulate multiple hazard impact dependencies as layers of a multidimensional network as introduced in /BER 20/. Each layer of the discussed multi-layer network characterises an individual hazard impacting the plant system described as a HC set. The hierarchical organisation of the hazard information facilitates the visual comparison of the dependency patterns through network graphs as well as the numerical comparison of local and global network

measures. The explicit formulation of HC dependency patterns as multiplex networks provides the basis for considering the complete spectrum of hazard impact patterns, in particular correlations between different hazard impact patterns in terms of intra-layer dependencies.

5.1 Interpreting Multiple Hazards as Aspects of a Conjoint Network

For taking into account impacts from multiple hazards including hazard combinations to a complex technical system, the HC network introduced in Chapter 4 can be considered for different aspects, respectively different representations of the network. In principle, it can be reasonable that the modifications of one hazard impact network required to adequately describe the dependency patterns of another hazard impact are only minor ones. For instance, it can be reasonable to consider the same HCs for different hazard impacts while only the dependency patterns, i. e. the set of edges and their properties, will change for different hazards as depicted in Fig. 5.1 (hazard 2 versus hazard 1). It can be also reasonable that a set of HCs, i. e. set of nodes are grouped together, or one HC is further partitioned to capture the dependency patterns of another hazard as illustrated in Fig. 5.1 (hazard 2 versus hazard 3).

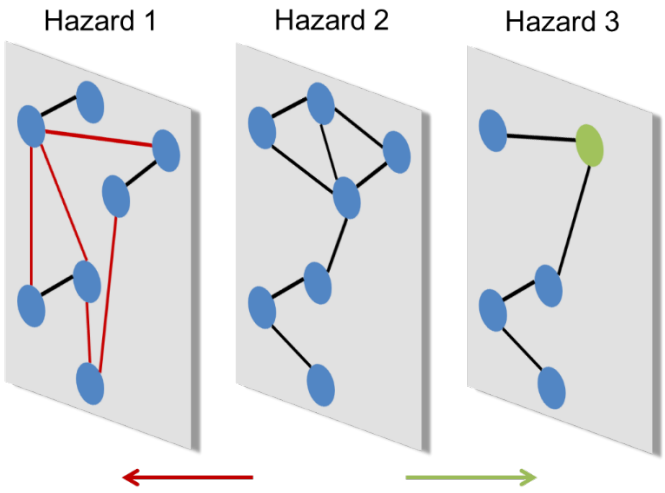


Fig. 5.1 Aspects of multidimensional network representation interpreted for different hazards (1-3) impacting a given technical system

Based on this perspective also discussed in /BER 19/, the networks representing different hazards impacting a complex technical system can be regarded as a multidimensional representation of a conjoint network graph. Hence, the multidimensional network characterises the HC dependency patterns of a system for a set of hazards and/or haz-

ard combinations. Each dimension (or layer) of the multidimensional network describes the dependency patterns of a specific hazard by a specific HC network topology. The concepts and applications of multidimensional (or multilayer) networks across disciplines are described in more detail in e. g. /BEL 11/ and /BIN 18/.

The multidimensional network representation approach discussed in the following has been implemented as an additional analysis module in the pyRiskRobot software. The implementation is based on the Python package NetworkX /HAG 08/ for complex network analysis in general and on the Python package Pymnet /KIV 14/ providing specific methods for the generation, analysis and visualisation of multidimensional networks.

5.2 Multidimensional Network Graphs

As a generalisation of a one-dimensional network a multidimensional network can be defined in terms of a graph G as

$$G \coloneqq G(V, E, D, f) \tag{5.1}$$

with $v \in V$ as the set of N nodes (or vertices), $e \in E$ as the set of links (or edges), $d \in D$ as a set of dimension (or layers) and $f: E \to V$ as a function mapping each link to an unordered pair of nodes (u, v, d). Different to simple networks, the edges are defined as triples(u, v, d) of two connected nodes plus the indicator of the dimensions in which the edge exists. Thus, a node belongs to or appears in a given dimension d if there is at least one edge labelled with d adjacent to it. As for one-dimensional networks, directed networks can be introduced by defining the edges as ordered pairs of nodes (and dimension label). In case of a weighted network each edge has an associated weight $w: E \to \in \mathbb{R}$ mapping each edge to a real number. A detailed and self-contained introduction to the mathematical formulation of multidimensional (or multilayer) networks can be found e. g. in /DED 13/.

5.2.1 Types of Multidimensional Networks

Depending on the context and purpose of the analysis, different multidimensional network models exist as discussed in /MAG 13/. A multi-type network refers to a network, where nodes can be associated to multiple node types, a multi-relationship network,

where multiple labelled links may exist between nodes, and multi-layer networks, where multiple, co-existing networks are combined to a joint multidimensional network with particular mappings between the different layers. An intuitive approach of interpreting multiple hazard as aspects of a conjoint network depicts the reformulation as layers of a multidimensional network. Hence, in a multi-layer network graph, each layer of the network characterises an individual hazard impacting the complex technical system. The hierarchical organisation of the hazard information facilitates the visual comparison of the dependency patterns as network topologies as well as the numerical comparison of local network measures. For combining the impact of independently, but simultaneously occurring hazard impacts on a plant system, the expressiveness and hierarchy of a multi-layer network graph suitably represents information of multiple HC sets.

For clarification, in general complex networks are used to model interactions in real-world phenomena and engineered systems as heterogenous networks with different types of nodes and edges. For instance, the representation of Level 1 PSA plant models as complex dynamic networks has already been discussed in /HIB 16/ and /RIF 18/ by associating centrality measures of complex networks to the risk increase factor calculated by PSA plant models. Focusing on a single type of nodes, a complex network would be better characterised by a multi-layer, that is a set of nodes related to each other with different types of inter- and intra-layer relations. Thus, the multi-layer representation is much richer than common complex networks.

Note that the focus of this work is on the analysis of available complex hazard impact data but not on inferring on the hazard impact dynamic affecting the complex plant system. All assumptions are based on the fact that it is intended to use networks to intuitively visualise, analyse, describe and compare HC dependency patterns impacting a complex plant system, but not to dynamically simulate specific complex hazard impacts, i. e. consider time-dependent network models. Nevertheless, an elaborated HC network can be a reasonable reference graph for modelling the dynamic of a complex hazard impact on a complex plant system, particularly with respect to the hazard propagation behaviour between HCs.

5.2.2 Multiplex Network Representation of Multiple Hazards

Based on a HC dependency network for a specific hazard, it can be reasonable to build upon the applied partitioning of other considered hazard impacts. The partitioning can be different for different hazard types, but they can as well be considered as a generic

database for elaborating the dependency patterns. By using different representation schemes in terms of multi-layer networks – such that different dimensions reflect different relationships various hazards can be studied applying network analysis. For some hazards it can be reasonable to assume a similar set of nodes, i. e. HCs, such that the elements of an existing HC network may serve as a generic common network suitable to represent the impact of multiple hazards aimed to be considered in a PSA plant model. The potentially altered SSC-compartment mapping does not impact the network graph, given that the set of nodes, i. e. HCs, remains unchanged. However, the dependency patterns, i. e. links between the HCs, most likely vary with respect to the hazard impact considered in a characteristic manner. In the terminology of network graphs, the interpretation of a set of nodes for different types of mutual dependencies is also referred to as different aspects of a network graph. In principle, multiple hazard impacts on a complex plant system can be intuitively represented as different aspects of a network, modelled as a multi-layer network graph of the type illustrated in Fig. 5.2.

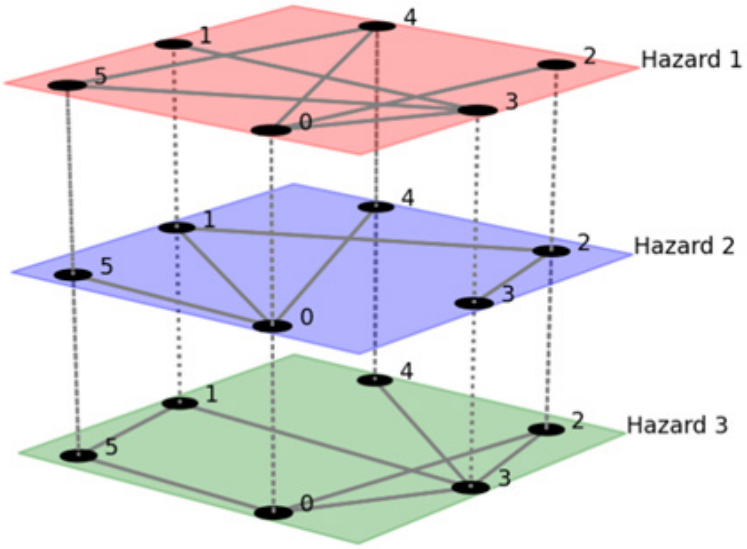


Fig. 5.2 Representation of HC dependencies for multiple hazard impacts (1-3) affecting a complex plant system as different aspects or layers of a multidimensional network graph

A special type of a multi-layer network depicts a multiplex network with the same set of nodes in each dimension, with potential inter-layer relations only between the same nodes, and specific dependency patterns in each layer in terms of intra-layer relations as indicated in Fig. 5.2. Given the discussion that a HC network can be a suitable representation for the impact dependencies of multiple hazards, a multiplex network provides an intuitive and expressive graph representation for this purpose. In particular, the intra-

layer links between HCs given a specific hazard (solid lines in Fig. 5.2) and inter-layer links between different hazards given an individual HC (dotted lines in Fig. 5.2) allow to describe the impact dependency patterns of a plant system for a set of hazards and/or potential hazard combinations. The concept of intra-layer relations makes multiplex networks a promising methodological concept to analyse hazard combinations beyond the assumption of independence. In principle, based on multiplex networks not only single induced hazards and credible combinations of independent hazards can be considered, but also the detailed correlation of multiple related hazards can be analysed prior to their integration in the Level 1 PSA plant model.

5.2.3 Benefits for Enhancing Hazards PSA

I should be noted that the above assumption of a constant set of nodes, i. e. HCs, may not be sufficient for the complete spectrum of considered hazards. For instance, it can be necessary that a set of compartments has to be merged into a joint HC, or one compartment has to be further partitioned to ensure that all SSCs assigned to it are jointly and equally affected by a specific hazard. Even though not discussed further in this context, the framework of complex network graphs also provides suitable multidimensional network models for a varying set of nodes across network layers.

Visualisation of Multiple Hazard Impact Patterns

Due to the complexity of the hazard specific information an advantageous representation of the corresponding dependency patterns as a multiplex network topology allows to gain insights into the characteristic properties of multiple hazard impact patterns on the complex technical system. In the frame of network-based analysis the dependency patterns of multiple hazards can be independently investigated via intra-hazard edges or jointly investigated via inter-hazard edges.

As in the one-dimensional network-based approach, the representation as a multiplex network aims to mutually support the analysis progress and information acquirement process about multiple hazard impacts on a complex system by indicating each information update as graphical change in the network topology or numerical change in relevant network measures.

Analysis of Multiple Hazard Impact Patterns

The multiplex network-based analysis of multiple HC dependency patterns – each associated to another hazard – can provide valuable insights about the importance of individual HCs given one or multiple hazards, and of clusters of HCs given one or multiple hazards. The local and global multiplex network measures allow to analyse and compare the HCs within and across the different hazard layers. Thus, the identification of conjoint important network elements aims to enhance the understanding of critical hazard impact contributors irrespective of the actual considered system state or event sequence assumed in the PSA.

Hence, transparent strategies can be developed to reduce the hazard impact mapping to the main nodes or clusters of highest importance relevant to the hazard impact combinations considered. The approach serves as an auxiliary, complementary pre-processing analysis step of HC patterns prior to their automated integration in a PSA plant model. Moreover, the network topologies derived can provide the base for further modelling hazard impact dependencies by means of complex dynamic networks.

5.3 Summary and Discussion

A generic network approach has been proposed that allows to formulate multiple hazard impact dependencies as layers of a multidimensional HC network. Each layer of the multi-layer network characterises an individual hazard impacting the complex engineered system. The hierarchical organisation of the hazard information facilitates the visual comparison of the HC dependency patterns as network topologies as well as the numerical comparison of local and global network measures. Thus, the network-based approach aims to mutually support the analysis progress and information acquirement process about multiple hazard impacts on a complex system by indicating each information update as graphical change in the network topology or numerical change in relevant network measures.

The complex network-based analysis concept has been extended by increasing the HC dependency network for a specific hazard to a multi-dimensional network-based concept for multiple hazards. For clarity, the concept is so far reduced to multiplex networks, based on the assumptions that all HCs are identical across layers, mutually connected by inter-layer edges, and that an individual HC is connected by intra-layer edges differ-

ently to the remaining HCs within each layer. Besides considering independent single or multiple hazard impacts, the multiplex network-based approach also provides a methodological framework capable of investigating combinations of subsequent or correlated (by a common initiator) hazard impacts. The multiplex network representation can provide valuable insights useful for identifying important HCs, analysing individual hazard impacts by intra-hazard dependencies and combining multiple hazard impacts by specifying inter-hazard dependencies of HCs.

It is foreseen to study the local and global network measures defined for multiplex networks with respect to their capability to indicate important elements of the HC network. Moreover, a transparent strategy needs to be developed in order to deploy these analysis results as an auxiliary analysis step prior to the explicit integration of potentially combined hazard impacts by the automated modification of the PSA plant model topology.

6 Conclusions and Outlook

This work introduced and discussed approaches to efficiently integrate hazard impacts in probabilistic safety analyses (PSA) of complex technical systems, such as nuclear power plants (NPP). The major goal is to enhance existing PSA plant models towards hazards PSA (HPSA) models by systematically considering multiple hazards in terms of induced hazards and credible combinations of related as well as independent hazards. The hazard impact can be mapped to the plant system by assigning jointly affected systems, structures and components (SSCs) important to safety to specific hazard compartments (HCs). By extending the corresponding fault trees (FTs) of SSCs for the additional hazard related failure causes, the hazard impact patterns are integrated in a given PSA plant model.

In order to efficiently and systematically integrate a particular hazard impact in an existing PSA plant model, GRS has developed the software tool pyRiskRobot as an approach to modify complex FT topologies in an automated and traceable manner directly within the database of the PSA software applied. The agent-based concept of pyRiskRobot provides a set of topological operations that can be combined to perform advanced modelling tasks, such as the automated duplication of conjoint FT topologies using an interactively elaborated relabelling scheme of the cloned FT elements. The topological operations fostered by pyRiskRobot are capable to extend existing Level 1 PSA plant models to appropriately assess the robustness of complex plant behaviour under hazard impacts. Thus, existing PSA plant models can be enhanced towards HPSA models by integrating the hazard impact as well as towards site-level PSA models by duplicating redundant trains to consider the risk aggregation on the plant site.

The consideration of hazard impacts is a challenging task due to the complexity of the given plant system as well as of the hazard specific impact patterns, i. e. the HC dependency patterns. Network graphs offer an intuitive approach to organise, visualise and analyse manifold relations between multiple objects. By representing HCs and their mutual directional dependencies as complex networks, the encoded hazard specific impact patterns can be analysed for statistical global and local network properties. The descriptive network measures can be used to objectively compare and potentially reduce networks as an analytical step prior to the hazard integration in the PSA plant model.

The partitioning of the plant system into HCs may vary for different hazards and cannot be applied to the entire spectrum of individual and combined hazards. However, for some

hazard impacts it can be reasonable to assume the same set of HCs. The complex networks of different hazards impacting the given plant system can be regarded as a multidimensional representation of a reference network topology, such that each layer of the network represents a HC set indicating the intra-hazard dependencies of an individual hazard impact. By representing multiple sets of HCs as a multidimensional network, the inter-hazard dependencies for an individual HC can be considered. The proposed network-based analysis approach is capable to investigate combinations of subsequent or correlated hazard impacts as mapped to a plant system as an analytical step prior to the hazard integration in the PSA plant model.

Based on the methodological framework of complex multidimensional networks, the introduced analysis concept is planned to be applied to a comprehensive hazard database describing the impact of multiple hazards on a given plant system. On the one hand, it is important to investigate the performance of the simple network analysis of HC dependency patterns of individual hazards and to identify network measures most suitable to indicate important network elements. On the other hand, a concept to appropriately assemble multiple HC networks as layers of a multidimensional network needs to be developed including potential inter-hazard dependencies. Given the derived network topology, suitability and efficiency of multiplex network measures need to be investigated. Moreover, a transparent strategy needs to be developed in order to deploy the network-based analysis results as an auxiliary step prior to the explicit integration of potentially combined hazard impacts through modification of the PSA plant model topology. In combination with the automated topological operations provided by pyRiskRobot, the network-based analysis approach aims to intuitively, efficiently and reliably support the extension and enhancement of Level 1 PSA plant models towards HPSA models in order to assess the robustness of complex plant behaviour under various hazard impacts and hazard impact combinations.

References

/BAB 09/ Babst, S., G. Gänssmantel, and R. Stück: Precursor Analyses for German Nuclear Power Plants. Kerntechnik, 74 (3), pp. 111 – 113, Carl Hanser Verlag, München, Germany, 2009.

/BAB 16/ Babst, S., G. Gänssmantel, and A. Wielenberg: Lessons Learned on Probabilistic Methodology for Precursor Analyses, Kerntechnik, 81 (5), pp. 520 – 526, Carl Hanser Verlag, München, Germany, 2016.

/BAY 12/ Bayer, M.: SQLAlchemy: Book chapter in: Brown, A., and G. Wilson (Eds.): The Architecture of Open Source Applications, Volume II: Structure, Scale, and a Few More Fearless Hacks, 2012, http://aosabook.org.

/BEL 11/ Berlingerio, M, et al.: Foundations of Multidimensional Network Analysis, in: Proceedings of 2011 International Conference on Advances in Social Networks Analysis and Mining, pp. 485 – 489, Kaohsiung, Taiwan, 2011, https://doi.org/10.1109/ASONAM.2011.103.

/BEL 13/ Berlingerio, M., et al.: Multidimensional networks: foundations of structural analysis, World Wide Web, 16, pp. 567 – 593, https://doi.org/10.1007/s11280-012-0190-4.

/BER 16/ Berner, N., and J. Herb: Generic framework for the automated integration of impacts from hazards in PSA models. Risk, Reliability and Safety: Innovation Theory and Practice, in: Walls, Revie, and Bedford (Eds.): Proceedings of the 26th European Safety and Reliability Conference 2016 (ESREL 2016). Glasgow, United Kingdom, 2016.

/BER 17/ Berner, N., et al.: Systematic Integration of Hydrological Hazards by Automatically Extending PSA Models. Safety and Reliability – Theory and Applications, in: Cepin, M., and R. Bris (Eds), Proceedings of the 27th European Safety and Reliability Conference 2017 (ESREL 2017). Portoroz, Slovenia, 2017.

/BER 17a/ Berner, N., and J. Herb: Weiterentwicklung der Methodik zur automatisierten Integration übergreifender Einwirkungen in PSA-Modelle der Stufe 1, GRS-454, ISBN 978-3-946607-36-6, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Germany, 2017, https://www.grs.de/publikation/grs-454 (in German).

/BER 19/ Berner, N., and M. Utschick: Network-based analysis of hazard dependency patterns prior to the automated integration in PSA models, in: Beer, M. and E. Zio (Eds.): Proceedings of the 29th European Safety and Reliability Conference (ESREL 2019), Hannover, Germany, 2019.

/BER 20/ Berner, N., and J. Scheuer: A multidimensional network approach for analysing hazard impact dependencies, in: Baraldi, P., F. Di Maio, and E. Zio (Eds.): Proceedings of 30th European Safety and Reliability Conference (ESREL 2020) and the 15th Probabilistic Safety Assessment and Management Conference (PSAM 15), Research Publishing, Singapore, ISBN: 981-973-4949-00-0, in publication 2020, https://doi.org/10.3850/981-973-4949-00-0 esrel2020psam15-paper.

/BIN 18/ Bianconi, G.: Multilayer Networks: Structure and Function, Oxford University Press, ISBN: 9780198753919, 2018.

/DED 13/ De Domenico, M., et al.: Mathematical formulation of multilayer networks, Physical Review X, 3(4), 041022, 2013, https://doi.org/10.1103/PhysRevX.3.041022.

/EC 20/ European Commission (EC): Advanced Safety Assessment Methodologies: Extended PSA, http://asampsa.eu, latest access: July 6, 2020.

/FOE 20/ Foerster, E., E. Raimond, and Y. Guigueno: Probabilistic safety assessment for internal and external events / European projects H2020-NARSIS and FP7-ASAMPSA_E, EPJ N-Nuclear Sciences & Technologies, *6*, 38, 2020, https://doi.org/10.1051/epjn/2019012.

/HAG 08/ Hagberg, A. A., D. A. Schult, and P. J. Swart: Exploring network structure, dynamics, and function using NetworkX, in: Varoquaux, Vaught, and Millman (Eds.): Proceedings of the 7th Python in Science Conference (SciPy2008), pp. 11 – 15, Pasadena, CA, USA, 2008.

/HER 11/ Herb, J., and J. von Linden: Procedures and tools comparing PSA in the frame of periodic safety reviews, in: Proceedings of ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis, pp. 1364 - 1373, Wilmington, NC, March 13-17, 2011, on CD-ROM, American Nuclear Society, LaGrange Park, IL, USA, 2011.

/HER 12/ Herb, J., et al.: Fault tree auto-generator: How to cope with highly redundant systems, in: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012), pp. 2704 – 2713, ISBN: 978-1-62276-436-5**,** Curran Associates, Inc., Red Hook, NY, USA, 2012.

./HER 15/ Herb, J., et al.: Automatic integration of a Fire PSA model in a Level 1 PSA, in: Proceedings of Annual European Safety and Reliability Conference 2015 (ESREL 2015), Zurich, Switzerland, September 6 – 10, 2015, CRC Press, https://www.crcpress.com/Safety-and-Reliability-of-Complex-Engineered-Systems-ESREL-2015/Podofillini-Sudret-Stojadinovic-Zio-Krger/9781138028791.

/HIB 16/ Hibti, M., A. Marechal, and A. Oudjit: Exploring Relations between Graph Metrics and Importance Measures in PRA Sequences, in: Proceedings of 13th International Probabilistic Safety Assessment and Management Conference (PSAM13), Seoul, Republic of Korea, October 2016, https://publons.com/journal/325745/proceedings-of-the-international-conference-on-pro.

/IAE 20/ International Atomic Energy Agency (IAEA): Protection against Internal Hazards in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-64, Vienna, Austria, in publication, 2020.

/KIM 08/ Kim, J., and T. Wilhelm: What is a complex graph?, Physica A: Statistical Mechanics and its Applications, 387(11), pp. 2637 – 2652, 2008, https://doi.org/10.1016/j.physa.2008.01.015.

/KIR 99/ Kirchsteiger, C.: On the use of probabilistic and deterministic methods in risk analysis, Journal of Loss Prevention in the Process Industries, 12(5), pp. 399 – 419, 1999.

/KIV 14/ Kivelä, M., et al.: Multilayer networks, Journal of Complex Networks, Volume 2, Issue 3, pp. 203 – 271, 2014, https://doi.org/10.1093/comnet/cnu016.

/KUM 16/ Kumar, M., S., et al.: Extreme Event Analysis – A benchmarking study at Armenian Nuclear Power Plant to examine plant robustness against the impacts of Extreme Events, in: Proceedings of 13th International Probabilistic Safety Assessment and Management Conference (PSAM13), Seoul, Republic of Korea, October 2016, https://publons.com/journal/325745/proceedings-of-the-international-conference-on-pro.

/KUZ 11/ Kuzmina I., A. Lyubarskiy, and M. El-Shanawany: An Approach for Systematic Review of the Nuclear Facilities Protection against the Impact of Extreme Events, in: Proceedings of the Nordic PSA Conference – Castle Meeting 2011, Stockholm, Sweden, 5 – 6 September 2011.

/LIN 07/ von Linden, J., et al: Methods for a Fire PSA exemplarily applied to a German BWR-69 type nuclear power plant. Kerntechnik 72(3), pp. 139 – 144, Carl Hanser Verlag, Munich, Germany, 2007.

/MAG 13/ Magnani, M., and L. Rossi: Formation of multiple networks, in: International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction. Vol. 7812 of LNCS, 10, 978-3, pp. 257 – 264, Springer, Berlin - Heidelberg, 2013.

/NAR 20/ New Approach to Reactor Safety Improvements (NARSIS): Project website,
http://www.narsis.eu/, latest access: July 6, 2020.

/NEA 20/ Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI): Status of Site-Level (Including Multi-Unit) PSA Developments, NEA/CSNI/R(2019)16, Paris, France, in publication, 2020.

/NEW 10/ Newman, M.: Networks: An Introduction, Oxford University Press, 2010, https://doi.org/10.1093/acprof:oso/9780199206650.001.0001.

/PAN 20/ The pandas development team, pandas-dev/pandas: Pandas, Zenodo, 2020, http://doi.org/10.5281/zenodo.3509134.

/PSA 20/ PSA – The Open PSA Initiative: The Open-PSA Model Exchange Format, Official Documentation 2.0,
https://open-psa.github.io/mef/index.html, latest access: July 6, 2020.

/PSF 19/ python Software Foundation (PSF): PEP 373 – Python 2.7 Release Schedule, https://www.python.org/dev/peps/pep-0373/, latest access: July 6, 2020.

/PYT 20/ PyTables Developers Team: PyTables: Hierarchical Datasets in Python, http://www.pytables.org/, latest access: July 6, 2020.

/RIF 18/ Rifi, M., M. Hibti and R. Kanawati: A Complex Network Analysis Approach for Risk Increase Factor Prediction in Nuclear Power Plants, in: Proceedings of the 3rd International Conference on Complexity, Future Information Systems and Risk - Volume 1: COMPLEXIS, ISBN 978-989-758-297-4, ISSN 2184-5034, pp. 23 – 30, SCITE-PRESS – Science and Technology Publications, Funchal, Madeira, Portugal, 2018, http://doi.org/10.5220/0006700000230030.

/ROE 17/ Röwekamp, M., et al.: Methoden zur Bestimmung des standort- und anlagenspezifischen Risikos eines Kernkraftwerks durch übergreifende Einwirkungen / Estimation of the Site and Plant Specific Risk of a Nuclear Power Plant from Hazards, Technischer Fachbericht / Technical Report, GRS-A-3888, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Germany, June 2017 (in German).

/ROE 18/ Röwekamp, M., et al.: Probabilistische Risikoanalysen der Stufe 1 für Standorte mit mehreren kerntechnischen Anlagen, GRS-A-3935, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Germany, September 2018 (in German).

/STA 11/ Stamatelatos, M., et al.: Probabilistic risk assessment procedures guide for NASA managers and practitioners. NASA/SP-2011-3421, HQ-STI-11-213, 2011, https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa. gov/20120001369.pdf.

/TUE 14/ Türschmann, M., S. Sperbeck, and G. Thuma: Recent research on natural hazards PSA in Germany and future needs, in: Probabilistic Safety Assessment (PSA) of Natural External Hazards Including Earthquakes. OECD Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI). NEA/CSNI/R(2014)9. Paris, France, 2014, https://www.oecd-nea.org/nsd/docs/2014/csni-r2014-9.pdf.

/TUE 15/ Türschmann, M., M. Röwekamp, and S. Babst: Concept for Comprehensive Hazards PSA and Fire PSA Application, Progress in Nuclear Energy, Volume 84, Special Issue: EUROSAFE 2013, pp. 36 – 40, 2015, http://www.sciencedirect.com/science/article/pii/S0149197015000876.

/TUE 15a/ Türschmann; M., et al.: Aufstellung, Quantifizierung und Auswertung von Brand-Ereignisabläufen, GRS-A-3837, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Germany, November 2015 (in German).

Abbreviations

API	Application Programming Interface
BE	Basic Event
CmpFT	Compare FTs
EEA	Extreme Event Analyzer
ET	Event Tree
FSA	Fault Sequence Analysis
FT	Fault Tree
GUI	Graphical User Interface
HC	Hazard Compartment
IAEA	International Atomic Energy Agency
IE	Initiating Event
MCS	Minimal Cut Set
MSSQL	Microsoft® SQL Server
NaN	Not a Number
NB	Notebook
NPP	Nuclear Power Plant
ORM	Object Relational Mapping
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Analysis
SQL	Structured Query Language
SSCs	Systems, Structures and Components

List of Figures

List of Tables

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-947685-50-9