Resilience Analysis of Offshore Safety and Power System

By

© Adnan Sarwar

A Thesis

submitted to the School of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Engineering

Faculty of Engineering & Applied Science

Memorial University of Newfoundland

May 2018

St. John’s Newfoundland

ABSTRACT

Harsh and deep waters create challenging environments for offshore drilling and production facilities, resulting in increased chances of failure. This necessitates improving the resilience of the engineering system, which is the capability of a system to recover its functionality during disturbance and failure. The present work proposes an approach to quantify resilience as a function of vulnerability and maintainability. The approach assesses proactive and reactive defense mechanisms along with operational factors to respond to unwanted disturbances and failures. The proposed approach employs a Bayesian network to build two resilience models. Two developed models are applied to: 1) a hydrocarbon release scenario during an offloading operation in a remote and harsh environment, and 2) the main requirements to improve the resilience of an offshore power management system. This study attempts to relate resilience capacity of a system to the system's absorptive, adaptive and restorative capacities. These capacities influence pre-disaster and post-disaster strategies that can be mapped to enhance resilience of the system. Furthermore, the technique of an object-oriented framework is adopted to better structure the resilience model as a function of a system's adaptability, absorptive and restorative capabilities. Sensitivity analysis is also conducted to analyze the impact and interdependencies among different variables to enhance resilience.

ACKNOWLEDGEMENTS

I thank, and praise be to Allah (the God) alone, The Sustainer, most Compassionate, ever Merciful, and I send salutations upon His prophet Muhammad peace be upon him.

I would like to express my sincere appreciation to my supervisor Dr. Faisal Khan, and co-supervisor Dr. Lesley James; members of the Faculty of Engineering and Applied Science at Memorial University of Newfoundland. If it were not their precious time, continuous guidance and advices, and financial support, the present undertaking would not be completed, nor it could be worth reading. I would also thanks to Dr. Majeed Abimbola, and team members of C-RISE for their professional feedbacks.

I thank to all my family members, for being beside me and provided moral support in completion of this endeavor. I know without their love, persuasion and prayers, I would never be able to complete this task.

I also acknowledge the financial support provided by the collaboration between Norwegian University of Science and Technology (NTNU), of Trondheim, Norway, and Memorial University of Newfoundland, Canada.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

BN: Bayesian Network

C-NLOPB: Canada-Newfoundland Labrador Offshore Petroleum Board

C-RISE: Centre for Risk, Integrity and Safety Engineering

CPT: Conditional Probability Table

DAG: Directed Acyclic Graphical

DARPS: Differential Absolute and Relative Position Sensor

ET: Event Tree

E: Evidence

FT: Fault Tree

FLNG: Floating Liquefied Natural Gas

FPSO: Floating Production Storage and Offloading

IN: Intermediate Node

M: Maintainability

MV: Medium Voltage

OOBN: Object-Oriented Bayesian Network

OREDA: Offshore Reliability Data Handbook

PN: Pivot Node

PPD: Presidential Policy Directive

R: Reliability

RN: Root Node

SCADA: Supervisory Control Data Acquisition

UPS: Uninterrupted Power Supply

V: Vulnerability

Chapter 1: Introduction

1.1 Background

The growing demand for energy has resulted in exploration of new fields in deep waters and harsher environments: one such example is the Flemish Pass Basin of Newfoundland, where, the exploration and production is mostly feasible using floating drilling vessels and Floating Production Storage and Offloading (FPSO). Due to the harsh environment and extended distance from shore, robust and resilient systems are needed to perform safe drilling and production operations, efficient storage and offloading and safe transportation. In these scenarios, the complex offshore infrastructure systems are facing a growing number of disruptions due to their environmental conditions and interdependence with other infrastructures. The offloading operation between an FPSO and a shuttle tanker or carrier is a challenging operation due to the interaction of two floating bodies in an uncertain environment. Transferring hydrocarbon from floating platforms to shuttle tankers using loading arms, rigid pipes and flexible hoses is a challenging operation. Furthermore, a robust and resilient process is a necessity and a resilience assessment require anticipating disruption preparation and recoverability with an adaption assessment (Bakkensen, Fox-Lent, Read, & Linkov, 2016). A reliable and secure operation is a prerequisite for a resilient power system which can survive in extreme conditions, maintaining load continuity and withstanding sudden disturbances such as the unexpected failure of power system components (Liu, et al., 2016).

The resiliency of an infrastructure system with a variety of possible disruptive events and resulting consequences has become an increasingly important issue among service providers and operators. Due to a harsh environment, the unfavorable condition may be seen or unforeseen, so the aim of the resilience system is not only to protect and prevent the infrastructure from man-made and natural disaster events, but also to enhance the capability of a system to recover from an unfavorable event to a new steady state, and finally to its original state. System resilience is defined as the capability of a complex system to adjust its operational functionalities during uncertain conditions and keep the system operable during disruptions. The difference between resilience and reliability is based on the survivability of a system when experiencing extreme events (Liu, et al., 2016). The resilient system must be designed in a way so that it adapts maximum resistance, withstands and recovers quickly from any disruptive events within a defined period of time (Hosseini & Barker, 2016). Resilience engineering gives an engineering system (using system design and its operation) the ability to withstand adverse conditions and to recover capability swiftly after disruptive events. Resilience is recognized as a fundamental characteristic requirement of maritime systems operating in harsh and remote locations.

This study designed the model to quantify and improved the system resilience for two individual systems which are considered an important for safe and sustainability of oil and gas facilities operating in harsh and deep waters environment. To maintain the reliable and safe system, we considered hydrocarbon release (major issue in Newfoundland offshore) during an offloading operations and resilient power management system (sensitive operation) to interact with other engineered systems to maximize the performance and minimize the potential failures to maintain continuous operations.

1.2 Objectives

The proposed work has three main objectives:

- To develop a resilience model that captures design and operational characteristics
- To test the developed model on potential hydrocarbon release scenarios in an offloading operation in a harsh environment
- To study resilience of an offshore power supply.

1.3 Thesis Outline Organization

This thesis is compiled in a manuscript format. The outline of each chapter is described below:

Chapter 2 presents the literature review pertinent to this research. This comprises a brief background and framework of resilience, strategies and principles of resilience, resilience definitions in terms of different disciplines, resilience assessment and risk assessment methods.

Chapter 3 presents the resilience model and its application to potential hydrocarbon release during offloading operations from a remote offshore oil and gas facility. This chapter explores the gap between quantitative and qualitative assessment of resilience in the domain of a complex engineering system. The developed model explains the quantification of resilience relevant to vulnerability and maintainability for hydrocarbon release scenarios of offloading between a Floating Production Storage and Offloading (FPSO) unit and a shuttle tanker. The design and operational factors are included in the risk and resilience analysis, using a Bayesian network model. This model updates failure probabilities as new information becomes available. The proposed resilience analysis model helps to improve system design and operational activities with a better grasp of the weaknesses and recovery from system disruptions induced by adverse failure events. This chapter is under review for publication in the journal of *Risk Analysis*.

Chapter 4 presents a new resilience assessment model developed using the Object-oriented Bayesian network (OOBN) framework. This model is used to study the power system in an offshore facility. This chapter identifies the main requirements and risk factors of the offshore power system, to assess and improve system resilience using integrated operations. The OOBN is used to better structure and model a system's adaptability, absorptive capability and restoration or recoverability. A sensitivity analysis is also performed to study the interdependencies of the variables and strategies used to assess resilience. This chapter is under the review for publication in the journal of *Ocean Engineering*.

Chapter 5 presents the overall summary of the thesis and includes concluding remarks regarding the outcomes of this research along with recommendations for future work.

1.4 Co-Authorship Statement

Dr. Faisal Khan provided background training and supervised the research. The author, Adnan Sarwar, developed the model, tested and analyzed the results and prepared the manuscript. Dr. Khan provided assistance in developing the model, reviewing the results, correcting the analysis and interpreting the model and results. He also reviewed and revised the manuscript. The co-supervisor, Dr. Lesley James, reviewed and provided detailed knowledge about the application of integrated operations, reviewed the model and the interpreted results and provided much needed feedback on the manuscript. Dr. Majeed Abimbola contributed to this work by reviewing the manuscript and model development. The continuous feedback from these supervisors has been a real contribution towards successful completion of this work.

The author is responsible for composing this thesis. He has conducted the literature review and developed the expert-built model and its software implementation. He has presented different scenarios performed using the software (*GeNIe* 2.0 and *Hugin*), collected the results, interpreted them and developed conclusions based on which the recommendations are made.

1.5 Literature Review

1.5.1 Introduction to Resilience

Resilience originates from the Latin word *Resiliere* which means “to bounce back” and defines a system property that is characterized by the ability to recover from catastrophic failures, complexities, and vulnerabilities that arise from environmental conditions, to maintain or recover system functionality (Hosseini, Barker, & Ramirez-Marquez, 2016). The term *resilience* is used in different disciplines in different ways. In physics, it is the ability of a system to return to the original state after its deformation. In medicine, it is defined as the ability of individuals to recover from trauma or illness. In the context of an ecological system, resilience implies the persistence of systems in relation to external influences and their ability to absorb disturbances and adapt their dynamics (Holling, 1973). Resilience can be defined as the ability of the system to have the competence to resist, absorb and accommodate to or recover from the effect of hazards within a defined period, including the preservation and restoration of its essential structures and functionality after exposure to hazards. Resilience of an engineered system refers to a systems ability to continue to function successfully during an adverse event by planning to absorb, adapt and recover. According to Haimes (2006), the terms resilience and vulnerability are the common parlance of risk analysis, where *vulnerability* denotes the inherent states of a given system (e.g., physical, technical, organizational and cultural) that can be exploited by an adversary to adversely affect (cause harm or damage to) that system. To design an enhanced resilient system, there is a need to focus on avoiding disruptive events which may weaken the system during its operation and adapt the capability of recovery, helping to reduce possible damage to the system and to improve the availability and accessibility. A resilient system helps to avoid undesirable situations by developing an efficient system design with well-planned emergency and control measures, making the system capable of functioning and possibly rapidly eliminating the potential hazard (Dinh, Pasman, Gao, & Mannan, 2012). To avoid hazardous scenarios, presenting strategies for early detection, interpretation and quick response to unexpected variations is very important to make the system robust. Good design principles include sustaining resilience with an emphasis on flexibility and coping with unplanned situations. They should respond to these types of events with excellent communication and mobilization of resources to intervene at critical points. There are three different approaches to achieve or assess resilience such as: 1) system should have the capability to continue operating, preventing or absorbing upsets or shocks through built-in redundancy, 2) repair or restoration through preparation and response measures, and 3) anticipating adverse situations, adapting to circumstances and recovering a stable state after the major mishap occurs. The different approaches to achieve resilience are shown in Fig 1.

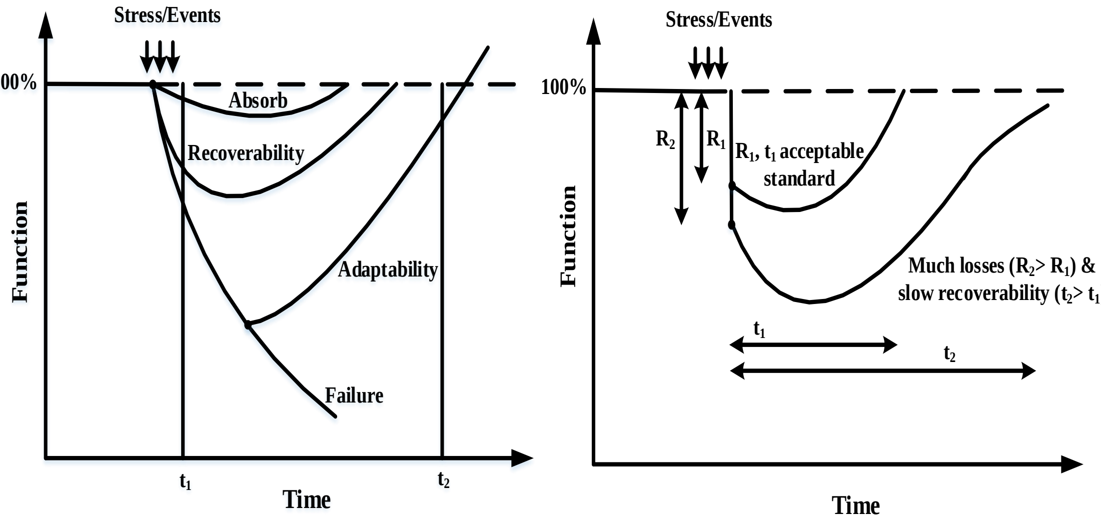

Figure 1: Resilience assessment framework. Adapted and modified from (Agarwal, 2015)

The main emphasis of the resilience operation is crisis management, provided by flexible and collaborative modeling of the system to address diverse risks of disruption proactively and anticipate upcoming new hazards constantly by evolving the scenarios. Resilience engineering enhances the organizational ability to make a robust, flexible process and monitors and revises risk models using the available resources proactively during disruption and ongoing production with the associated economic pressures. Resilience which works as a proactive defense to control the situation by minimizing the probability of failure, its consequences and restoration or recovery, is called a *triple resilience strategy* (Dinh, Pasman, Gao, & Mannan, 2012).

1.5.2 Strategies and Principles of Resilience

To achieve high resilience of the system, the following proposed strategies need to be implemented.

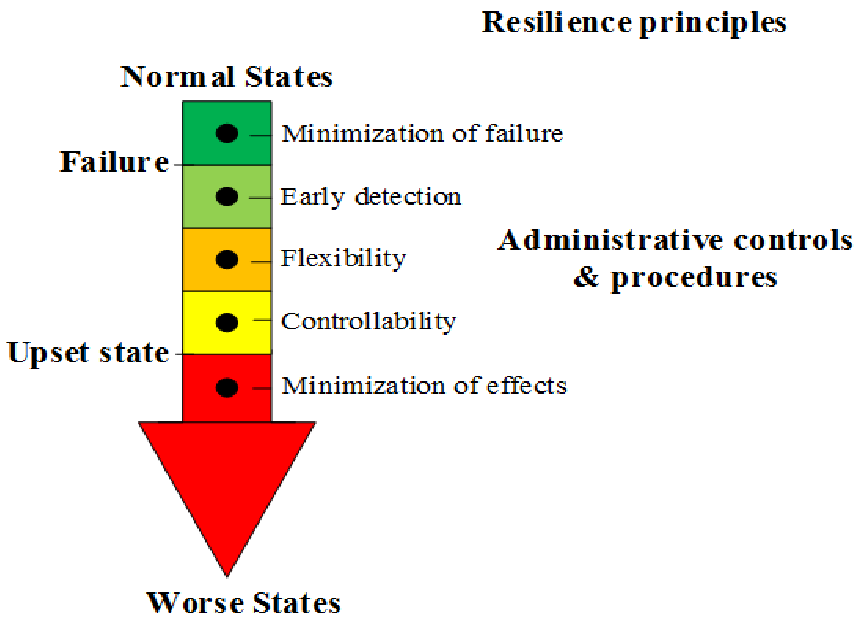

Figure 2: Strategies and principles of resilience. Adapted and modified from. Luthar et al. (2000)

The minimization of failure, principle is to avoid disruptions using preventive measures. An inherently safe designed system uses protective equipment and appropriate safety management. For example, a preventive measure includes choosing gaskets which help to minimize the leakage of hazardous substances.

Early detection, if the preventive method does not work efficiently to prevent failure, the role of autonomous early detection comes into place. For instance, the leak should be detected as soon as possible to avoid gas cloud formation, which will lead to worse situations. The detection is usually done by gas sensors.

Flexibility, the performance of the system needs to be maintained within the desired range or steady state through the system design and its operation. Input variables or parameters can be changed due to a disturbance. The flexibility principle for a resilience system is to design a more flexible progression that can operate with various instabilities. It is not essential to bring the system into its previous condition; it can remain somewhat disturbed as long the constraints and specifications are met. For example, a flexible design will allow operations to continue during a gas leak scenario. The leaked equipment segment could be by passed or the gas pressure reduced to minimize the leak rate while production is maintained online. Both measures can prevent a hazardous situation from escalating to cloud formation.

Controllability, a system can be controllable if the output parameters can be controlled and tuned to the target points in an acceptable time when an unexpected input causes the parameters to deviate from the set points. In the gas leak example, the flexible design allows the process to operate in bypassed or pressure-reduced conditions. However, whether operators can perform the changes and the length of time required depend on controllability of the process. The cloud formation can be stopped only when the new condition is obtained. The sooner the new condition is reached, the less flammable gas is released.

Limitation of effects, the principle of using protection or mitigation measures is to limit the consequences of an upset event. For example, equipment can be designed in a distributed way with easy access, so that leakages can be controlled or avoided within a short period of time.

Administrative Controls and Procedures—for certain unexpected disturbances, a solution in the form of a resilient design may be unfeasible. Moreover, not every risk can be foreseen by detection; therefore, the resilience principle should involve management systems with administrative controls and procedures. For example, proper maintenance procedure can even prevent a leak from occurring. Other measures include good emergency response plans to help quickly stop the leak, isolate the unit, shut down the plant or evacuate the community to minimize the consequences of lethality, injuries, harm to the environment and damage to equipment.

1.5.3 Resilience Framework

There are five basic attributes of a resilience framework that need to be considered for building a resilience into a system. These include: 1) proactive operational and reactive time periods, for different 2) system configurations, 3) events classifications, required 4) necessary actions and the necessary predefined 5) quality level needed to achieve a resilient system, as shown in Fig. 3:

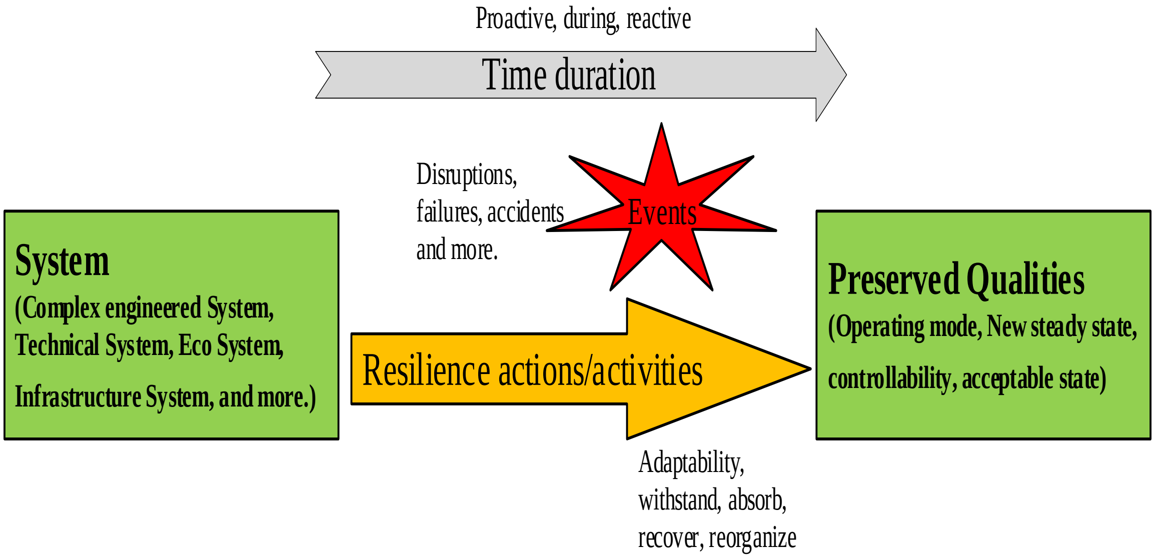
Proactive, during, reactive
Time duration
Disruptions, failures, accidents and more.
Events
System
(Complex engineered System, Technical System, Eco System, Infrastructure System, and more.)
Resilience actions/activities
Preserved Qualities
(Operating mode, New steady state, controllability, acceptable state)
Adaptability, withstand, absorb, recover, reorganize

Figure 3: Resilience Framework. Adapted and modified from (Sheard, 2008)

Time periods—different studies use terms such as: *before*, *prior*, *during*, *while*, *after*, *proactive*, and *reactive*. The time periods of resilience of a system can be understood in terms of *system anticipation*, including prevention of and preparation for an adverse situation before an event occurs. *Adaptability* and *absorptivity* help the system to survive during the event, with or without achieving the level of operational efficiency. The *recoverability* of the system's steady state after disruption or failure occurs whether the system returns to its previous state or to a new steady state. The general characteristics of a resilience system are defined with five sets of time periods. Based on the given set of time periods, different approaches are required to undertake the strategies to achieve high resilience.

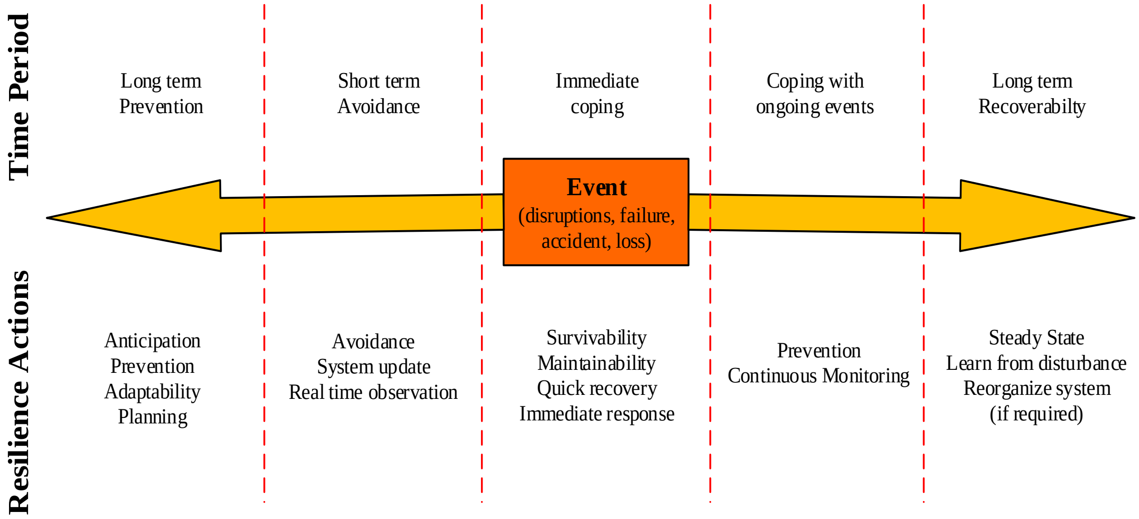

Figure 4: Resilience actions with respect to time periods. Adapted and modified from (Sheard, 2008)

- *Long term prevention*, works as a foresight prevention that involves prediction, anticipation, and planning for disturbances to prevent disruptions or loss of control of system. This is performed by anticipation of the future changes in an environment that may affect system stability, and is part of the identification and management of risks.

- *Short term avoidance*, this refers to the management of hazards that could affect the system quickly, by keeping the safety system updated to avoid system disruption.

- *Immediate-term coping*, survivability and coping with sudden disruptions. The system must respond quickly and efficiently to disruptions and threats, and must recover from loss of control, resisting harmful influences.

- *Coping with ongoing trouble*, in addition to surviving the events, the resilience system requires continuous monitoring for irregularities and threats to endure disruptions by implementing different strategies.

- *Long-term recovery*, this is defined as recovery from disruptions that have occurred. The system must learn from disturbance and build the capability to adapt and reduce the harmful influences.

System that exhibits resilience, the term *system* generally refers in this research to "*whatever is resilient"*, having constituent components, strategies and emergent properties to perform specific purposes. For example, a critical infrastructure can continue its operation and functionality during disruptive events through redundant and automatic switchover within a specified response time after certain events.

Events, the challenges in terms of disturbances, perturbations, environmental changes, mishaps due to accidents, failures and more to the ongoing well-being of a system are known as events. When resilience in a system is lacking, an event can cause unwanted consequences of many types, such as accidents, brittleness, mishaps, and more.

Required actions to consider a system resilient, the system should have the following properties: absorption, adaption, prevention and restoration or recoverability. The system can be considered resilient if it survives, sustains and maintains the important qualities. A system must be capable of reducing the likelihood of disruptive events with necessary actions needed to keep a state of equilibrium.

Preserved qualities refer to the functionality of the system sustaining its operations, objectives and controllability

1.5.4 Analysis of Resilience Definitions in Terms of Different Discipline Perspectives

Resilience is defined as the capability of a complex system to recover from severe disruptions and damage that have been recognized as significant characteristic dangers for critical offshore operations, especially in harsh environments. In recent years, research on resilience has been widely conducted for different disciplines such as ecology, economics and organizational science, critical infrastructures, psychology and more. There are several definitions of resilience offered in terms of different disciplines or domains, many of them similar and overlapping with existing concepts such as robustness, fault-tolerance, flexibility, survivability and agility, among others. For example, according to Webb (2007), ecosystem resilience is defined as "the ability of the system to maintain its functionality when faced with a novel disturbance". According to

Sheffi (2005), for economics and organizational science, resilience is defined as the “intrinsic ability to keep or recover a stable state, thereby allowing continuous operations after a disruption or in the presence of continuous stress”. According to psychology, resilience is defined as the dynamic process when individuals exhibit the positive behavioral response of adaptability when facing a critical situation (Luthar, Cicchetti, & Becker, 2000). According to Hollnagel et al. (2007), resilience is defined as the inherent capability of system to adjust its functionalities prior to or following changes and disturbances so that it can sustain operations even after a major mishap or in the face of continuous disruption or stress. The critical complex system is uncertain; a security incident may arise due to vulnerability that induces a certain degree of disruption in the system. Resilience can be used as an innovative management strategy to achieve a high level of security in an uncertain and dynamic environment (John, Yang, Riahi, & Wang, 2016).

Haimes et al. (2006), defined the resilience for system infrastructure as the “ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks”. Allenby and Fink (2005) defined social and ecological resilience as “capability of a system to maintain its functionalities and structure in the face of internal and external change and to degrade gracefully when it must”. Keogh and Cody (2013) defined resilience as “the robustness and recovering characteristics of utility infrastructure and operations, which avoid or minimize interruptions of service during an extraordinary and hazardous event”. Bruneau et al. (2003) defined infrastructural resilience as the “ability of the system to reduce the chances of shock, to absorb a shock if it occurs, and to recover quickly after a shock (re-establish normal performance)”. Thorisson et al. (2017), proposed the concept of achieving high resilience in terms of prioritization of restorative initiatives related to the degree of disruption or stressors, to achieve continuous operations. Vugrin et al. (2010) defined resilience as “…given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels”. The concept of organizational resilience is defined by Vogus and Sutcliffe (2007) as “the ability of an organization to absorb strain and improve functioning despite the presence of adversity”. Static economic resilience is defined by Rose (2007) as “the capability of an entity or system to continue its functionality like producing when faced with a severe shock, while dynamic economic is defined as the speed at which a system recovers from a severe shock to achieve a steady state”. The concept of resilience is comparatively new compared to other domains (Hosseini, Barker, & Ramirez-Marquez, 2016). According to Hollnagel et al. (2006), engineering resilience is defined as “the intrinsic ability of a system to adjust its functionality in the presence of a disturbance and unpredicted changes”. The American Society of Mechanical Engineers (ASME) (2009) defines resilience as the ability of a system to sustain external and internal disruptions without discontinuity of the system’s performance, or, if the function is disconnected, to fully recover the function rapidly. A resilient system must have the capability of system anticipation (foreseeing the threats or harmful activities), recover capability (robustness to sudden threats with flexibility), clearly monitoring ongoing changes and updating the CPT after the previous disruption to recover successfully.

1.6 Quantitative Risk Assessment

The quantification of the risk assessment approach uses an efficient probabilistic framework for assessing the resilience of a complex engineered system. There are many techniques that have found popularity for risk assessment in reliability engineering, among which the fault tree (FT), event tree (ET), and Bayesian network (BN) are prevalent.

1.6.1 Bayesian Network

A Bayesian network (BN) is a directed acyclic graphical probabilistic tool that can be used efficiently to represent uncertain information and interdependencies for the construction of reliability models. In a graphical probabilistic model, the nodes are used as random variables and directed arcs signify probabilistic dependencies and independencies among the risk factors. According to Barlow (1987), initially the Bayesian framework was introduced for the field of artificial intelligence, has later become popular in engineering systems (Langseth & Portinale, 2007) and has been promoted in many subfields such as fault finding (Langseth & Jensen, 2003), structural and system reliability (Mahadevan, et al., 2001) and risk analysis. BN enables probabilistic updating and performance assessment of components and systems having uncertain and evolving information, thus providing an effective tool for near-real time and post-event applications (Bensi, et al., 2011). It also allows a wide range of scenarios to be explored through the propagation of probabilistic information, making it an excellent framework for infrastructure risk assessment and decision support (Straub & Kiureghian, 2010).

In the Bayesian network described in Fig. 5, the initial nodes with no directed arc are considered as root nodes, which possess prior probabilities. All other nodes in the network are called intermediate nodes and each node is defined with its own conditional probability table. The intermediate nodes having arcs directed to them are known as child nodes and the nodes that have arcs directed from them are known as parent nodes. Each child node is associated with the CPT, given all combinations of the states of its parent nodes. The nodes with no further attached nodes are known as leaf nodes.

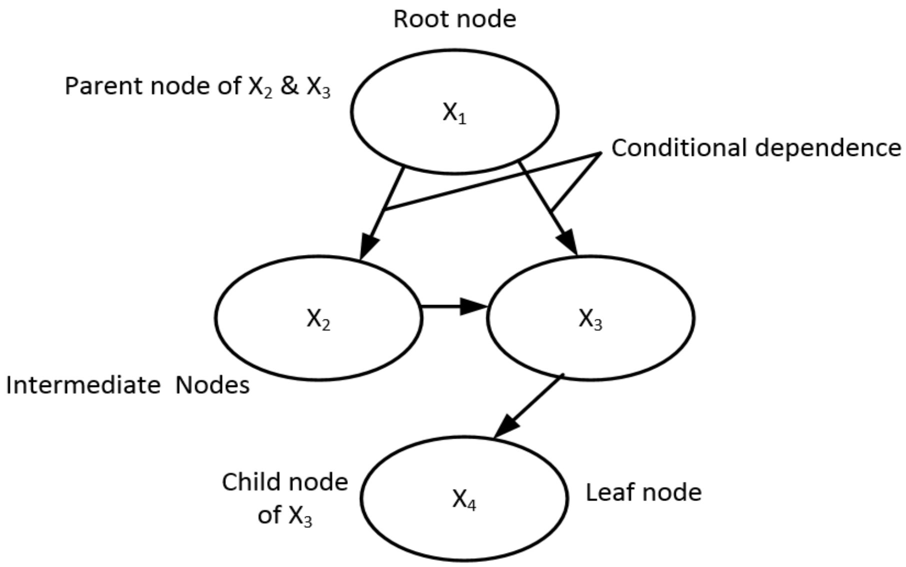

Figure 5: Typical Bayesian network

Bayesian networks use the “d-separation” principle and the chain rule to calculate the conditional dependencies among the involved factors or nodes within a network. For instance, node X_1 d-separates from node X_3, where X_2 blocks the link between node X_1 and node X_3. As a result, Node X_1 is conditionally independent of Node X_3, given X_2, which can be presented as: $P(X_1|X_2,X_3) = P(X_1|X_2)$. From Fig. 6 (a) and Fig. 6 (b), in the scenario of serial and diverging paths, node X_1 and X_3 are d-separated from each other, if node X_2 is known, while in a converging path, shown in Fig. 6 (c), node X_1 and X_3 are independent and the state of X_2 is unknown. According to the three given conditions, the root nodes are independent of each other and the intermediate nodes are conditionally dependent on their parent nodes.

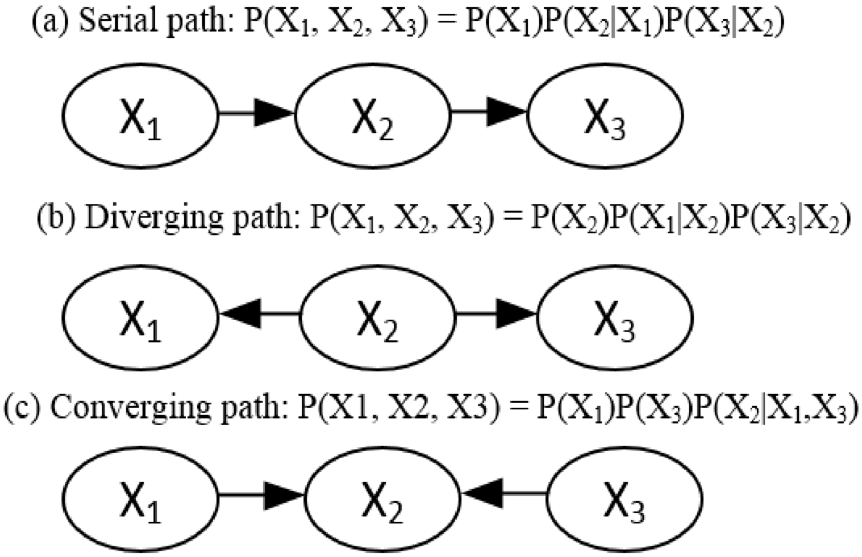
(a) Serial path: P(X₁, X₂, X₃) = P(X₁)P(X₂|X₁)P(X₃|X₂)
X1
X2
X3
(b) Diverging path: P(X₁, X₂, X₃) = P(X₂)P(X₁|X₂)P(X₃|X₂)
X1
X2
X3
(c) Converging path: P(X1, X2, X3) = P(X₁)P(X₃)P(X₂|X₁,X₃)
X1
X2
X3

Figure 6: D-separation criteria

The probability of each node or variable defines the conditional dependency on its parent nodes. The joint probability distribution of the network variables in Fig. 5 are specified as the product of these conditional probabilities in Eq. (1): (Wilson & Huzurbazar, 2007)

$$P(X_1,X_2,X_3, X_4) = P(X_1) \times P(X_2| X_1) \times P(X_3| X_1, X_2) \times P(X_4|X_3) \tag{1}$$

where $P(X_2| X_1)$, $P(X_3| X_1, X_2)$ and $P(X_4|X_3)$ are conditional probabilities given as X_1,X_2,X_3, while $P(X_1)$ denotes the prior probability. Moreover, with the assumptions of the Markov property and conditional independence (d-separation principle), the joint probability distribution for *n^th^* variable $P(X) = \{X_1,X_2,X_3,\ldots,X_n\}$ is given as Eq. (2):

$$P(\boldsymbol{X}) = \prod_{i=1}^{n} P\big(X_i|Pa(X_i)\big) \tag{2}$$

where $Pa(X_i)$ is the set of parent nodes X_i. One of the main advantages of Bayesian networks is the inference ability to calculate the probability of events based on new observed evidence. The beliefs (probabilities) are updated in accordance with the observations using Bayesian updates. Assume an evidence *E* is observed, i.e. occurrence or non-occurrence of primary events, and then:

$$P(\mathbf{X}| E) = \frac{P(X,E)}{P(E)} = \frac{P(X,E)}{\sum_X P(X,E)} \tag{3}$$

Eq. (3) can be used for prediction of probability or updating. However, computation through Eq. (3) can be practical if the available network is small and has few states and therefore requires an efficient algorithm to be adopted to avoid complex computation. In resilience assessment, conditional probabilities of the form P(Risk factors | events) or P(Disruptions | events) can be calculated as: the effect of a given risk factor with respect to the occurrence and non-occurrence of a known event, and the occurrence probability of disruption given the occurrence and non-occurrence of a known event. Moreover, in updating analysis, P(Events | Disruptions) are evaluated to show the occurrence probability of certain events that will cause a certain amount of disruption or losses to the system. The effectiveness of the Bayesian networks is mostly dependent on the accuracy of the conditional probability tables (CPT). The CPT tables can be estimated from different sources, such as statistical databases, experimental data, expert opinions, laws and regulatory bodies and more. The validation of the Bayesian network analysis can be performed using sensitivity analysis, result comparison and testing and evaluation of different scenarios. The Bayesian network is increasingly used in risk assessment and overall safety analysis of the engineered system, and helps to achieve the development of resilient system design and model a complex system with many variables in a compact representation through localized network clusters. Moreover, due to the Bayesian updating capability, Bayesian networks integrate expert opinions and new observations to handle the situation when there is insufficient data available or whenever new data become available for any variable; these can be implemented in the whole network.

Khakzad *et al.* (2011) explained the advantage of the Bayesian network over Fault Tree Analysis and Event Tree Analysis, in terms of modeling and risk assessment. Bobbio et al. (2001) showed that the limitations of fault trees can be overcome by relying on

Bayesian networks. There has been plethora of research on the conversion of fault tree and event tree analysis to a Bayesian network, with its comprehensive application in the field of risk analysis, safety and risk assessment and reliability engineering. This demonstrates its usefulness to design and model resilience systems (Montani, Portinale, Bobbio, & Codetta-Raiteri, 2008).

1.6.2 Object Oriented Bayesian Networks (OOBNs)

An Object-Oriented Bayesian network is a special class of Bayesian network. In addition to the usual nodes, an OOBN contains instance nodes (Weidl, Madsen, & Israelson, 2005). An instance node holds sub-networks to represent another Bayesian network, where complex networks of large systems can be divided into hierarchies of sub-networks with desired levels of abstraction using OOBN. The abstract entity or the relationship between two entities are represented as objects. The fundamental unit of the OOBN probabilistic graphical model is an object, which characterizes either a node (defined variable) or an instantiation of a network class which consists of instance nodes. An instance node is an abstraction of different network fragments into a single unit. The network of each class allows OOBNs to be more generic and able to be reused in other classes to facilitate the hierarchical description of a problem domain. To represent the simplified OOBN in Fig. 7, the following notations are commonly used: the instance nodes are squares with input and output interfaces; input nodes are separated with shadowed dashed line borders and output nodes are shown with shadowed bold line borders.

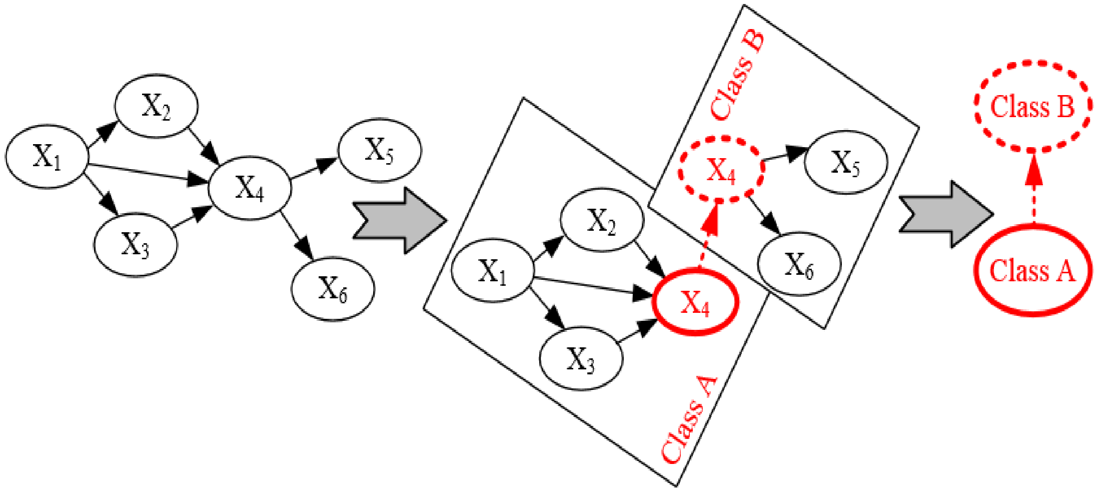

Figure 7: Modularization of Bayesian network into OOBN

The OOBN facilitates the construction of complex models and communication between the sub-network models is efficiently performed, avoiding the tedious repetition of identical network fragments and reducing the conditional probability tables. As shown in Fig. 7, instance nodes are connected with other class nodes through an interface node which includes input and output nodes. Input nodes have the same probability as their immediate parent node, so the input of each class cannot have more than one parent node. In contrast, the output nodes are considered to be ordinary nodes which convey their probability to the input nodes or affect the probability of their other usual nodes. Thus, each output node can have multiple child nodes (Khakzad, Khan, & Amyyotte, 2013).

Fig. 7 illustrates an example of how Bayesian networks can be developed with the hierarchy of smaller networks to make an instance node such as: Class A and Class B (in the middle), having Node X_4 (thick and dashed border) selected as an output node in the instance node of Class A and an input node in the instance node of Class B to connect them. Finally, the complex OOBN can be represented by using only instance nodes of Class A and Class B (right).

1.6.3 Fault Tree

Fault tree analysis is considered to be a widespread failure analysis tool among reliability engineers. It uses a top-down approach to determine the potential failure of the system, which is referred to as the top event (undesirable event), through the cause and effect relationship. The top event usually represents a major accident caused by safety hazards and includes loss of life, injury, or economic loss to the system, and more. Inventory characteristics and expert judgements are applied to recognize the top event and the single event, or combinations of events which could cause a top event are investigated. The relationships between events in FT are represented by means of gates, of which AND-gates and OR-gates are commonly used. The result of FT can be analyzed qualitatively and quantitatively. In qualitative analysis, an expression in terms of a combination of primary events is derived for the top event using Boolean algebra. In the quantitative evaluation, the terms of occurrence probability of the primary events and or minimal cut-sets are used to express the probability of the top event. For analyzing the FT result, methods used include the analytical method, Monte Carlo simulation and the binary decision diagram. An analytical approach is more frequently used for evaluation of FT, due to the limitations of Monte Carlo simulation (e.g., minimal cut-sets determination). To minimize the margin of error due to primary events data that are inaccurate and incomplete, fuzzy set theory and evidence theory have recently been used for FT analysis (Ferdous, Khan, Veitch, & Amyotte, 2009).

Fault trees are composed using gates and events. The gates most commonly used in a Fault tree are the AND and OR gates. For example, consider the top event (or a system) composed of two different events. An AND gate is used for connecting the system if both events need to occur to make the top event occur, while the OR gate is used for the condition where either of the events cause the occurrence of the top event. In this state, the probability of the top event, is equal to the combination probabilities of these two events. Fig. 8 below shows the two typical gates, OR (left), and AND (right) and their corresponding Boolean algebra.

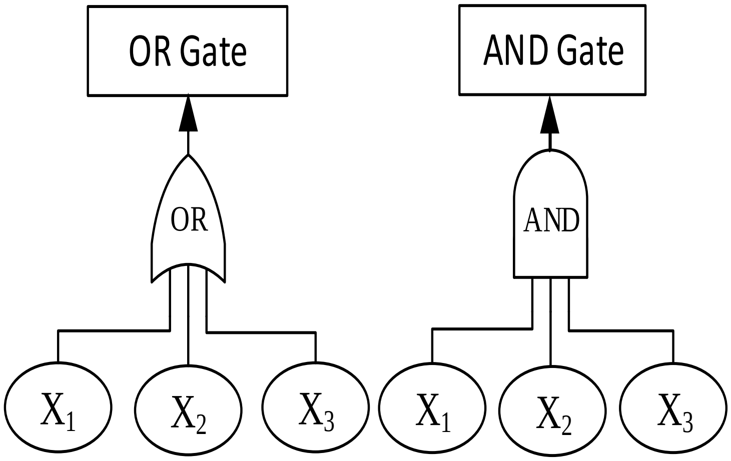

Figure 8: Representation of AND gate and OR gate in the Fault tree

Conventional fault trees presume that the events are considered as independent, because they are unable to examine conditional dependencies. Hence the corresponding Boolean algebra for *AND* and *OR* gates will be:

$$\mathrm{P(AND)} = \mathrm{P}\ (\mathrm{X}_1 \cap \mathrm{X}_2 \cap \mathrm{X}_3) = \mathrm{P}(\mathrm{X}_1)\mathrm{P}(\mathrm{X}_2)\mathrm{P}(\mathrm{X}_3) \qquad (4)$$

$$\mathrm{P(OR)} = \mathrm{P}\ (\mathrm{X}_1 \cup \mathrm{X}_2 \cup \mathrm{X}_3) = 1 - \{1 - \mathrm{P}(\mathrm{X}_1)\}\ \{1 - \mathrm{P}(\mathrm{X}_2)\}\ \{1 - \mathrm{P}(\mathrm{X}_3)\} \qquad (5)$$

In the case of having more than three events, the equation for an OR gate can be written as below:

$$\mathrm{P}\ (\mathbf{X}|\ \mathrm{E}) = \frac{\mathrm{P}(\mathrm{X},E)}{\mathrm{P}(E)} = \frac{\mathrm{P}(\mathrm{X},E)}{\sum_X \mathrm{P}(X,E)} \qquad (6)$$

Since conventional fault trees are unable to examine the conditional dependencies, this usually leads to underestimation or overestimation of the probability of the top event. As an example, in Fig. 9 the intermediate events E_1 and E_2 share the root cause event X_1. Root event X_1 is considered as a common-cause failure.

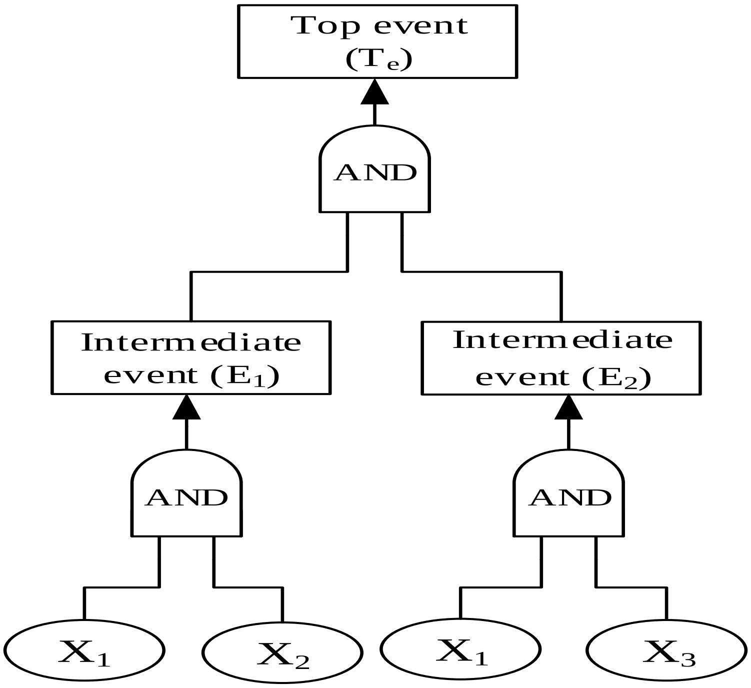

Figure 9: Fault tree having common cause failure X_1

The probabilities of E_1 and E_2, according to the logical relationship in the AND gate will be:

$$P(\mathrm{E}_1) = P(\mathrm{X}_1)P(\mathrm{X}_2) \text{ and } P(\mathrm{E}_2\,) = P(\mathrm{X}_1)P(\mathrm{X}_3) \qquad (7)$$

As E_1 and E_2 are assumed to be independent, the probability of the Top Event (T_e) will be:

$$P(\mathrm{T}_e) = P(\mathrm{E}_1 \cap \mathrm{E}_2) = P(\mathrm{E}_1)P(\mathrm{E}_2) = P(\mathrm{X}_1)^2P(\mathrm{X}_2)P(\mathrm{X}_3) \qquad (8)$$

However, E_1 and E_2 are not independent because they share the common cause X_1. As a result:

$$P(\mathrm{T}_e) = P(\mathrm{E}_1 \cap \mathrm{E}_2) = P(\mathrm{E}_1)P(\mathrm{E}_2|\mathrm{E}_1) = P(\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3) \tag{9}$$

Comparing the probabilities of a top event using Eq. (8) and Eq. (9), the top event of the fault tree given in Fig. 9 underestimates the factor of P(X_1). Therefore, if E_1 and E_2 were connected to T_e using an OR gate, the probability of the respective top event would be overestimated instead. Such a limitation can be minimized by using state-dependent methods such as Markov chains and a Bayesian network (Khakzad, Khan, & Amyotte, 2011).

Chapter 2: Resilience Analysis of a Remote Offshore Oil and Gas Facility for a Potential Hydrocarbon Release

Adnan Sarwar,[1] Faisal KhanI,[1, *] Majeed Abimbola,[1] Lesley James [2]

[1)] Centre for Risk, Integrity and Safety Engineering (C-RISE),

Faculty of Engineering & Applied Science,

Memorial University, St. John’s, NL A1B 3X5, Canada.

[2)] Faculty of Engineering & Applied Science,

Memorial University, St. John’s, NL A1B 3X5, Canada.

Preface

This version of the presented paper has been approved to the journal, *Risk Analysis* in Dec 2017. The lead author, Adnan Sarwar, performed the necessary literature review, developed the model in a Bayesian network, conducted the research analysis and discussion, and developed the manuscript of the paper. The co-author Dr. Majeed Abimbola guided the principal author, while Drs. Khan and James were the principal supervisors of the research and provided expert guidance, technical support and overall editing of the manuscript.

Abstract

Resilience is the capability of a system to adjust its functionality during a disturbance or perturbation. The present work attempts to quantify resilience as a function of reliability, vulnerability and maintainability. The approach assesses proactive and reactive defense mechanisms along with operational factors to respond to unwanted disturbances and perturbation. This paper employs a Bayesian network format to build a resilience model. The application of the model is tested on hydrocarbon-release scenarios during an offloading operation in a remote and harsh environment. The model identifies requirements for robust recovery and adaptability during an unplanned scenario related to a hydrocarbon release. This study attempts to relate the resilience capacity of a system to the system's absorptive, adaptive and restorative capacities. These factors influence pre-disaster and post-disaster strategies that can be mapped to enhance the resilience of the system.

Keywords: Resilience; risk management; hydrocarbon release; offloading operation; harsh environment and Bayesian network

2.1 Introduction

The exploration and production of oil and gas resources are becoming more challenging as they move towards deep water and remote harsh locations such as the Flemish Pass Basin of Newfoundland and the Barents Sea of the Arctic region. To produce these resources in such harsh environments, a combination of a Floating Production Storage and Offloading (FPSO) with shuttle tankers is a more feasible practice for production, processing, storage and transportation. Many efforts have been made to make the FPSO-shuttle tanker offloading system more robust and effective in a hostile environment; however, disruptions still occur due to random natural events (wind, sea ice, sea state, and more), technical errors and equipment failures (Yeo, et al., 2016). In the offshore oil and gas industry, a hydrocarbon release is one of the main precursor events that can escalate to catastrophic events which may result in workforce casualties, asset destruction and damage to the environment and the coastal marine ecosystem (Baksh, Abbassi, Garaniya, & Khan, 2016; 2015). Resilience engineering ensures the design of complex systems that can withstand adverse conditions and recover quickly after disruptions (Agarwal, 2015). It has been recognized as an important characteristic of maritime operations (John, Yang, Riahi, & Wang, 2016). Bakkensen et al. (2016) defined system resilience as the ability of a system to continue its functionality and performance efficiently over the duration a disruptive event. Guikema et al. (2015) identified knowledge gaps related to the vulnerabilities, risk and resilience of modern infrastructure systems that are critical for an improved system performance. Alderson et al. (2015) introduced the concept of assessing operational resilience by identifying critical vulnerabilities and possible disruptions of a continuous operation and encouraging policymakers to promote the resilience of an infrastructure system. They model the quantification of infrastructural operational resilience by evaluating consequences of interconnected components which contribute to the analytical support and enhancement of infrastructure protection.

Considering the characteristics of a remote and harsh environment, offshore infrastructure and associated operations need to be designed so that they are robust, capable of resisting failure causing events and able to recover quickly when disrupted. The dominant method to prevent failures in complex engineering systems has been risk analysis, through risk assessment and management methodologies. The risk analysis paradigm starts with hazard identification, which for a complex system is often challenging, as emerging threats are usually not fully identified (Park, Seager, Rao, Convertino, & Linkov, 2013). This makes risk analysis inadequate to ensure a complete complex infrastructure system's protection. However, the quantification of risk plays a key role in developing strategies to prevent accidents and mitigate their consequences if they occur. Probabilistic risk analysis methods estimate the probability of an accident occurrence in relation to the possible consequences. Furthermore, the concept of resilience extends the scope of risk assessment to deal with strategies to address pre- and post-failure scenarios through preventive, mitigated and recovery measures (Hosseini, Yodo, & Wang, 2014). The difference between resilience and risk approaches is that resilience requires preparing for an unforeseen disruptive event while risk analysis proceeds from the premises where the hazards are identifiable (Holling, 1973; Holling, 1996). The resilience capacity of a system is the ability to not only prevent and protect the system from a disruption but also to improve the restoration of a safer condition. Consequently, resilience assessment thus requires both failure and recovery analysis. A network of closely arranged different complex systems in offshore locations makes the prevention of hydrocarbon release a greater challenge. Hydrocarbon releases are the primary contributors to major accidents in the oil and gas industry (Øien, 2001; Snorre, 2006), especially during offloading operations and transportation to onshore transshipment terminals. One main advantage of using a FPSO for such operations is the capability to store crude oil in cargo tanks and then offload it to shuttle tankers using tandem offloading operations (Chen, 2003).

The objective of this research is to develop a resilience model for an offshore oil and gas facility to assess the potential of a hydrocarbon release during offloading operations. The resilience model is based on a Bayesian network (BN) format for a probabilistic dependability analysis. The model is tested for a hydrocarbon release during offloading and transportation operations considering two different scenarios. The frequent offloading operations, along with long transportation routes in harsh environments characterized by adverse weather conditions, such as sea ice, icebergs, high waves, low visibility and very low temperatures, severely affect the safety of the tandem offloading system between a FPSO and the shuttle tanker. The risk of a hydrocarbon release in the aforementioned circumstances is thus high, considering the impact of environmental conditions on the closely positioned floating structures (Yeo, et al., 2016). This research work proposes a resilience model as a function of reliability, vulnerability and maintainability (explained in Section 4) of an engineered system. The model considers the reactive and proactive capabilities of a system and their integration in defining the resilience of the system.

The paper is structured as follows: Section 3.2 defines the concept of resilience. Section 3.3 discusses basic BN concepts relevant to resilience assessment. Section 3.4 presents the development of the resilience model while in Section 3.5, the implementation of the model is demonstrated. Section 3.6 highlights the results of the analysis and discussion, including a sensitivity analysis to validate the proposed model. The concluding remarks are presented in Section 3.7.

2.2 The Concept of System Resilience

System resilience is the ability of a system to efficiently reduce the magnitude and duration of deviation during a disruption (Vugrin, Warren, & Ehlen, 2011). The Presidential Policy Directive (PPD) (2013) which defines resilience for critical infrastructure systems as the ability to predict, withstand or adapt and/or recover capability from hazards or disruptive events. This definition was later accepted by the National Academy of Sciences (Cutter, et al., 2013) and Ganin et al. (2016). Arsenault and Sood (2007) defined the concept of a resilient organization as one that is capable of deflecting deliberate attacks and environmental disruptions (or their effects), absorbing unavoidable damages and resuming operations to pre-event levels, all with the utmost speed. According to Haimes (2009), infrastructural resilience systems withstand major disruptions within acceptable degradation parameters and recover them with maintainability features within an acceptable time period, composite costs and risks. Johnsen et al. (2005) associate resilience with an appropriate strategy to be used in any system to follow complex and uncertain induced risk factors. According to Thiago et al.

(2006) the main objective of a resilient approach is to identify the disturbances in a system that degrade performance level and then study how these degrading factors may be mitigated to increase the performance level. Hosseini et al. (2016) discuss resilience as the intrinsic ability of a system to adjust its functionality in the presence of disturbances, external threats and unpredicted changes, and to withstand internal and external disruptive events without letting the system become discontinuous by performing system functionalities. If the system is disrupted, it should have the capability to recover its functionality within a defined period of time by adapting the available maintainability features such as onsite maintenance, management of available resources, standardization of the system and more. Maintainability is a measure of how easily the system is restored to a specified condition within a defined period of time (Ebeling, 1997). Moreover, Keogh and Cody (2013) defined resilience as the robustness and recovering characteristics of utility infrastructure and operations that avoid or minimize the interruptions of service during an extraordinary and hazardous event.

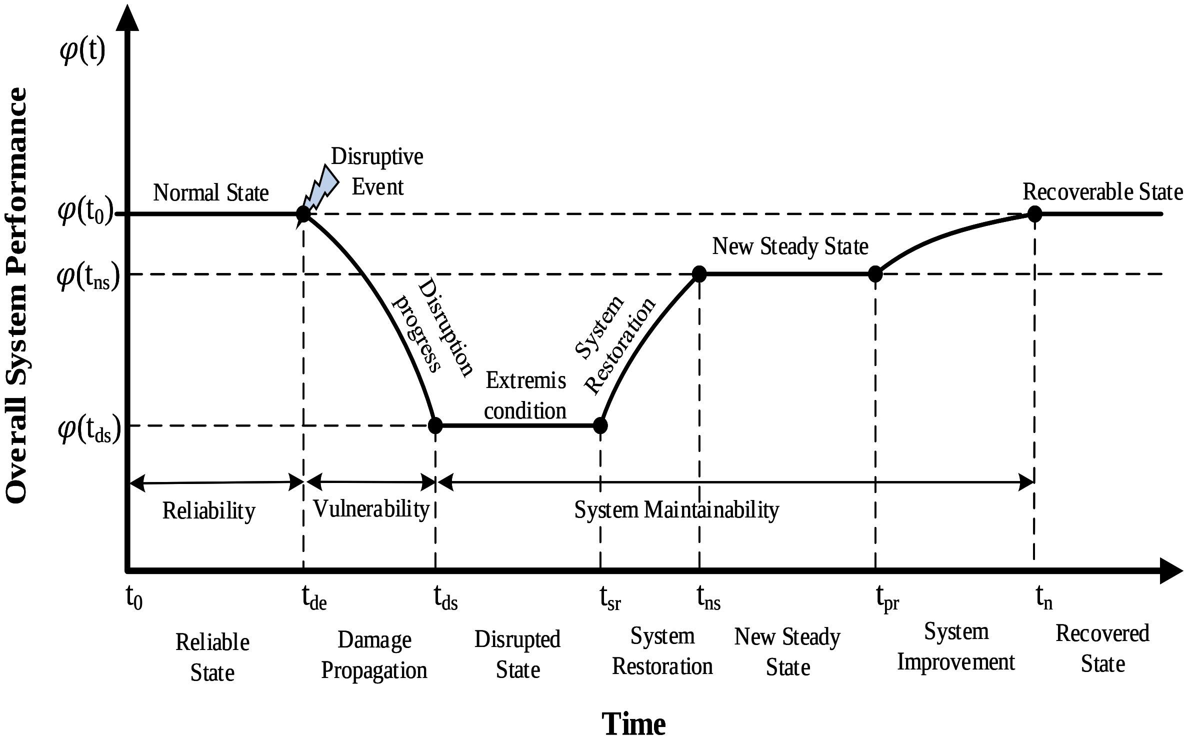

Figure 10: States and performance (delivery) evolution in time. Adapted and modified from (Hosseini & Barker, 2016)

Figure 10 illustrates the aspects of resilience concept which include: system *reliability*, *vulnerability* and *maintainability*. Fig. 10 demonstrates how resilience, $\varphi(t)$, as a concept, evolves as a function of time given that a disturbance event occurs. Hosseini et al. (2014) propose assessing a system's resilience in the presence of internal and external disruptions by exploiting the concepts of *reliable* state, *vulnerable* state, *new steady* state and *recoverable* state. The reliable state is a normal or baseline state where the system performs its task normally. The *vulnerable* state occurs when the system undergoes disruptions or failures. The recoverable state is a restoring state that results from restoration by maintenance. The new steady state is the new acceptable performing state resulting from the application of enhanced recoverability features.

Fig. 10 shows how a system goes from the vulnerable state to the disrupted state after it undergoes a disruption. In the event of a disruption such as harsh weather, at the time (t_{de}), the hydrocarbon offshore offloading system should be able to adapt to the emergent conditions. $\varphi(t_0)$ represents the assessment of resilience at time t_0, which is the initial *reliable* state. Resilience demands that the system hold a high value of $\varphi(\mathrm{t})$ at $t = t_0$ for better adaptability. With an initial failure event at $\varphi(t_{de})$, the resilience decreases significantly to $\varphi(t_{ds})$. Now, the impact of a failure event can be estimated by the difference, $\varphi(t_{ds}) - \varphi(t_0)$, that helps to determine the appropriate corrective measures before applying them at t_{sr}. The initial restoration to state $\varphi(t_{ns})$ is an intermediate arrangement because, the system may take longer to be fully restored, i.e., $(t_n - t_{ns}) > (t_{ns} - t_{sr})$, to the final *recoverable* state, $\varphi(t_n)$. The way (for example, how fast, and how many intermediate post-restoration states there might be) a system progresses from state $\varphi(t_{ns})$ to $\varphi(t_n)$ depends on various factors, such as the strength of the system to withstand a disruptive event, the severity of the disruption, the adaptability of the system and the response processes, which are divided into stages, such as $(t_0 \leq t \leq t_{de})$, that show resilience during normal operations.

2.3 Bayesian Network (BN)

The inference probabilistic technique based on Bayes' theorem is widely used for safety and risk assessment of complex systems having uncertain information. It computes the posterior probability of an unobserved dependent variable that is conditionally dependent on some observable variables. It illustrates the problem in an abstract form through a directed acyclic graphical representation, composed of connected nodes with initial and intermediate events, based on the functional decomposition of the system (Weber & Jouffe, 2006; Hosseini & Barker, 2016). The BN analysis is not static and has advantages compared with other techniques, to overcome their limitations. The principal reason to use BN analysis is that it enables the modeling of complex systems by incorporating new evidence to reduce parametric uncertainty, which is often difficult with other conventional techniques such as a fault tree (FT) and an event tree (ET) (Yeo, et al., 2016). BN is a useful technique to represent the analysis of data, the testing of expert knowledge and its presentation, that are related to the conditional dependencies among variables in an uncertainty model (Wiegerinck, Kappen, & Burgers, 2010; Yeo, et al., 2016).

Figure 11 illustrates the directed acyclic graphical (DAG) presentation, composed of connected nodes with basic events, intermediate events and the top event based on the functional decomposition of the system. In Fig. 11, the BN structure for probabilistic analysis, RN, represents root nodes which are those nodes without child nodes, (like the primary events in FT); IN represents the intermediate nodes (referred to as intermediate events in FT), and PN denotes the pivot node (top event in FT) which shows the possible output in terms of resilience through system reliability, vulnerability and maintainability (Jensen & Nielsen, 2007). A set of conditional probability tables (CPT) represents the dependence relation and the arrow represents the causal relationship and sensitivity link amongst variables (Khakzad, Khan, & Amyyotte, 2013; El-Gheriani, Khan, & Zuo, 2017).

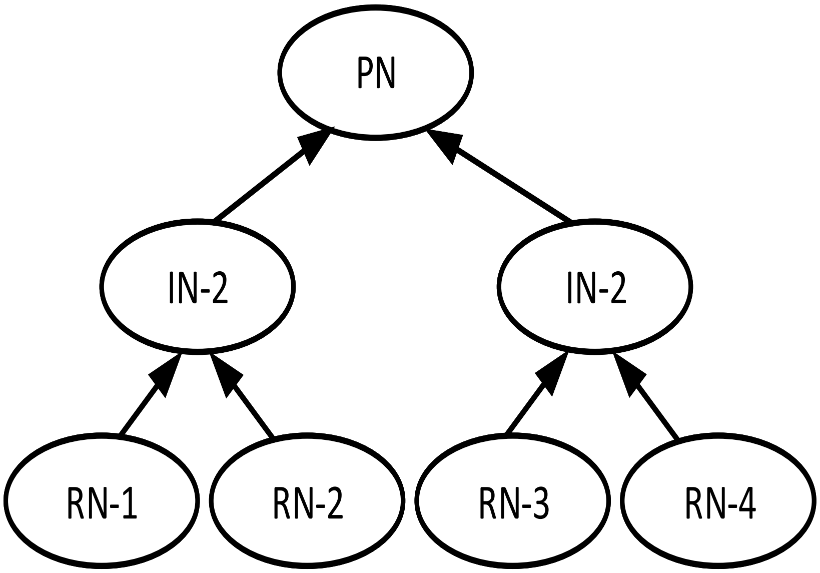

Figure 11: Simplified structure of BN model, arrow represents causal relationship among nodes through probability distribution functions

The quantitative analysis has been performed based on the d-separation principle where basic events are conditionally independent and intermediate events are dependent on their influenced parent nodes. The BN represents the joint probability distribution of variables based on conditional dependencies in the network as: $P(X) = (x_1, x_2, \dots, x_n)$.

$$P(X) = \prod_{i=1}^{n} P(x_i)|Pa(x_i) \tag{10}$$

In Eq. (10), $Pa(x_i)$ represents the set of parent nodes of x_i in the DAG presentation and $P(X)$ reflects the properties of BN (Jensen & Nielsen, 2007). The advantage of BNs to allow prior probability updates with new information is called evidence, E. Updated or posterior probabilities can be calculated as in Eq. (11):

$$P(X|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_{U} P(U,E)} \tag{11}$$

Equation (11) can be used either for prediction or updating probability. For instance, Eq. (11) can be explained in terms of predictive analysis, where the conditional probability, $P(vulnerability|events)$, indicates that the existence of vulnerability in a system is dependent on the occurrence and non-occurrence of disruptive events. Moreover, for updating a scenario, $P(events|vulnerability)$ shows that the occurrence probability of certain disruptive events leads to the vulnerability of a system (Khakzad, Khan, & Amyotte, 2011; Przytula & Thompson, 2000).

A BN can be used to perform both predictive (forward) and diagnostic (backward) analysis. In predictive analysis, the marginal probabilities of intermediate and pivot nodes are computed on the basis of marginal prior probabilities of root nodes and conditional probabilities of intermediate nodes. However, for diagnostic analysis, the states of some nodes are instantiated, and the updated probabilities of conditionally dependent nodes are calculated (Bobbio, Portinale, Minichino, & Ciancamerla, 2001; Khakzad, Khan, & Amyotte, 2013).

2.4 Resilience Assessment Methodology

As mentioned earlier, this study model's resilience as a function of reliability, vulnerability and maintainability. Reliability (R) is the probability that a system will perform a required function for a given period of time under specific operating conditions (Ebeling, 1997). Vulnerability (V) measures the system failures during and after a disruption. Maintainability deals with the ease of restoration of the system to a normal state within a period of time (Ebeling, 1997). The maintainability (M) of a system is used as a key factor to consider when restoring the system to its recoverable state. A system's functionality returning to the normal state requires it keeping a high maintainability value. This would, in turn, lower the effect of vulnerability. The effects of vulnerability and maintainability are hence inversely proportional to each other. Holling (1973; 1996) defined the ecological resilience concept as "the magnitude of disturbance that can be absorbed before the system changes its structure by changing variables and processes that control behavior". Deduced from the definition of resilience by Youn *et al.* (2011), the resilience of an engineered system can be expressed as the summation of a system's passive survival rate (i.e. *system reliability*) and proactive survival rate (i.e. *system recovery*), as represented in Eq. (12).

$$\text{Resilience } (\varphi) \triangleq \text{Reliability (R)} + \text{Recoverability } (\eta) \tag{12}$$

In Eq. (12), recoverability *(η)* is a function of vulnerability (V), represented as (1-*R)* and restoration (*ρ).* Restoration (*ρ)* measures the ability of an engineered system to maintain its performance and restorative capacity when subjected to a disruption. The restorative capacity of a system is a function of its maintainability (M). By considering the recoverability function of a system, the resilience can be formulated as shown in Eq. (13).

$$\varphi \triangleq \mathrm{R} + \ \mathrm{\eta}[(1-\mathrm{R}), \mathrm{M}] \tag{13}$$

In Fig. 12, a framework describing the relationships among the involved generic variables is proposed. Based on these relationships, the proposed base model has *resilience (R)* as a leaf output node, which is dependent on three parent variable nodes, *reliability (R)*, *vulnerability (V)* and *maintainability (M),* to quantify the overall resilience of the designed system. In the model, the main function of maintainability, which is dependent on influencing design and operational factors, is to bolster the system's vulnerability by reducing the disruption level through different strategies, such as distribution and management of resources, availability of trained staff on site to keep the work strategy unified, which will be easily incorporated by workers and the availability of maintenance on site, in order to avoid disruption and achieve quick recovery. The influencing design factor is divided into two roles: 1) The proactive strategy is meant to achieve higher system availability by using strong absorptive and adaptability features before and during disruptive events. 2) The reactive design strategy has the capability of adaptability as well as restoration during and after a disruption. The advantage of this model is that it can be applied to any complex system to analyze and identify resilience. Since there is a general understanding of reliability further detailed discussions are only provided for system vulnerability and maintainability.

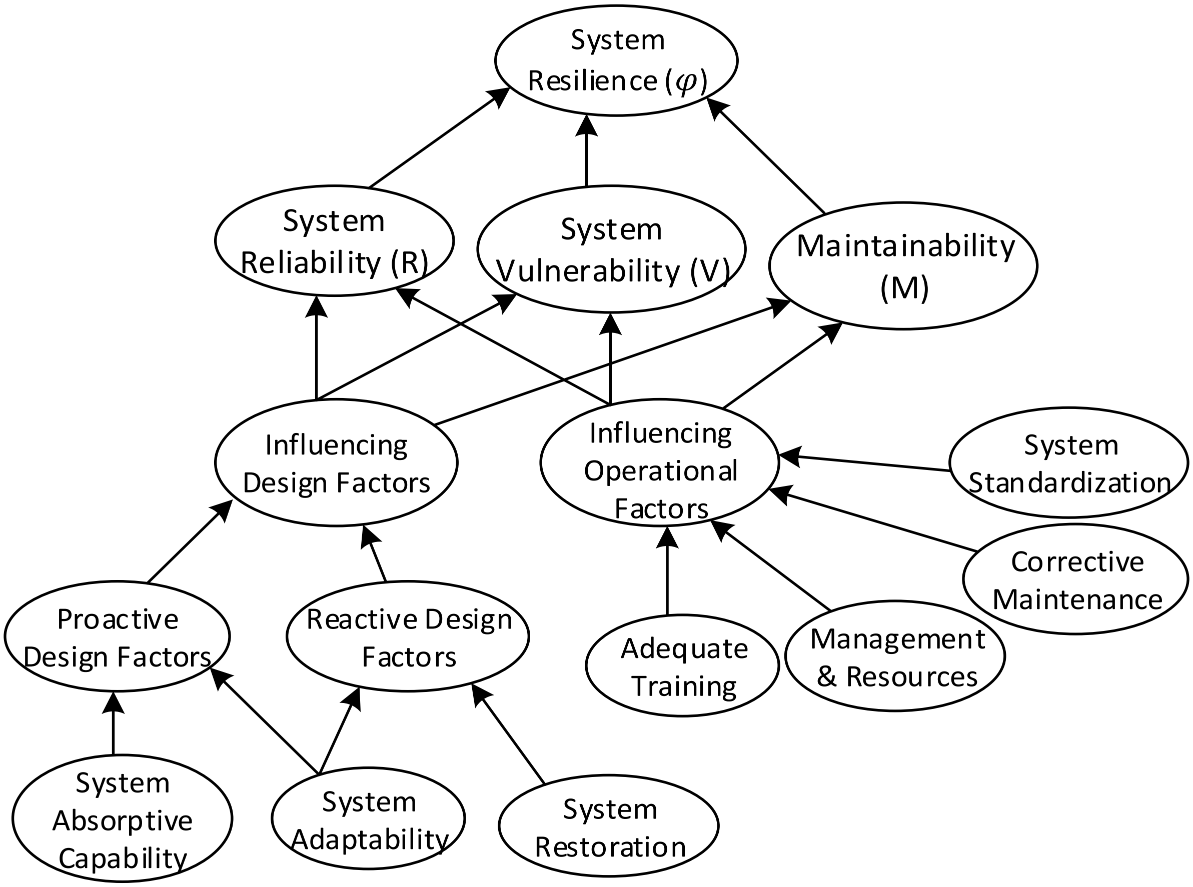

Figure 12: The proposed BN resilience model

2.4.1 Modeling Vulnerability

Vulnerability of a system is modeled as the failure state into which the system enters when it is no longer in a normal/stable state. This could be due to an error at the design level of the system (Sheffi, 2005) or operational failures or errors in the operational state of the system. Operational failures may occur irrespective of the existence of design errors. One instance would be the high waves in harsh offshore environments that make it difficult to maintain the standard distance keeping and position management that are required between a shuttle tanker and FPSO. Johansson *et al.* (2013) defined the term vulnerability as the inability of a system to withstand a failure. Vulnerability analysis is performed to identify the major factors that contribute to the cascading failures of systems (internally or interdependently). Thorisson *et al.* (2017) proposed the concept of resilience analysis in terms of identifying stressors (single or multiple) that affect the overall performance of the system. Khakzad and Reniers (2015) defined the concept of vulnerability analysis as an explanation of weakness and critical components failures that can affect the system performance, which is different than traditional risk analysis because of its ability to identify hazardous events, their possibility and potential consequences. Jönsson *et al.* (2007) defined vulnerability as the extent of damage done by the presence of disruptive events to the system which are dependent on the type and level of disruption.

In this study, vulnerability analysis used as a network with two different perspectives: (i) influencing design factors and (ii) influencing operational factors. Influencing design factors can be interpreted as the consideration of proactive and reactive approaches to risk management, and inherent safety design aspects that are able to withstand abnormal scenarios. This interpretation of vulnerability modeling can be useful during a system design stage to select a robust strategy. The influencing operational factors can enhance the system's operation and performance. Included in these two general factors, several technical and design issues may be addressed. This work intends to focus on seven major factors where the design factors are further classified into *proactive* and *reactive* design strategies. These design strategies serve as the basis for incorporating the notions of *system adaptability*, *system absorptive capability* and *system restoration* (Vugrin, Warren, & Ehlen, 2011). The operational factors considered here are: adequate training, management and resources (Hosseini & Barker, 2016), corrective maintenance (Arora, 2004; Kumar & Suresh, 2008), and system standardization (Chen & Moan, 2004; Bazerman, 1998). The above-mentioned factors affect the vulnerability function, as shown in the proposed model.

2.4.2 Modeling Maintainability

As discussed earlier, maintainability is the ability of a system to withstand disruptions and be restored. It measures the duration of maintenance outages to restore the system back to its original position. Maintenance is an essential component of the system and needs to be performed within a set amount of time, regardless of the conditions present. This can be achieved by providing staff with adequate training, such as specific skills, procedures, and resources (Barringer, 1997). System equipment design can also determine maintenance procedures and the length of repair time. There are several factors to be considered in accounting for a system's total down time. These include: diagnostic process, active repair time, removal/replacement, resource management, standardization of equipment, and system absorptive, adaptive and restorative capabilities to avoid system failure or to keep repair time short. As shown in Fig. 12, high maintainability raises the system's resilience. Consequently, to increase the system's maintainability design, and operational factors must be considered. These factors must have been designed so that the system is protected before, during and after a failure. This will help to achieve maximum resilience and recovery, which will be discussed further in the following subsections.

2.4.3 Modeling Design Factors

The design factors are those features that are taken into consideration at the time of system design. This involves two types of strategies, a proactive strategy and a reactive strategy (Hosseini, Barker, & Ramirez-Marquez, 2016). The proactive design strategy defines those factors that need to be considered before and during the initiation of any disruptive/failure events. The reactive strategy considers the factors that influence the system resilience during and after the occurrence of disruptive events.

2.4.3.1 Pro-active and re-active design factors

The proactive and reactive strategies are further subdivided into three categories, where the model incorporates input by associating problem specific nodes: (a) *system absorptive capability* measures the ability to absorb the impact of disruptive events and present defined mechanisms to withstand the disruption; (b) *system adaptive capability* calls for certain arrangements that help the system adapt to the impact of disruptive events; and (c) *system restoration capability* is a permanent feature of the system, unlike adaptive capability, where temporary arrangements may be made to make the system functional (Hosseini & Barker, 2016; Vugrin, Warren, & Ehlen, 2011). A system with restorative capability may offer permanent solutions for damage from an incident. For instance, if a pipeline is ruptured, then a restorative strategy will call for a replacement of the portion of the damaged pipeline, whereas an adaptive capability may mean many different arrangements. The adaptive arrangements may include dropping flow pressure or closing the valve or may involve using a temporary fix to the ruptured portion of the pipe. Restorative capability often means high cost repairs, due to their permanent nature.

2.4.4 Modeling Operational Factors

The factors that are required to enhance the system performance and enable it to operate efficiently in order to achieve its high maintainability are considered here. Five operational factors related to the oil and gas industry are identified. These are adequate training of workers, effective management of resources, corrective maintenance and system regulation with standardization (Fleming, Gordon, Flin, Mearns, & Fleming, 1996; Gordon, 1998).

3.4.4.1 Adequate training

Adequate training is represented as a logical-OR variable in the system with possible values such as adequate and inadequate training of workers. Inadequate training may involve a discrepancy, a lack or a deviation from standards in operating and safety procedures. There are four major factors which constitute adequate training, namely: *manning competence*, *lessons learned*, *toolkit training* and *best practices*. Only logical-OR values are considered, so that the model will consider the staff competent if the value is true; otherwise, the staff is said to be incompetent and requires further training. Similarly, for a lesson learned—primarily consisting of a result of root cause analysis of failures—the model takes the values as true if the staff learns from experience. The other two factors in adequate training are the toolkit training and good practice guidance, which are proactive measures, also modeled as logical-OR variables.

3.4.4.2 Management and resources

This node considers factors that are essential in good system management. For example, “under-manning” is a condition that can overload’s existing operators, which gives rise to operator fatigue. Similarly, the workload can be demotivating at times, leading to a reduction in an operator’s performance.

3.4.4.3 Corrective maintenance

Corrective maintenance is considered an essential element of complex system’s operations, which will ensure high consistency in an offshore facility, especially in harsh operating environments which cause a high frequency of failures, requiring different kinds of preventive maintenance. There are four major types of maintenance philosophies to be considered, namely: (a) *Preventive maintenance,* which is performed on a system at predetermined intervals during its expected life or operations. The system is ideally replaced or repaired before it breaks to avoid downtime with the help of regular facility inspections (Kumar & Suresh, 2008; Fedele, 2011). In most cases, such maintenance is better than “run-to-failure” maintenance; the mean time between failures is often hard to establish for a well-maintained system that seldom leads to downtime and complete shutdowns (Mobley, 2002). (b) *Predictive maintenance* is performed through non-destructive techniques and technologies (visual monitoring, microprocessors, SCADA system, instrumentation and more), to detect, identify and prevent machine failures at the most opportune time (Rabelo, 1998; Mobley, 2002; Fedele, 2011). This involves diagnosis through specific measurements of some degradation processes (vibration monitoring, tribology, thermography and more) prior to the occurrence of any significant deterioration. This philosophy helps to reduce frequent machine breakdowns, create a necessary spare parts inventory at site, avoid unforeseen downtime and achieve a higher availability of the system. (c) *Proactive maintenance* can be identified by its 'failure-oriented' nature and is the first line of defense, performed only for essential components and providing a pre-alert signal of failure with sufficient lead time for an operator. It targets the root causes of the possible deterioration rather than involving routine repairs. Thus, it involves a thorough inspection of a system and condition monitoring to evaluate imminent failures (Fitch, 1992; Fedele, 2011). (d) *Periodic maintenance* is time based maintenance performed on the equipment at regular intervals made by its user, even if the system is in working order. This involves a series of certain preventive measures and elementary tasks which may not require advanced training (lubrication, retightening valves, checking seals and pressure gauges and more). These four types of maintenance strategies used in the model contain Logical-OR nodes that deal with the presence or absence of these strategies.

3.4.4.4 System standardization

The general purpose of system standardization is to assess whether the system is following standard operating procedures for good decision making (Bazerman, 1998). However, Chen (2003) proposed a standardization technique that is used particularly in drive-off scenarios. This technique provides operational guidelines to standardize an operator’s attention to the data that is of utmost importance in a drive-off situation. It minimizes recurrent screen checks so that more focused attention on diagnosis and situation awareness can occur within a short time, which is useful in decision making. Offloading operations considered in this case study require four logical factors in order to ensure system standardization. These are: (a) *Relevant met-ocean data*, (b) *Equipment calibration schedules*, (c) *Avoiding failure data*, and (d) *Procedures and documentation.*

2.5 Case Study: Hydrocarbon Release Resilience Model During Offloading Operations

Step Change in Safety (2015) states that a hydrocarbon release is one of the major concerns or key performance indicators for offshore installation integrity. To present a working example of the proposed resilience model in Fig. 12, a case study of hydrocarbon release during an offloading operation from an FPSO to a shuttle tanker is analyzed using BN (see Fig. 13). According to the Canada-Newfoundland Labrador Offshore Petroleum Board (C-NLOPB) (2016) reports, the offloading operation is one of the major contributing factors for the release of hydrocarbons. The proposed model identifies the disruptive events for the selected scenario with the series of sub-events which indicate the vulnerability of the system. To estimate the vulnerability in the system, prior probabilities are assigned to the root nodes and the conditional probability table is developed based on previous research and expert judgment. Similarly, the maintainability of the system is presented to avoid and overcome the disruptive effect of failure events by keeping the system resilient and trying to return it to the original state. The initiating causes identified in this case study serve as evidence for the BN model. Based on congregated information and the quantitative relation among factors or nodes, the potential resilience of a given system is quantified. This study concludes that the contributing factors that sustain a system's maintainability consequently reduce vulnerability and thus increase system resilience.

In applying the proposed methodology to the case study, the following possible contributing factors are considered:

2.5.1 Contributing Factors for Offloading Operations Case Study

The contributing factors for offloading operations include: system absorptive capability, system adaptability and system restoration, as further discussed below.

3.5.1.1 Factors in system absorptive capability

Four major factors have been identified for the case study of the offloading operation that constitute the absorptive capability. These factors are as follows:

– *Offloading monitoring system*. The main responsibility of this system is to monitor hose connections, the bow loading system and the overall facility. The hose connection system deals with delivering oil under high pressure from the FPSO to the shuttle tanker. This system monitors the security of hose connections on the FPSO and the shuttle tanker, the durability and longevity of floating hoses and the valve control system that controls the oil flow, and checks joints for possible ruptures. The facility monitoring system eliminates chaotic equipment/structural vibrations so that it remains within the defined threshold range (Thomsen, 2003). Sensor malfunctions and erosions are monitored, and seals are checked for leakages. The bow loading operation deals with the telemetry system, which helps to initiate, control and terminate hydrocarbon release between a shuttle tanker and an FPSO by maintaining a parallel and duplicate fail-safe UHF transceivers' link (Norwegian Petroleum Industry, 2015). This helps to avoid the communication errors and a controllable/variable pitch propeller to allow the shuttle tanker to securely and efficiently offload hydrocarbons from an offshore production storage facility.

– *Hydrocarbon release prevention plan.* The hydrocarbon release prevention plan is one of the key performance indicators for installation, asset integrity and performance. The prevention plan identifies sensitive zones that are prone to hydrocarbon release and organizes preventive measures in terms of sensitive zone distribution and the zones' isolation from sources of ignition and electrical shocks, providing extra protection during oil spillage incidents (McGillivary & Hare, 2008; Turner, Skinner, Roberts, Harvey, & Ross Environmental Research Ltd., 2010). Offshore oil and gas operators are responsible for a robust and immediate reaction plan if an oil spillage event occurs, and they work closely with spill specialists and authorities (Turner, Skinner, Roberts, Harvey, & Ross

Environmental Research Ltd., 2010). Hydrocarbon release prevention planning also includes an adequate flow control and level monitoring. Monitoring and assessing the spill's trajectory is a top priority. Following that, an operator must quickly mobilize the appropriate material and equipment.

– *Facility protection*. This system is included in the model to incorporate elements that protect the entire offloading facility. Here, it is ensured that the telecommunication links are secure and operable, especially in harsh weather. Corrosion management and adherence to acceptable limits are taken into account, as external corrosion causes more than 90% of damage leading to failure in distribution (Fesseler, Baker Jr., & Inc., 2008). Maintaining a minimum distance of approximately 80 to 90 meters between the shuttle tanker and the FPSO prevents a collision (Vinnem, 2003; Chen, Lerstad, & Moan, 2010). Lastly, any erroneous operation that may be caused by technical errors and/or failure of communication between the FPSO and shuttle tanker, mostly as a result of the two prone situations (surging and yawing caused by excessive fishtailing motion and heading deviation), should also be eradicated by improving the safety of offloading operations from both design and operational perspectives (Chen & Moan, 2002).

– *Platform safety*. These are general safety features that encompass: *alarm systems*, *hydrocarbon release detection systems,* and *operating threshold systems*. The corresponding node takes a logical-OR value, that is, the presence or absence/failures of such systems. Hydrocarbon release detection plays a significant role in safe and secure offloading operations. The petrochemical industry employs various methods of leak detection, such as infrared detectors, acoustic leak detectors, flame ionization and more, to improve overall platform safety (Abdel-Moati, Morris, Ruan, & Zeng, 2015). The operating thresholds include harsh weather conditions, such as wave height, wind intensity, low visibility and the presence of ice. These situations can potentially disconnect the offloading system, especially in the Flemish Pass Basin, because harsh weather most frequently misaligns the angle of deviation between vessels (Williams, Brown, Shaw, & Howard, 1999).

3.5.1.2 Factors in system adaptive capability

These include: *emergency shutdown system* (Sklet, 2006), *position keeping management*, *distance keeping* and *avoiding drive-off* (Chen, 2003).

– *Emergency shutdown system*. The emergency shutdown system prevents any chaotic situation that can occur at a facility by observing hydrocarbon leakage, spread and overflow. It also prevents ignition, explosion and fatalities and protects an asset's integrity (Sklet, 2006).

– *Position keeping management*. This node is dependent on the following factors: (a) *Position reference system* monitors the position of the FPSO and the shuttle tanker by using available position data logs with a reference system, i.e. DARPS (Differential Absolute and Relative Position Sensor) (Chen, 2003). (b) *Dynamic positioning system* promotes an automatic safe positioning and heading angle of the shuttle tanker (Norwegian Petroleum Industry, 2015). (c) *Avoidance of risky maneuvering* may occur between the shuttle tanker and the FPSO during an offloading operation during connection, loading and disconnection (Rodriguez, Martha de Souza, & Martins, 2009).

According to Rodriguez *et al.* (2009) a hazardous event can occur due to programming errors of the shuttle tanker's automation system and misjudging maneuverability conditions. To overcome this problem, assistance from a nearby standby vessel is requested to correct and track the position of the shuttle tanker. (d) The *vessel motion monitoring system* is responsible for improving the safety and efficiency of operations by using accurate motion data.

– *Distance keeping* during tandem offloading means that the shuttle tanker needs to maintain a certain distance from the FPSO to avoid a collision, depending on the conditions. To minimize tension on the hawser and the loading hose, the tanker adjusts its own dynamic positioning system or Taut hawser mode to obtain the maximum uptime in a harsh environment, using the adaptable features (Chen, 2003).

– *Avoid drive-off* means that the shuttle tanker needs to avoid unwanted and unplanned movement from the FPSO due to the tanker's thrusters, and keeps the reference position stable during an offloading operation. Most of the drive-off scenarios are considered forward drive-off in default unless they are astern or sideways. The drive-off initiates if there are errors in the system's hardware or software, excessive relative vessel motion, or complex operator and machine interactions (Chen, 2003).

3.5.1.3 Factors in system restorative capability

The case study uses restorative capability from a failure's detection to the repair phase. The factors included are: (a) *early detection* of failure causes, (b) *available workforce,* (c) *onsite restoration facilities* and (*c*) *reactive maintenance*.

– *Early detection* refers to swift situation awareness during different scenarios, such as drive-off, to reduce the reaction time of the operator. When the first abnormal signal is identified, the operator requires some time to analyze the situation, which needs quick formulation and accurate execution of recovery action (Chen, 2003).

– *Available workforce* is the human-based resources, e.g. skilled labor, operators and engineers, to ensure a timely and coordinated response.

– *Reactive maintenance* is described as a remedy to adjust failures or incidents by replacing broken parts or tools and allowing the equipment to run until failure occurs (Swanson, 2001). The damaged equipment is later repaired or restored, which is usually undertaken as a result of unplanned downtime or failure. This maintenance reduces the manpower and budget spent to keep the equipment operational (Paz & Leigh, 1994).

– *Onsite restoration facilities* are the equipment restoration resources which are, for example, based on availability of a workshop and spare equipment for repair that must be present at the site to eliminate downtime, strengthen the ability of the facility to withstand disruptions and maintain continuity of site operations (Hosseini & Barker, 2016).

3.5.1.4 Management and resources

Preventing hydrocarbon release should be a major goal of facility operators, and can be achieved by effective management and appropriate resources. There are three major factors identified in offloading operations which can prevent a hydrocarbon release. These are to avoid *lack of motivation* and *operator fatigue* and to promote *safety culture*. Safety meetings and safety reviews must be included to develop a proper safety culture at oil and gas facilities. The authors define operator fatigue as a type of human error that may serve as a potential cause of hydrocarbon release.

For this research, the prior probabilities of the basic evidence nodes (i.e. root nodes or causal risk factors) of this case study are sourced from previously conducted related research as well as expert opinions on rare events data, as shown in Table I on next page.

Table I: Generic BN evidence nodes probabilities (Abimbola, Khan, Khakzad, & Butt, 2015; Khakzad, Khan, & Amyotte, 2011; OREDA, 2002; Song, Khan, Wang, Leighton, & Yuan, 2016; Sun, Kang, Gao, & Jin, 2016; Hosseini & Barker, 2016; Chen & Moan, 2004), (Chen, 2003) and expert opinion.

Node Symbol	Node description	Failure Probability	Node Symbol	Node description	Failure Probability
E_1	Equipment vibration	9.5E-02	E_{27}	Position reference system	2.0E-03
E_2	Malfunction of sensors	1.9E-03	E_{28}	Dynamic positioning system	5.0E-04
E_3	Erosion	7.6E-03	E_{29}	Avoid risky maneuvering	7.9E-03
E_4	Seals	1.2E-01	E_{30}	Vessel motion monitoring	1.0E-01
E_5	Shuttle tanker (ST) hose connection	1.1E-01	E_{31}	Distance keeping	3.8E-02
E_6	Hose Ageing	1.7E-01	E_{32}	Avoid drive-off	5.4E-03
E_7	Joints rupture	4.5E-02	E_{33}	Early detection	7.2E-05
E_8	Valves control system	1.0E-03	E_{34}	Available workforce	1.0E-01
E_9	Telemetry system	2.4E-02	E_{35}	Re-active maintenance	2.3E-03
E_{10}	Communication	6.2E-03	E_{36}	Onsite restoration facility	1.7E-01
E_{11}	Controllable pitch propeller	1.8E-02	E_{37}	Manning competence	2.7E-01
E_{12}	Zones classification in terms of sensitivity	1.5E-01	E_{38}	Lesson learned	1.0E-01
E_{13}	Adequate flow control	1.5E-02	E_{39}	Tool kit training	1.6E-03
E_{14}	Level monitoring	1.0E-05	E_{40}	Good Practice Guidance	1.0E-03
E_{15}	Oil spillage preparedness program	1.0E-01	E_{41}	Lack of motivation	1.6E-03
E_{16}	Avoid Collision	3.1E-03	E_{42}	Prevent operator fatigue	1.0E-03
E_{17}	Erroneous operations	3.3E-03	E_{43}	Safety culture	1.0E-03
E_{18}	Corrosion management	3.7E-03	E_{44}	Facility Inspection	1.0E-04
E_{19}	Secure connection	9.9E-02	E_{45}	Avoid downtime	4.4E-03
E_{20}	Malfunction of alarm system	9.0E-03	E_{46}	Pro-active maintenance	1.7E-03
E_{21}	Hydrocarbon release detection system	2.3E-03	E_{47}	Periodic maintenance	1.9E-03
E_{22}	Tension cause by waves height	4.5E-02	E_{48}	Predictive maintenance	7.0E-04
E_{23}	High wind intensity	1.0E-01	E_{49}	Procedures and documentations	7.0E-03
E_{24}	Low visibility	5.5E-04	E_{50}	Avoid failure/irrational data	1.0E-02
E_{25}	Ice management	1.0E-01	E_{51}	Equipment calibration schedules	6.0E-04
E_{26}	Emergency shutdown system failure	1.3E-04	E_{52}	Updated relevant met-ocean data	1.0E-02

2.6 Results & Discussions

The operation of transferring hydrocarbons involves a combination of different systems, i.e. electrical, mechanical, electro-mechanical, electronic sensors and communication systems. Due to the complex interaction of the systems involved, there are many factors affecting the efficient delivery of the hydrocarbons to the destination which can result in hydrocarbon release—a phenomenon of vital interest in the oil and gas industry (Chen & Moan, 2004; Sun, Kang, Gao, & Jin, 2016) especially in harsh environments such as Newfoundland (C-NLOPB, 2016).

2.6.1 Identifying Variables

A BN is developed to quantify resilience by considering relevant Boolean variables with failure probabilities adopted from different sources, with expert judgments for rare events (Table I). The outcome of these variables is categorized into two states, the *True state*, representing a positive outcome and the *False state*, representing a negative outcome. Similarly, High/Low states, are the counterparts of True and False states. For example, BN analysis demonstrates that an adequate flow control has a failure probability, as illustrated in Table I, where False = 1.5E-02 and True = 9.85E-01, which suggests that 98.5% of the time the adequate flow control is successful, and 1.5% of the time such activity fails during an offloading scenario. The identified relevant factors for the given case study, where each factor represents an evidence node, are considered as inputs to the model.

Table II illustrates the conditional probability table for the resilience node with two possible states of high and low resilience, which are dependent on the relative weighted sum of the parent nodes of system vulnerability and maintainability. To model the causal influence of parent nodes on system resilience, the Noisy-OR function is adopted. For instance, if maintainability of the system is high with a low system vulnerability the system resilience will be 98%. A similar explanation holds for other node states.

Table II: Conditional probability table for the resilience node given the value of maintainability and vulnerability

Maintainability (M)	High				Low			
Vulnerability (V)	Low		High		Low		High	
Reliability (R)	High	Low	High	Low	High	Low	High	Low
High	9.8E-01	8.5E-01	9.2E-01	8.5E-01	7.2E-01	6.5E-01	1.1E-01	1.0E-02
Low	2.0E-02	1.5E-01	8.0E-02	1.5E-01	2.8E-01	3.5E-01	8.9E-01	9.9E-01

Baseline scenario

The baseline scenario comprises the standard mode in which all the factors are working perfectly. This reflects the best practice that is followed in an offloading operation, as shown in Fig. 13. The model calculates the probability of system resilience as 8.3E-01, with vulnerability equal to 6.4E-02, and maintainability of 4.7E-01. The given scenario includes an assumption that the system is capable of absorbing shocks. This can be inferred by percentages, as follows: *absorptive capability* with 95% success; *system adaptability* with 97% success and *system restorative capability* with 92% success. It depicts perfect system resilience with negligible hydrocarbon release, achieving a successful performance of the operation.

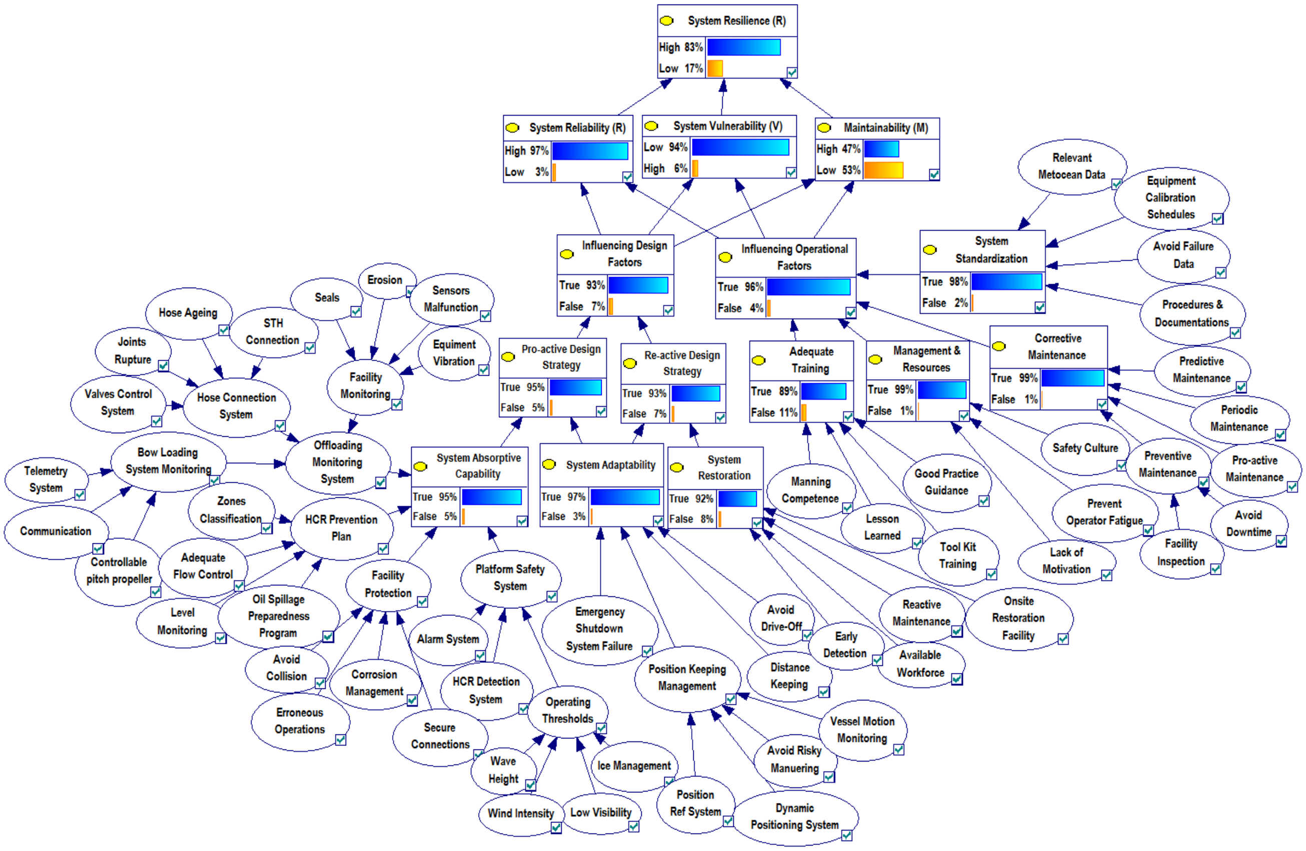

Figure 13: Resilience model for offloading between FPSO and shuttle tanker

It is inferred from the model above that if an *offloading monitoring system*, a *hydrocarbon release prevention plan*, *facility protection*, and *platform safety* are not effectively executed at the site, system absorptive capability deteriorates. For instance, the model clearly illustrates that when absorptive capability fails, the maintainability increases by default to 5.8E-01, which will keep the system resilience at 81%, as shown in Table I (scenario 1), because of the availability of the default maintainability feature to overcome the negative effects on the system.

2.6.2 Sensitivity Analysis

One of the best ways to analyze and validate the expert-built model is to perform a sensitivity analysis by selecting a target node and subsequently observing the results and impact of variables on that node. In the given analysis, resilience node, vulnerability and maintainability have been set as target nodes and the impact of other critical variables is analyzed, as they affect performance monitoring. These are presented in Table III of next page.

Table III: Scenario for forward propagation sensitivity analysis

Scenario created for forward propagation sensitivity analysis									
Evidence node	**States**	**Scenario 1**	**Scenario 2**	**Scenario 3**	**Scenario 4**	**Scenario 5**	**Scenario 6**	**Scenario 7**	**Scenario 8**
System absorptive capability	True		✓	✓			✓		✓
	False	✓			✓	✓		✓	
System adaptability	True	✓		✓		✓			✓
	False		✓		✓		✓	✓	
System restoration	True	✓	✓		✓				✓
	False			✓		✓	✓	✓	
Adequate training	True	✓	✓	✓	✓	✓	✓	✓	
	False								✓
Management and resources	True	✓	✓	✓	✓	✓	✓	✓	
	False								✓
Corrective maintenance	True	✓	✓	✓	✓	✓	✓	✓	
	False								✓
System standardization	True	✓	✓	✓	✓	✓	✓	✓	
	False								✓
System vulnerability (%)	High	28	28.5	19.9	49.0	41.4	41.1	61.6	30.8
	Low	72	71.5	80.1	51.0	58.6	58.9	38.4	69.2
Maintainability (%)	High	57.9	58.2	54.0	68.3	64.5	64.4	74.5	46.7
	Low	42.1	41.8	46.0	31.7	35.5	35.6	25.5	53.3
System resilience (%)	High	81.2	81.4	81.9	80.1	80.5	80.6	79.3	72.0
	Low	18.8	18.6	18.1	19.9	19.5	19.4	20.7	28.0

Eight different forward propagation scenarios are performed, as reported in Table III. The effect of treated variables can be observed clearly in terms of their respective impact on target nodes. For example, in Scenario 1, system vulnerability, maintainability and resilience are chosen as target nodes, as well as the evidence nodes mentioned, which are considered important for the performance of resilience. The system's absorptive capability is instantiated to a failed state, with other variables (system adaptability, system restoration, and others) instantiated to the normal or true state. It is observed that vulnerability in the given scenario is 2.8E-01, and that the maintainability of 5.8E-01 cancels the effect of disruption and maintains the resilience value at a new steady state of 8.1E-01.

Similarly, in Scenario 5 of Table III, *system absorptive* capability and *restorative* capability are set to "failed" states. This leads to a negative impact on system resilience, whereby maintainability increases accordingly to achieve a higher resilience of 8.5E-01.

The graphical representation of the sensitivity analysis for the different scenarios is shown in Fig. 14. This illustrates the system failure in terms of vulnerability and the required maintainability to achieve an acceptable resilience called "*new steady state*". The system becomes vulnerable if some of the design factors fail, but at the same time, it is observed that the model attempts to compensate for the effect of these disruptive events by increasing the default maintainability of the system through operational factors. Thus, the disruption results in resilience rising to 81%, which clearly demonstrates that this is because of the respective increase in maintainability that inhibits the decline in resilience.

In other words, the inverse relationship between design factors and maintainability nodes in the base model (as shown in Fig. 12) is set to maintain resilience so that it will slow down the effect of increasing vulnerability, which is the desired property of any resilient system. The present model may show a decline in resilience at any point. For instance, if the whole absorptive capability and system restorative nodes are considered to have failed, the resilience is decreased by 1.5% which is still in an acceptable range, and maintainability is increased from 4.7E-01 to 6.4E-01 in the baseline case shown in Fig. 13, where the vulnerability is 6.4E-02.

The quantification results of the model show that when vulnerability occurs in the system, it adapts maintainability and resists lowering the system's functionality. Thus, it keeps the resilience high, which is not necessarily at the same but can be maintained within desired limits. At this position, the system successfully continues to its functions. If most of the design factors stop working, the system will put a high load on maintainability and attempt to increase its value until a threshold is achieved that is required maintaining minimum changes in the overall resilience of the system. This in no way implies that the failure of all components of the system would maintain resilience. Furthermore, the failure of the operational factors is observed to greatly reduce system maintainability. The operational design factors form the backbone of maintainability in the proposed model. If any of them are disturbed, it will, in turn, affect maintainability as well as make the system vulnerable.

Figure 14 shows the comparative result of *vulnerability, maintainability,* and *resilience*. From Scenario 1 to Scenario 7, the resilience is analyzed in terms of influencing design factors by applying sensitivity analysis. The value of resilience is maintained above 7.8E-01 with the presence of extreme vulnerability due to the failure of several factors. In Scenario 8, it can be clearly observed that the value of resilience declines, even in the presence of comparatively low vulnerability. This is due to the fact that *operational factors* either fail or are set to be ineffective, resulting in a direct negative effect on maintainability. This eventually makes the vulnerability cross dangerous limits.

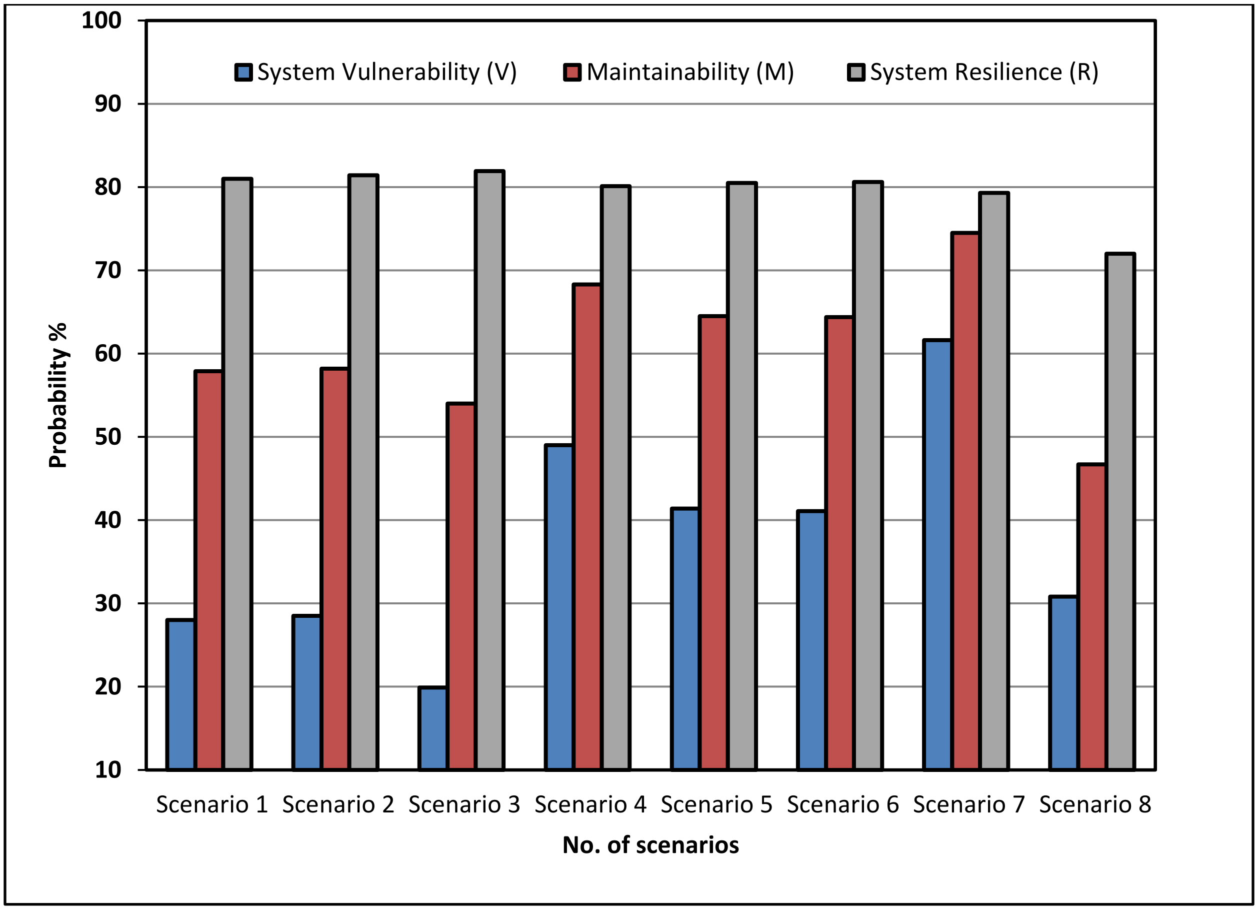

Figure 14: Sensitivity analysis of the overall resilience model

2.6.3 Accident Scenarios

The following accidents are considered part of the case study to verify the rationale of the proposed model. These accidents are described using different verified resources.

Incident A*: "Statfjord incident"*

On December 12th, 2007, an oil spill occurred due to a rupture in a hose near the *Statfjord* oil field in the North Sea in Norway. Around 3840m^3 of oil was spilled into the sea. This amounts to almost 24,154 barrels of oil, which is considered to be the second largest spill in Norwegian oil history (Tisdall, 2007). The main causes, as reported in Chen, *et al*. (2010) and Chen (2003), were the *controllable pitch propeller*, *position reference system*, some identified *sensors malfunction*, errors in the *DP system software*, and *human operators' error*, as identified in Fig. 13.

Incident B: *"Uisge Gorm FPSO incident"*

A similar incident occurred on April 4th, 1999, in the *Uisge Gorm* FPSO of Fife, Fergus, Flora and Angus fields of the North Sea, UK, due to the lack of a vent line opening after the maintenance operation (Torgeir, Amdahl, Wang, & Spencer, 2002; Knapp, 1999). The pressure that developed severely damaged the vessel's hull and its vicinity. The main causes of this incident were: valve control system failure, erroneous operation, inadequate flow control, reactive maintenance failures, manning incompetence, and bad practice guidance, also identified in Fig. 13.

The model investigated the results from Incident A, where the system vulnerability (loss of hydrocarbon) occurred due to five evidence factors, as mentioned above. It can be noted that in the results, vulnerability rose from 6.5E-02 to 1.2E-01. The model also calculated the desired maintainability which was required to keep the system in a *steady state* and the achieved resilience was 82%. The model also investigated the results for scenario B, where the system vulnerability (loss of hydrocarbon) occurred due to six different evidence factors, as mentioned above, in which vulnerability was raised from 6.5E-02 to 1.5E-01, and counterpart maintainability increased to 5.0E-01, which was required to keep the system resilient up to 8.1E-01, in terms of operational factors such as adequate training, deploying maintenance, following system standardization and resources management.

2.7 Concluding Remarks

This study has investigated system resilience during an offloading operation, considering hydrocarbon release at offshore facilities. Calculating overall system resilience is imperative as it is necessary to withstand inevitable difficulties, and is thus essential for the planning and execution of complex infrastructure systems. Offshore infrastructure such as drilling equipment, power plants and complex facility systems are constantly dealing with natural and human-made disasters; hence, they need to be scrupulously designed to withstand disruptions and recover rapidly.

The proactive design strategy depends on the system's absorptive and adaptive capabilities, while the reactive design strategy relies on the system's adaptability and restoration features. These unforeseen but understandable phenomena may be modeled in terms of a respective feed forward network that undermines system resilience. To counter the negative effects of vulnerability, there needs to be a comprehensive parallel model for system maintenance and its underlying factors. Fortunately, this study reveals a similar feed forward network that approaches positive convergence towards system resilience. The research study demonstrates the interconnection between three major factors: reliability, vulnerability and maintainability, and the underlying sub-factors as they affect the resilience of a system. The extent of vulnerability in the present model may adequately be controlled (or lowered) by a corresponding increase in maintainability. The model allows this to happen by anticipating the effect of changes in the connected factors of maintainability. In turn, this enables preemptive testing and analysis of hazards that may arise with no prior knowledge. The model thus generally permits extended functionality if augmented with additional factors that may prove to be of value using future sensitivity analysis. The selected factors have been tested for effectiveness by incorporating rigorous sensitivity analysis. This not only ensures the strength of the model in understanding the combined effect of all underlying multi-level factors on system resilience but also in reducing the respective probabilistic weights. The system enables engineers to predict with better accuracy the effects of any hidden disastrous events and thus manage the influence of various risk factors that inhibit the ideal execution of events within the framework. The model thus emphasizes the deep concern regarding resilience in the construction of infrastructure.

The concluding sensitivity analysis assisted in guiding the pre-order and post-order strategies required as building blocks of resilience within the system. The generalization of this model explicitly allows researchers to further extend its use by incorporating other sets of features in correct network arrangement, to study the net effect of resulting factors on either system resilience or some other outcome of high value. The quantification strategy for resilience further increases its value by breaking it down into numbers, thus enabling the respective user to deal with it more efficiently. The results of this study are quite convincing and inspire real-time deployment of the proposed model. The effect of the use of continuous variables in modeling the resilience of a complex system will be investigated in future studies.

Acknowledgments

The authors greatly acknowledge the financial support provided by the collaboration between the Norwegian University of Science and Technology (NTNU), of Trondheim, Norway, and Memorial University of Newfoundland, Canada.

References

Abdel-Moati, H., Morris, J., Ruan, Y., & Zeng, Y. (2015). Advanced techniques for autonomous detection of gas releases. Al-Khobar, Saudi Arabia: Society of Petroleum Engineers.

Abimbola, M., Khan, F., Khakzad, N., & Butt, S. (2015). Safety and risk analysis of managed pressure drilling operation using Bayesian network. *Safety Science, 76*, 133-144.

Agarwal, J. (2015). Improving resilience through vulnerability assessment and management. *Civil Engineering and Environmental Systems, 32*, 5-17.

Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015). Operational models of infrastructure resilience. *Risk Analysis, 35*(4), 562.

Arora, K. (2004). *Comprehensive production and operations management.* New-Delhi: Laxmi Publication.

Arsenault, D., & Sood, A. (2007). Reslience: A systems design imperative. *CIPP Working Paper 02-07.* Arlington, VA: George Mason University.

Bakkensen, L. A., Fox-Lent, C., Read, L. K., & Linkov, I. (2016). Validating resilience and vulnerability indices in the context of natural disasters. *Risk Analysis, 37*(5), 982-1004.

Baksh, A.-A., Abbassi, R., Garaniya, V., & Khan, F. (2016). A network based approach to envisage potential accidents in offshore process facilities. *Process Safety Progress, 36*(2), 178-191.

Barringer, H. P. (1997). Availability, Reliability, Maintainability, and Capability. Humble, TX: Barringer & Associates, Inc.

Bazerman, M. (1998). *Judgment in managerial decision making* (4th ed.). New York: Wiley.

Bobbio, A., Portinale, L., Minichino, M., & Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering and System Safety, 71*, 249-260.

Chen, H. (2003). *Probabilisitic evaluation of FPSO-tanker collision in tandem offloading operation.* Trondheim – Norway: Department of Marine Technology, Faculty of Engineering Science and Technology, Norwegian University of Science and Technology.

Chen, H., & Moan, T. (2002). Collision risk analysis of FPSO-Tanker offloading operation. Oslo: Norway.

Chen, H., & Moan, T. (2004). Probabilistic modeling and evaluation of collision between shuttle tanker and FPSO in tandem offloading. *Reliability Engineering and System Safety*, 169-186.

Chen, H., Lerstad, A., & Moan, T. (2010). Probabilistic evaluation of collision between DP shuttle tanker and geostationary FPSO in direct offloading. *Proceedings of the ASME 2010 29th Internation Conference on Ocean, Offshore and Arctic Engineering.* Shanghai: ASME digital collections.

C-NLOPB. (2016, November). *http://www.cnlopb.ca/information/statistics.php#environment.* St. John's, NL:

Canada-Newfoundland and Larador Offshore Petroleum Board. Retrieved from http://www.cnlopb.ca.

Cutter, S. L., Ahearn, J. A., Amadei, B., Crawford, P., Eide, E. A., Galloway, G. E., . . . Zoback, M. L. (2013). Disaster resilience: A national imperative. *Environment, 55*(2), 25-29.

Ebeling, C. E. (1997). *An introduction to reliability and maintainability engineering* (1st ed.). New York: McGraw-ill.

El-Gheriani, M., Khan, F., & Zuo, M. J. (2017). Rare event analysis considering data and model uncertainty. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*.

Fedele, L. (2011). *Methodologies and techniques for advanced maintenance.* London: Springer-Verlag.

Fesseler, R., Baker Jr., M., & Inc., B. C. (2008). *Pipeline corrosion.* U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration Office of Pipeline Safety.

Fitch, E. C. (1992). *Proactive maintenance for mechanical systems.* FES Inc: Stillwater, Oklahoma.

Fleming, M. T., Gordon, R. P., Flin, R., Mearns, K., & Fleming, M. (1996). Assessing the human factors causes of accidents in the offshore oil industry,. *SPE Health,* *Safety and Environment in Oil and Gas Exploration and Production Conference.* Richardson, TX: Society of Petroleum Engineers (SPE), Inc.

Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J. M., Kott, A., . . . Linkov, I. (2016). Operational resilience: concepts, design and analysis. *Scientific Reports, 6*, 1-12.

Gordon, R. (1998). The contribution of human factors to accidents in the offshore oil industry. *Reliability Engineering & System Safety, 61*(1), 95-108.

Guikema , S., McLay, L., & Lambert, J. H. (2015). Infrastructure systems, risk analysis, and resilience—research gaps and opportunities. *Risk Analysis, 35*(4), 560-561.

H Jönsson, H., Johansson, J., & Johansson, H. (2007). Identifying critical components in technical infrastructure networks. *J. Risk and Reliability, 222*, 235-243.

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis, 29*(4), 498-501.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4*, 1-23.

Holling, C. S. (1996). Engineering resilience versus ecological resilience. In P. C. Schulze (Ed.), *Engineering within ecological constraints* (pp. 31-44). Washington, D.C., USA: National Academy Press, .

Holling, C. S. (1996). Engineering within ecological constraints. In P. C. Schulze (Ed.), *Engineering resilience versus ecological resilience* (pp. 31-44). Washington, D.C., USA.: National Academy Press.

Hosseini, S., & Barker, K. (2016). Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports. *Computer & Industrial Engineering, 93*, 252-266.

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety, 145*, 47-61.

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety, 145*, 47-61.

Hosseini, S., Yodo, N., & Wang, P. (2014). Resilience modeling and quantification for design of complex engineered systems using Bayesian networks. Buffalo, New York: International Design Engineering Technical Conferences & Computers and Information in Engineering Conference.

Jensen, F. V., & Nielsen, T. D. (2007). *Bayesian networks and decision graphs* (2nd ed.). New York: Springer-Verlag.

Johansson, J., Hassel, H., & Zio, E. (2013). Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. *Reliability Engineering & System Safety, 120*, 27-38.

John, A., Yang, Z., Riahi, R., & Wang, J. (2016, October). A risk assessment approach to improve the resilience of a seaport system using Bayesian networks. *Ocean Engineering*, 136-147.

Johnsen, S., Herrera, I., Vatn, J., & Rosness, R. (2005). Cross border railway operations: building safety at cultural interfaces. *SINTEF Industrial Management, Safety and Reliability, Norway*.

Keogh, M., & Cody, C. (2013). *Resilience in regulated utilities.* Washington, DC, USA: The National Association of Regulatory Utility Commissioners (NAURC).

Khakzad, N., & Reniers, G. (2015). Using graph theory to analyze the vulnerability of process plants in the context of cascadinng effects. *Reliability Engineering and System Safety, 143*, 63-73.

Khakzad, N., Khan, F., & Amyotte, P. (2011). Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering and System Safety, 95*, 925-932.

Khakzad, N., Khan, F., & Amyotte, P. (2013). Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection, 91*, 46-53.

Khakzad, N., Khan, F., & Amyyotte, P. (2013). Quantitative risk analysis of offshore drilling operations: A Bayesian approach. *Safety Science*, 108-117.

Knapp, D. (1999). *International energy agency - Monthly oil market report.* London, UK: Executive Director and Secretariat of the International Energy Agency.

Kumar, S. A., & Suresh, N. (2008). *Production and operations management (with skill development, caselets and cases).* New Delhi: New Age International (P) Limited, Publishers.

McGillivary, A., & Hare, J. (2008). *Offshore hydrocarbon releases 2001-2008.* Buxton: Health and Safety Laboratory, Health and Safety Executive.

Mobley, R. K. (2002). *An introduction to predictive maintenance* (2 ed.). Woburn, MA: Elsevier Science.

Norwegian Petroleum Industry. (2015). *Norwegian oil and gas recommended guidelines for offshore loading shuttle tankers.* Stavanger, Norway: Norwegian Oil and Gas Association.

Obama B. Presidential Policy Directive/PPD-21. (2013). *Presidential policy directive -- Critical infrastructure security and resilience*. Retrieved 2017, from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Øien, K. (2001). Risk indicators as a tool for risk control. *Reliability Engineering & System Safety, 74*(2), 129-145.

OREDA. (2002). *Offshore reliability data handbook* (4th ed.). Trondheim, Norway: SINTEF Industrial Management.

Park, J., Seager, T. P., Rao, P. S., Convertino, M., & Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis, 33*(3), 356-367.

Paz, N., & Leigh, W. (1994). Maintenance scheduling: Issues, result and research needs. *International Journal of Operations & Production Management*(14), 47-69.

Przytula, K. W., & Thompson, D. (2000). Construction of Bayesian networks for diagnostics . *Proceedings of IEEE Aerospace Conference, 5*, 193-200.

Rabelo, E. C. (1998). *Ingenieria del mantenimiento.* Argentine: Nueva Libreria.

Rodriguez, E., Martha de Souza, F., & Martins, R. (2009). Risk-based analysis of offloading operations with FPSO production units. *20th International Congress of Mechanical Engineering.* Gramado, RS, Brazil: Preceedings of COBEM 2009.

Sheffi, Y. (2005). *The resilient enterprise: Overcoming vulnerability for competitive advantage* (1st ed.). Cambridge: MIT Press Books.

Sklet, S. (2006). Hydrocarbon releases on oil and gas production platforms: Release scenarios and safety barriers. *Jounal of Loss Prevention in the Process Industries, 19*, 481-493.

Snorre, S. (2006). Hydrocarbon releases on oil and gas production platforms: Release scenarios and safety barriers. *Journal of Loss Prevention in the Process Industries*, *19*, 481-493.

Song, G., Khan, F., Wang, H., Leighton, S., & Yuan, Z. (2016). Dynamic occupational risk model for offshore operations in harsh environments. *Reliability Engineering and System Safety, 150*, 58-64.

Step Change in Safety. (2015). *Hydrocarbon release reduction TOOLKIT*. Aberdeen: www.stepchangeinsafety.net.

Sun, L., Kang, J., Gao, S., & Jin, P. (2016). Study on maintenance strategy for FPSO offloading system based on reliability analysis. *Proceedings of the Twenty-sixth (2016) International Ocean and Polar Engineering Conference Rhodes.* Greece: International Society of Offshore and Polar Engineers (ISOPE).

Swanson, L. (2001). Linking maintenance strategies to performance. *International Journal of Production Economics, 70*, 237-244.

Thiago, M., David, G., Gajewski, H., Colleen, H., Maria, L., Andre, S., . . . Woods, D. (2006). Application of Resilience Engineering on Safety in Offshore Helicopter

Transportation. In M. D. Devore (Ed.), *Proceedings of the 2006 Systems and Information Engineering Design Symposium*, (pp. 228-233).

Thomsen, J. J. (2003). *Vibratons and stability: Advanced theory, analysis, and tools* (2nd ed.). New York: Springer.

Thorisson, H., Lambert, J. H., Cardenas, J. J., & Linkov, I. (2017). Resilience analytics with application to power grid of a developing region. *Risk Analysis, 37*(7), 1268-86.

Tisdall, J. (2007, December 12). Large north sea oil spill. *Aftenposten - English*.

Torgeir, M., Amdahl, J., Wang, X., & Spencer, J. (2002). Risk assessment of FPSO's, with emphasis on collision. *Society of Naval Architects and Marine Engineers (SNAME)* (pp. 199-229). Boston: Society of Naval Architects and Marine Engineers (SNAME).

Turner, M., Skinner, J., Roberts, J., Harvey, R., & Ross Environmental Research Ltd., S. (2010). Review of Offshore Oil-spill prevention and remediation requirements and practices in Newfoundland and Labrador. St. John's: Government of Newfoundland and Labrador.

Uzcategui, M., Mathison, J., & Soto, A. (2015). Design of resilient production facilities through innovation and risk management. Bogota, Colombia: Society of Petroleum Engineers.

Vinnem, J. E. (2003). *Operational safety of FPSOs shuttle tanker collision risk summary report.* Sudbury: Health and Safety Executive.

Vinnem, J. E., & Røed, W. (2015). Root causes of hydrocarbon leaks on offshore petroleum installations. *Journal of Loss Prevention in the Process Industries, 36*, 54-62.

Vugrin, E., Warren, D., & Ehlen, M. (2011). A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. *Process Safety Progress, 30*(3), 280-290.

Vugrin, E., Warren, D., & Ehlen, M. (2011). A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. *Process Safety Progress, 30*(3), 280-290.

Weber, P., & Jouffe, L. (2006). Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN)*. *Reliabilty Engineering & System Safety*, 149-162.

Wiegerinck, W., Kappen, B., & Burgers, W. (2010). Bayesian networks for expert systems: Theory and practical applications. In R. Babuska, & F. C. Groen (Eds.), *Interactive Collaborative Systems* (pp. 547-578). Delft, The Netherlands: Springer.

Williams, J., Brown, D., Shaw, M., & Howard, A. (1999). Tanker loading export systems for harsh environments: A risk-management challenge. *Offshore Technology Conference* . Houston, Texas.

Yeo, C., Bhandari, J., Abbassi, R., Garaniya, V., Shuhong, C., & Shomali, B. (2016). Dynamic risk analysis of offloading process in floating liquefied natural gas (FLNG) platform using Bayesian Network. *Journal of Loss Prevention in the Process Industries, 41*, 259-269.

Youn, B. D., Hu, C., & Wang, P. (2011). Resilience-Driven system design of complex engineered systems. *Journal of Mechanical Design*, *133*(10), 10101(15).

Chapter 3: Enhancing Integrated Offshore Power Operations and Resilience Assessment by using Object-Oriented Bayesian Network

Adnan Sarwar, [a] Faisal Khan, [a,*] Lesley James, [b] Majeed Abimbola [a]

[a)] Centre for Risk, Integrity, and Safety Engineering (C-RISE),

Faculty of Engineering & Applied Science,

Memorial University, St. John's, NL A1B 3X5, Canada.

[b)] Faculty of Engineering & Applied Science,

Memorial University, St. John's, NL A1B 3X5, Canada.

Preface

This version of the presented paper has been submitted to the journal, *Ocean Engineering* in September 2017. The lead author, Adnan Sarwar, performed the necessary literature review, development of model in Object-oriented Bayesian network, conducted the research analysis and discussion, and developed the manuscript of the paper. The co-author Dr. Majeed Abimbola guided the principal author, while Drs. Khan and James were the principal supervisors of the given research and provided expert guidance, knowledge based support and overall editing of the manuscript.

Abstract

Harsh weather and deep waters create challenging environments for offshore drilling and production facilities, resulting in increased chances of failure. These necessitate improving the resilience of engineering systems. Having a robust power system is an essential element of an offshore facility. A power management system interacts with other engineering systems to maximize performance and limit potential failures. Ensuring a safe and continuous operation requires technological advancement, increased reliability of integrated operations, and improvement of power system resiliency. This paper identifies the main requirements for an improved resilience of an offshore power management scheme. Different potential failure scenarios are identified and analyzed to quantify the resilience of the system. The object-oriented Bayesian network format is adopted to model resilience as a function of anticipated reactions, system adaptability, absorptive capability and restoration. Sensitivity analysis is conducted to study the impact and interdependencies among different variables and strategies used to quantify resilience of an offshore power system, and also to improve the system performance during certain failures by adapting control measures.

Keywords: Resilience; Object-oriented Bayesian network (OOBN); Integrated operations; Power system.

3.1 Introduction

The failure of an electrical power system has been identified as the most prominent common cause of failure for many engineering systems. For offshore facilities, such as: FPSOs and drilling ships, the prevailing high-power demands necessitate the provision of an integrated power supply system that is largely dependent on parallel and synchronized generators (Weingarth, et al., 2009). To ensure successful operations, it is of utmost importance to improve the overall efficiency and stability of the electrical power system. Otherwise, the occurrence of any common mode fault could result in a total blackout. The development of a control and power management system (PMS) is critical to improving the system's resilience to power failures, governance of major systematic faults, and minimal stress in all operational conditions (Voltz, et al., 2008).

In harsh offshore environments, dynamic positioning of drilling rigs is the preferred technology. In such tumultuous settings, undesirable electrical system outages or blackouts could lead to economic losses, increased risk of environmentally devastating incidents and the attendant company's reputational loss. Consequently, an improved resilience of the power supply system is desired to forestall the occurrence of blackouts at offshore facilities, particularly due to severe weather conditions.

In this study, a model of an electrical power system resilience is proposed using the object-oriented Bayesian network (OOBN). The quantification of resilience is performed by means of integration of several operations such as the integrated control system, and its maintainability. The major factors that contribute to resilience are divided into two main categories: vulnerability factors and recovery factors. Vulnerability factors are those factors that may bring vulnerability to the power system, whereas recovery factors are those that mitigate the effects of vulnerability.

The study uses known risk factors and employs important safety measures to estimate the probability of having a resilient system. Particularly, fault-tolerance capability, quick response, recoverability and avoiding vulnerability are emphasized. A sensitivity analysis is conducted for the developed model to study the importance of the various process parameters and altering field observations in real time. The OOBN based model enables both predictive and diagnostic analysis, with the help of intermediate nodes in the respective Bayesian network (BN) model, and estimates the posterior probabilities as new evidence is obtained.

Section 4.2 presents the literature review of resilience modeling and its concept, Bayesian and OOBN and Noisy-OR gate formats. Section 4.3 discusses the proposed methodology, the development of resilience modeling and its contributing factors for an offshore electrical power system. The proposed OOBN model is also presented along with a description of the basic events failure probabilities, which are used to assign prior probabilities to the OOBN model discussed in Section 4.3. Section 4.4 presents the results and discussion and employs sensitivity analysis to identify the influence of system parameters. Applications of the proposed model to two different incident scenarios related to the offshore oil and gas industry are also presented in Section 4.4. Finally, the concluding remarks are presented in Section 4.5.

3.2 Literature Review

This section reviews resilience modeling concepts, the use of Object-oriented Bayesian networks and the Noisy-OR gate, which will be applied to assess resilience in this study.

3.2.1 Resilience Modeling and its Concept

Resilience is the ability to minimize the magnitude and/or duration of disruptive events. The measure of the effectiveness of an infrastructures resilience depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially catastrophic event (NIAC, 2010). From the perspective of critical infrastructure, resilience refers to coordinate planning, responsive behavior, the implementation of flexible and timely recovery measures, as well as the development of a professional environment that requires minimal service during severe disruptions, emergencies and disasters to quickly return operations back to their original state. Arsenault and Sood (2007) defined the concept of a resilient organization as one capable of deflecting deliberate attacks and environmental disruptions (or their effects), absorbing unavoidable damages and resuming operations to pre-event levels, all with utmost speed. According to Haimes (2009), infrastructural resilience is the ability of the system to withstand major disruptions within acceptable degradation parameters and recover them with maintainability features within an acceptable time, composite costs, and risks. Moreover, Keogh and Cody (2013) defined resilience as the robustness and recovering characteristics of utility infrastructure and operations that avoid or minimize the interruptions of service during an extraordinary and hazardous event.

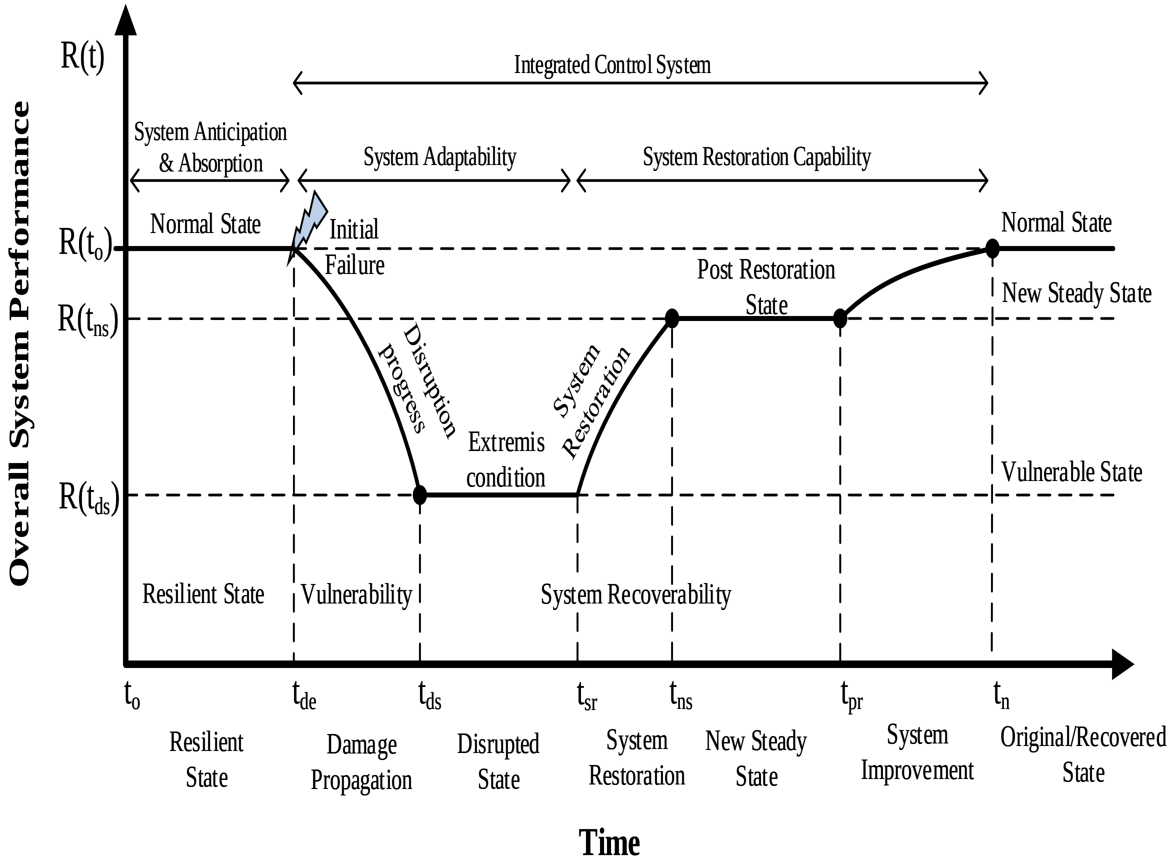

Figure 15: Resilience concept graph with respect to events. Adapted and modified after (Panteli & Mancarella, 2015)

Figure 15 shows how resilience, R(t), as a concept, evolves as a function of time given that a disturbance event occurs. In the event of a disruption, say harsh weather, at the time (t_{de}), the power system should be able to adapt to the emergent conditions. R(t_0) represents the assessment of resilience at time t_0, which is the initial state. Resilience demands that the system hold a high value of R(t) at $t = t_0$ for better adaptability. With an initial failure event, the resilience decreases significantly to R(t_{ds}). Now, the impact of a failure event can be estimated by the difference, R(t_{ds}) – R(t_0), that helps to determine the appropriate corrective measures before applying them at t_{sr}. The initial restoration to state R(t_{ns}) is an intermediate arrangement because the system may take longer to be fully restored, i.e., ($t_n - t_{ns}$) > ($t_{ns} - t_{sr}$), to the final steady state R(t_n). The way (for example, how fast, and how many intermediate post-restoration states there might be) a system progresses from state R(t_{ns}) to R(t_n) depends on various factors, such as the strength of the system to withstand a disruptive event, the severity of the disruption, the adaptability of the system and the response processes, which are divided into stages, such as ($t_0 \leq t \leq t_{de}$), that show the resilience during normal operations. The prevalent concept of a system resilience reported in (Panteli & Mancarella, 2015) is extended here by introducing the concept of anticipation parallel to system absorption before any disruptive event. As explained in Section 4.3.3.2, system anticipation involves discovering potential risks and preparing preventive measures. The condition ($t_{de} < t \leq t_{ds}$) denotes the damage propagation interval, after an initial failure that mainly reflects the absorptive and adaptive capacity to minimize the initial damages and consequences such as cascading failures. The condition ($t_{sr} < t \leq t_n$) is the recovering stage where extremis information is collected for assessment and resources are distributed to restore a new steady state quickly and effectively.

3.2.2 Bayesian Network

The inference probabilistic method based on *Bayes' theorem* is widely used for safety and risk assessment of complex systems having uncertain information. It illustrates the problem in a directed acyclic graphical presentation, composed of connected nodes with initial and intermediate events, based on the functional decomposition of the system (Weber & Jouffe, 2006; Hosseini & Barker, 2016). Furthermore, arcs of corresponding nodes and the conditional probability table represent the causal relationship and sensitivity link amongst variables (Khakzad, et al., 2013; El-Gheriani, et al., 2017). The quantitative analysis has been performed based on the d-separation principle where base events are conditionally independent and intermediate events are dependent on their influenced parent nodes. The Bayesian network (BN) represents joint probability distribution of variables based on conditional dependencies as: $P(U) = (v_1, v_2, \dots, v_n)$.

$$\mathrm{P(U)} = \prod_{\mathrm{i}=1}^{n} \mathrm{P}\big(v_{\mathrm{i}} \big| \mathrm{Pa}(v_{\mathrm{i}})\big) \tag{14}$$

From the given Eq. (14), $Pa(v_i)$ represents the set of parent nodes v_i, which indicates summation of all variables except u_i (Nielsen & Jensen, 2007).

$$\mathrm{P(a)} = \sum_{\mathrm{U}\backslash v_i} \mathrm{P(U)} \tag{15}$$

The advantage of BN is to allow prior probability updates with new information, called evidence *E*. Updated or posterior probabilities can be calculated as Eq. (16):

$$\mathrm{P(a)} = \frac{\mathrm{P(U,E)}}{\mathrm{P(E)}} = \frac{\mathrm{P(U,E)}}{\sum_{\mathrm{U}} \mathrm{P(U,E)}} \tag{16}$$

3.2.3 Object-oriented Bayesian Network (OOBN)

The development of the resilience model used here is the object-oriented modeling approach, where several sub-networks (instance nodes) are created in a model representing another Bayesian network (Khakzad, et al., 2013), as shown in Fig. 16. The OOBN allows an effective communication between sub-networks, avoids repetition of the same node structure by enabling reusable networks, and achieves a lessened conditional probability table, which is the primary objective in dealing with the complex system. These sub-network causal factors with the explicit labeling of output are linked with the top level of the model, where the output of the instance node provides interfacing functionality to become the input of the top-level model (Weber & Jouffe, 2006). The sub-nets *input node* accepts the same probability of its immediate parent node; thus, each input node should have one parent node. In contrast, output nodes convey the probabilistic value to other input nodes or affect the probabilities of other usual nodes; as a result, the output can have more than one child node (Khakzad, et al., 2013). Fig. 16 illustrates an example, where the input nodes are represented by dashed lines, output nodes are denoted with bold lines, and instance nodes classes are also provided. As is evident in Fig. 16, from left to right, Bayesian networks systems are simplified by using OOBN methodology. This work is developed in Section 4.3, by converting the BN resilience model into OOBN.

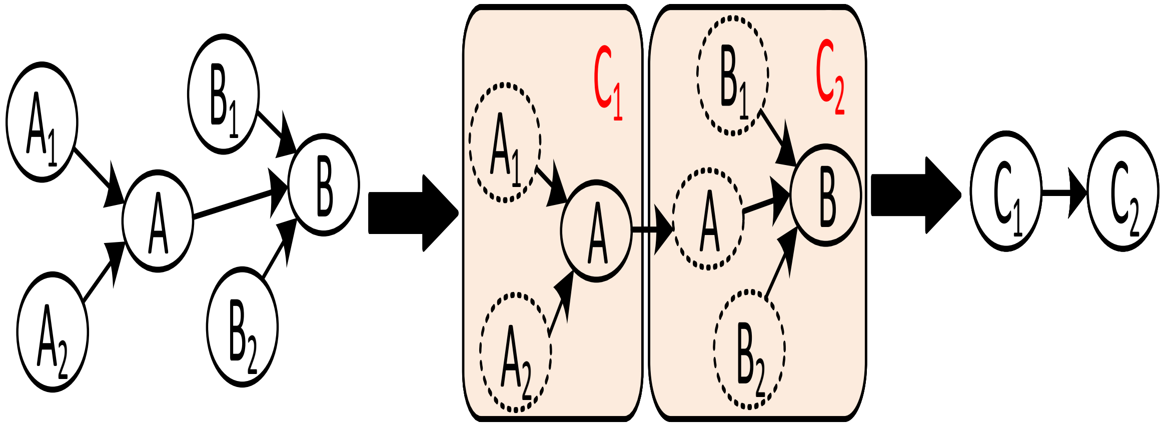

Figure 16: Simplified Bayesian network, and its conversion into an Object-Oriented Bayesian network.

3.2.4 Noisy-OR Gate

The Noisy-OR function is used in the model to interact between varying factors in terms of cause and effect of binary states: *true* or *false*. Noisy-OR describes diverse interactions between *n* number of causes, X_1, X_2…, X_n, and their common effect, represented by Y, which means Noisy-OR assumes that the causes of X_i influence Y independently. Suppose the probability distribution of *n* number of causal factors, P_1, P_2…, P_n. where P_i denotes the probability for Y being true if one causal factor, X_i, is true and the rest of the parameters are false, such as: X_j; $j \neq i$ (Hosseini & Barker, 2016; Onis´ko, Duzdzel, & Wasyluk, 2001). The mathematical expression will be Eq. (17):

$$P_i = P\,(Y= \text{“true”} \mid X_i = \text{“true”};\, X_j = \text{“false” for each } j \neq i) \qquad (17)$$

Eq. (18) is utilized for the probability of having Y from the given subset X_p of the X_i which is true:

$$P\ (Y= \text{“}true\text{”} \mid X_p) = \prod_{i:X_i \in X_p}(1 - P_i) \qquad (18)$$

The Noisy-OR function is also defined in Eq. (19) (Fenton & Neil, 2013), where the term *‘l’* denotes the *leaky* factor as shown in Eq. (20), which represents a situation where the probability of a system, here expressed as Y, could *fail* if all its causal factors are true, and vice versa. This extended feature of the binary Noisy-OR gate is appropriate to the system criteria where all causal factors of Y are not considered (Bobbio, et al., 2001; Adedigba, et al., 2016). Normally, such types of scenario are represented as:

$$\text{Noisy-OR}\ (X_1, P_1, X_2, P_2..., X_n, P_n, l) \qquad (19)$$

$$l = P\ (Y= \text{“true”} \mid X_1 = \text{“false”} \ldots, X_n = \text{“false”}, X_n = \text{“false”}) \qquad (20)$$

The estimated conditional probability of Y with the given subset X_p of X_i can be achieved through the *Noisy-OR* function by using following Eq. (21) (Hosseini & Barker, 2016; Adedigba, Khan, & Yang, 2016):

$$P\ (Y= \text{“}true\text{”} \mid X_p) = 1 - \{(1 - l) \prod_{i:X_i \in X_p}(1 - P_i)\} \qquad (21)$$

3.3 Methodology

3.3.1 Proposed Methodology Framework of Resilience Modeling

Fig. 17 explains the basic strategy that is adopted here to model system resilience. The first step is to identify the pertinent case study factors. The second step is to arrange intermediate nodes to model and integrate strategies that are used to reduce vulnerability and increase maintainability of the system. Then different strategies are classified in terms of operational and design level. The nodes obtained are used to construct various classes which are later combined to form the OOBN model (see Fig. 18 and Fig. 19). Then, prior probabilities (see Table IV) are assigned to the input nodes, and based on these posterior probability of resilience is obtained.

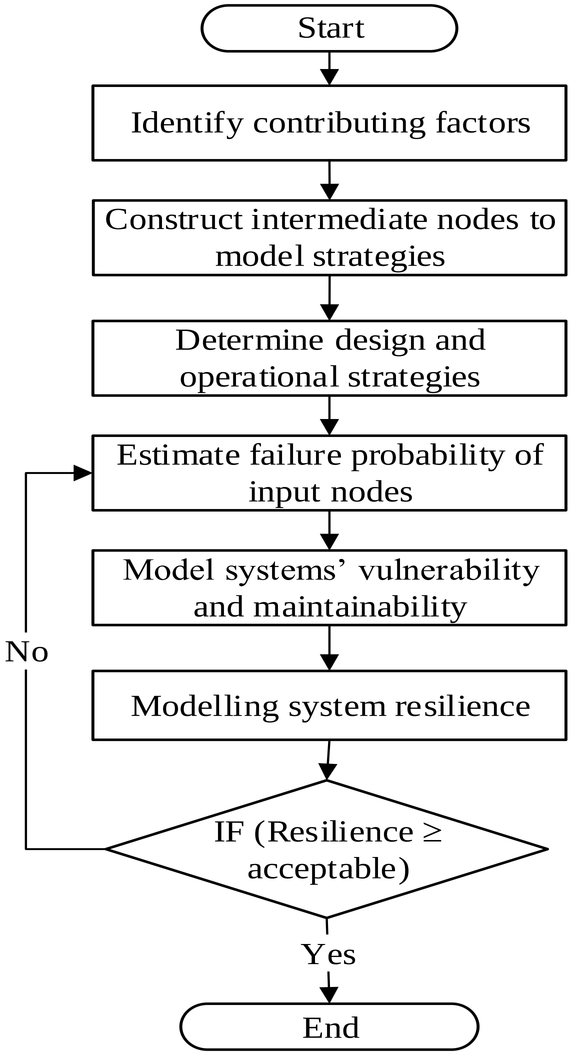
Start
Identify contributing factors
Construct intermediate nodes to model strategies
Determine design and operational strategies
Estimate failure probability of input nodes
Model systems' vulnerability and maintainability
Modelling system resilience
IF (Resilience ≥ acceptable)
No
Yes
End

Figure 17: Proposed methodology framework of resilience model

3.3.2 Modeling System Resilience, Vulnerability and Maintainability

In this work, maintainability is discussed as the key factor in restoring the system to a workable state. Based on this assumption, resilience is defined as a function of system vulnerability (V) and maintainability (M). Because vulnerability indicates negative effects of system disruptions, maintainability is required to lower or cancel out the effects of vulnerability. The factors are inversely proportional to each other. To simplify, the resilience is defined as an operator that minimizes the vulnerability and maximizes recovering capabilities by implementing maintainability features as shown in Eq. (22) (Sarwar, et al., 2017).

$$\text{System Resilience} \triangleq \text{Resilience}\ (1/V, M) \tag{22}$$

In Fig. 17, the interdependency among involved variables in the proposed base model describes quantification of the overall system *resilience* (R) as a leaf in output node, which is dependent on two parent variable nodes, i.e. *system vulnerability* (V) and system *maintainability* (M). In the model, the function of maintainability is dependent on the *integrated system design* and *operational system*, to reduce the system's vulnerability by introducing different operational strategies. The vulnerability of the system is modeled as the defective state due to system design failures and operational errors.

4.3.2.1 Modeling vulnerability

The system deteriorates due to errors or deficiencies in the integrated system design, or caused by integrated operational failures. As depicted in Fig. 17, the existence of system vulnerability is dependent on the integrated system design and the integrated operational system. If any individual component of the system fails, this inadequacy will affect either the integrated system design or operation and thus the system vulnerability; therefore, it is critical that the overall system be based on a high technical design and consider operational variability. One instance of vulnerability would be the blackout condition in a harsh offshore environment that causes a total loss of the vessel’s propulsion system as well as the power provided to auxiliary systems of FPSO and drilling rigs, which may lead to catastrophe when the facility is operating in rough seas and is in proximity to other vessels. Therefore, to achieve higher resilience, vulnerability is modeled using two factors: 1) *influencing design factors*, considering proactive and reactive approaches to risk management, and inherent safety design aspects able to withstand abnormal scenarios; and 2) *influencing operational* factors, enhancing system operation and overall performance. With these two general factors, several technical and design issues may be addressed.

4.3.2.2 Modeling maintainability

Maintainability is the capability of the system to anticipate disruptive events, withstand them and restore systems to operate effectively within well-defined conditions. Improving maintainability increases resilience, which reduces the vulnerability. Overall, system maintainability depends on the integrated system design and operational systems, as demonstrated in Fig. 18. Figures 18 and 19 presents object oriented network model of the overall system resilience. In Fig. 19, elements in circle/eclipse represents the root parameters, whereas object oriented Bayesian nodes are represented in rectangular shape. Resilience has two parent nodes: vulnerability and maintainability. These two parent nodes have multiple parents. For example, the overall system Maintenance is an operation activity represented as node that is dependent on set amount of time (duration of maintenance activity) regardless of the conditions present. The definition of maintenance can vary depending on how it is scheduled (Arora, 2004; Kumar & Suresh, 2008; Birolini, 2007); achieving high maintainability will raise the system's resilience. To raise the system's maintainability, its design and operational factors must be designed so that the system is protected before, during and after failure, which will help to achieve maximum resilience. This relationship is highlighted in object oriented Bayesian network model presented in Fig. 19.

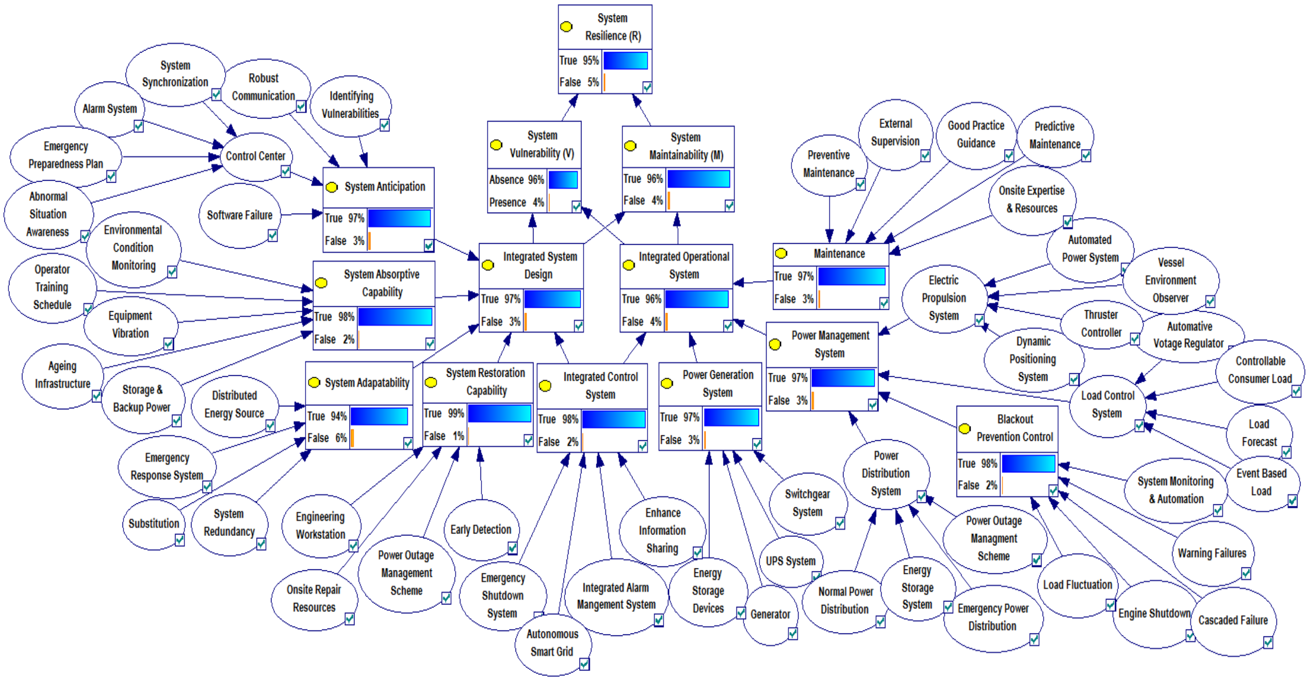

Figure 18: The graphical depiction of the proposed Bayesian network model for offshore power system

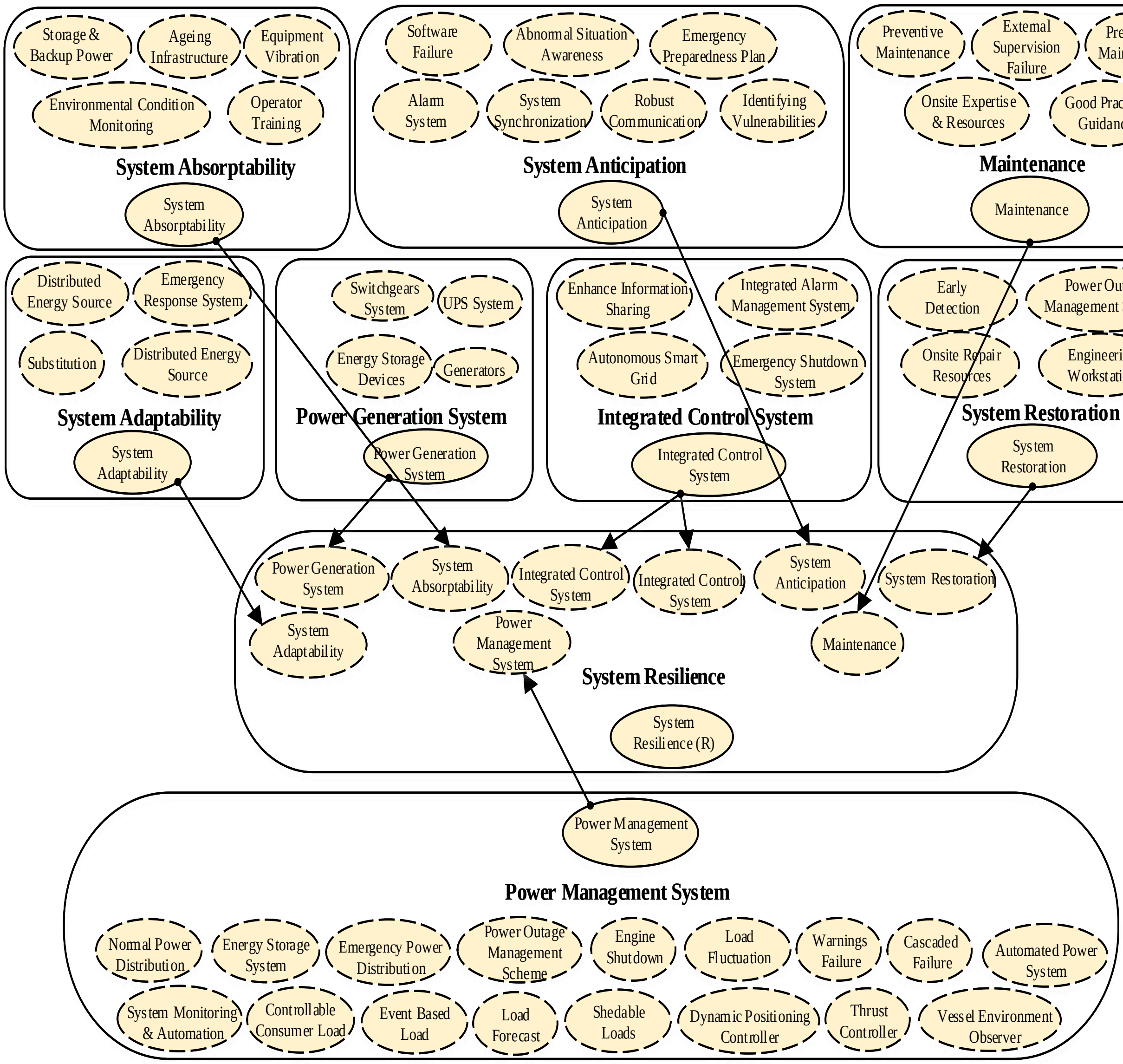

Figure 19: The graphical depiction of the proposed OOBN networks model for offshore power system

3.3.3 Resilience Modeling Factors for Offshore Electrical Power System

4.3.3.1 Integrated system design

During system design, the essential integrated factors that must be considered include a proactive strategy (the ability to withstand disruptive events or behavior of the system) and a reactive strategy (the capability of the system to restore the original or a new steady state after a disruption). It is necessary that the power system be designed based on reliability to achieve competence, sustain high performance and ensure security; these principles must correspond with known system failures with peak resilience to guarantee utmost quality and uninterrupted power supply to the infrastructures (Panteli & Mancarella, 2015). The perspectives to consider for the resilience system are: anticipation of an extraordinary event; absorption and endurance of disruptive events (minimizing consequences, achieving robustness); development of adaptive means of operations to accommodate changes within or around system infrastructure; quick restoration of the damages from a disruption by inducing smart control-based actions to provide an asset with control capability; and access to resources to deal efficiently with a crisis scenario. More concisely, the design strategies of modeling resilience system depend upon the ability to integrate different operations such as: *system anticipation, system absorptive capability, system adaptability, system restorative capability,* and an *integrated control system* (Francis & Bekera, 2014; Gholami, Aminifar, & Shahidehpour, 2016; NIAC, 2010).

4.3.3.2 System anticipation of vulnerable scenarios

System anticipation involves factors such as the ability of the system to forecast the set of risks, build in a reserve capacity that may be exploited when required and prepare a strategy to effectively withstand disruptions (Francis & Bekera, 2014). System anticipation can be performed to deal with potential disruptions by using the following functions such as: (a) *robust communication*: the system operator is obligated to use preventive control measures quickly, depending on the severity of the disturbance, to cope with a sudden electrical outage or extreme conditions (Panteli & Mancarella, 2015). The continuous (b) *identification of system vulnerabilities* (Gholami, et al., 2016): in large centralized power plants, substations, and electrical equipment (transformers, switchgears, and more), which are potential points of vulnerability in a power system, owing to the fact that minor uncontrollable incidents may cause interruption of megawatt flows, thus interfering with the provision of real-time control measurements and increasing the physical vulnerability of the electricity grid. Thus, the power system can improve the situational awareness of the overall system resilience. The (c) *control center* (Subbarao & Srinagesh, 2012): the central control room located onshore performs a paramount role for the system’s security and capability of anticipation, allowing continuous monitoring and minimizing the control errors of electricity grids and critical components of an offshore power system. To effectively maintain integrated alarm management systems, it is vital to provide an effective emergency preparedness plan and supervise ongoing activities at the site or off location through the (d) *abnormal situation awareness wall* (Subbarao & Srinagesh, 2012), and real-time (e) *system* synchronization:

for example, the means to synchronize a set of generators, and the critical protection applications (Weingarth, et al., 2009).

4.3.3.3 System absorptivity

Vugrin et al. define system absorptivity as the capability of the system to absorb and withstand the impact of disruptive events or system perturbations, as well as minimize their consequences. Absorptive capability refers to all activities that need to occur to contain the shocks of a disruption in advance (Vugrin, Warren, & Ehlen, 2011; Francis & Bekera, 2014). An essential feature of system absorptivity is its ability to control and absorb the shocks in terms of blackout prevention, power shortages, and system irregularities in advance. The identified effective features of absorptive capabilities for the study are: (a) *environmental condition monitoring* (Hansen & Wendt, 2015), which refers to maintaining continuous monitoring of operational environments, specifically harsh environments; (b) *operator training* (Subbarao & Srinagesh, 2012), which includes the skilled laborers, training operators, and managers responding to and controlling the disruption and maintaining the continuity of the system. The (c) e*quipment vibration*, which is the major cause of equipment failure, reduces the life cycle of critical equipment. Thus, the vibration suppression mechanism is required to achieve long-term reliability and availability of equipment. Furthermore, (d) *ageing infrastructure* deals with properly following the life cycle of the equipment to avoid discontinuity of operation, and (e) *storage and backup power* is the necessity of providing a backup or standby generator. These help in avoiding the overall downtime and power cut-off to the sensitive equipment.

4.3.3.4 System adaptability

System adaptability pertains to the accommodation of the changing conditions within or around the system, as well as the enhancement of the ability of the critical infrastructure and functions to withstand and rapidly recover from damage and disruptions (Berkeley & Wallace, 2010). The adaptability of a system also necessitates changes in the current practices, policies, and rules to overcome a variety of imminent disruptions (Francis & Bekera, 2014). The adaptive capacity is the capability of the system to adapt independently and attempt to overcome a disruption without any recovering activity; in other words, reorganizing the system and performing efficiently with some extra effort and resources to avoid vulnerabilities (Vugrin, Warren, & Ehlen, 2011). The contributing adaptive factors for the present study are: (a) *distributed energy source* (Farzin, et al., 2016; Panteli & Mancarella, 2015): smart distribution can be viewed as multiple energy sources with distributed optimization and control, sufficient generation, energy storage capacity, and autonomous management to achieve acceptable levels of supply during an emergency or unforeseen failure, thus functioning in a key role in resilience-boosting efforts. The (b) *emergency response system* (Craig & Islam, 2012), is the primary tool to prevent blackouts and provide a fast recovery to avoid emergency disconnects. The loss of dynamic positioning of vessel electrical and control systems equates to loss of station keeping, and the response system requires an emergency disconnect from the well-head, which is a serious event to avoid. The (c) *substitution of equipment* refers to a situation when the failure of equipment occurs during the disruption. The availability of reserve equipment gives the flexibility to overcome such a situation. For example, a standby generator and UPS system provide a substitute power source during power failures (Hosseini & Barker, 2016). The (d) *system redundancy* performs a key role in mitigating the consequences of disruption such as blackout prevention, by enabling the quick response of available recovering strategies in the system (Panteli & Mancarella, 2015).

4.3.3.5 System restoration

System restoration refers to the ability of the system to renew or recover from disruptions and to apply effective measures of the recovery plan for large scale outages such as a "*black start*", in which power generation must be brought back online without connection to external power sources (Vugrin, Warren, & Ehlen, 2011; NIAC, 2010). The restorative capacity of a system is often categorized as the rapidity of the normalization process. It is returning the system after a disruption to its normal functionality or improved operations, and system reliability should be assessed against a defined set of requirements that are derived for a desirable level of service and control (Francis & Bekera, 2014). In the context of power system resilience, the ability of the system to withstand low-probability and high-impact events in an effective manner ensures the least possible interruption in the supply of electricity to critical equipment and operations, and facilitates swift recovery or restoration to normal operations (Khodaei, 2014). The contributing factors are: (a) *early detection*: awareness of vulnerable situations and disruptions in earlier stages to allow the protection system and operators to take swift action to avoid system failures and enhance restoring capabilities. (b) The *engineering workstations* provide an operator interface, system configuration tools for control stations and a record of the historical data of the running applications (alarm management system, emergency shutdown system, and more), which aid in the maintenance of early failure detection through live status reports of the critical equipment (Subbarao & Srinagesh, 2012). The (c) *power outage management scheme* proposes the hierarchical outage management structure that can enhance the resilience of the electrical system by adapting a smart distribution system, which comprises multi-microgrids against disruptive events and complete blackout facility. The autonomous management and control of its microgrids through central controllers, operations, and management must be decentralized. Furthermore, it must be made possible to share all available power generation and storage resources among equipment, which will achieve better diversification of power outage management and enhance the resilience of the overall distribution system (Farzin, et al., 2016). The (d) *onsite repair resources* pertain to the possibility of resources in terms of accessible on-site spare equipment for critical components, the availability of repair teams, the ability to perform resource mobilization, and the prioritization of repairs based on the criticality of individual equipment (Hosseini & Barker, 2016; Mensah, 2015).

4.3.3.6 Integrated control system

The integrated control system emphasizes building maximum integration of system design and the operation of the current system. This helps to manage overall functionality of a power system, by optimizing steady state performance, and provides the possibility for future expansion and continuous improvement (Radan, 2008; Subbarao & Srinagesh, 2012). The system has the potential to monitor, control, and safeguard the system operation through the following features: (a*) autonomous smart grid* that utilizes a digital information network to help maintain efficient power generation, its transmission, and consumption (Montoya, 2008). The (b) *abnormal situation management* facilitates quick reactions, especially during operational emergencies or breakers' tripping that may further lead to a catastrophic situation (blackout). Through (c) *integrated alarm management* system, emergency shutdown of the system can be achieved. The (d) *enhanced information sharing* refers to high speed, dedicated and redundant information network sharing and managing the information to the control system for operators, maintenance staff and external users to monitor and prevent disturbances in the electrical system, allowing peak performance and efficiency (Subbarao & Srinagesh, 2012). System synchronization between equipment and standby generators is performed and checked by control systems before the generator circuit breakers are closed (Hossain, et al., 2013)**.**

4.3.4 Integrated Operational System

The integration of work, processes, and technology enable the system to make smarter decisions and achieve better execution by using real-time information, collaborative advanced technology and multiple expertise across multiple disciplines (Lima, et al., 2015). The exploration of new offshore oil and gas fields pushes workers and structures into deeper waters and harsher environments, so an integrated power system design for these offshore energy vessels and deep-water rigs is required. For a modern oil and gas vessel, there is an array of dependent factors, subsystems and interfaces. The integrated marine power operation mainly relies on four subsystems: (a) *power generation system*, (b) *power management system*, (c) *integrated control system,* and (d) *maintenance*.

4.3.4.1 Power generation system

The power generation system is the most vital system on-board. The generated power is supplied to electrically driven thrusters and provides energy to the facility, drilling activities and more. The continuity of power generation is most important, so the critical components which must be considered in the generation system are: *energy storage devices*, *generators*, *UPS systems*, and *MV switch gears*.

4.3.4.2 Power management system

As shown in Fig. 20, the focus of power management systems is to improve the electrical system robustness during disruption, increase the capability to deal with major failures, maximize the performance of the system, and maintain the critical components under minimal stress in operational conditions. The power management system plays a crucial part in automation, and power systems on marine vessels are especially important for the vessels with electric propulsion systems and station keeping thrusters. It also provides an integrated set of control, supervision, and management functions for engines, generators, switchgears, and overall electrical control systems. In the model, four major factors that largely depend on the power management system, such as: the *power distribution system*, the *blackout prevention strategy*, the *load limit control system*, and the *electric propulsion system* are considered.

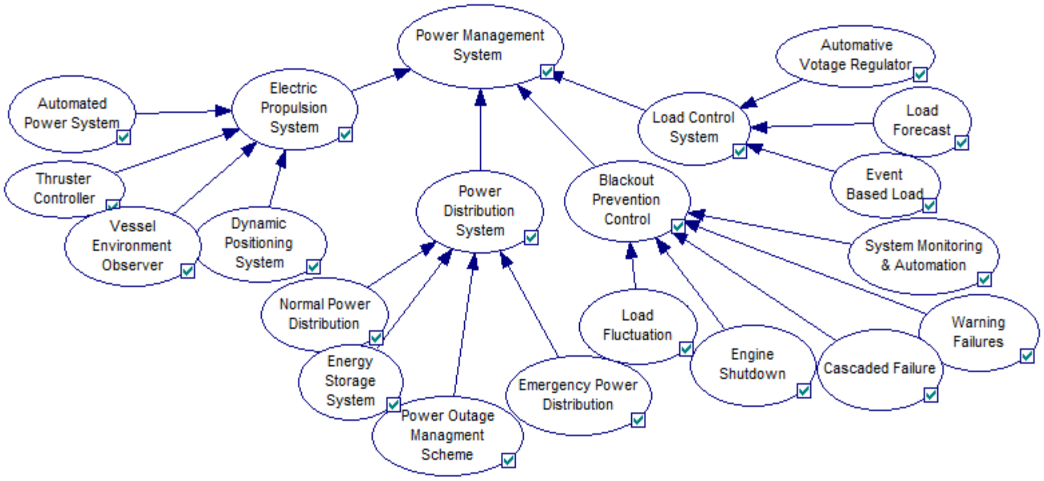
Power Management System
Automative Votage Regulator
Automated Power System
Electric Propulsion System
Load Control System
Load Forecast
Thruster Controller
Event Based Load
Blackout Prevention Control
Power Distribution System
Vessel Environment Observer
Dynamic Positioning System
System Monitoring & Automation
Normal Power Distribution
Load Fluctuation
Warning Failures
Energy Storage System
Engine Shutdown
Cascaded Failure
Emergency Power Distribution
Power Outage Managment Scheme

Figure 20: Interdependency of Power Management System in the Model

– *Power distribution system.* The interconnecting point for all installed power equipment is the power distribution system. Power distribution is entirely dependent on the power generation and power management systems. The integrated power management system with high power and high voltage for floating facilities offers additional regulation challenges, with many unknown problem areas in electrical generation and its distribution (Voltz, et al., 2008). The allocation of power can be divided into the following categories: *normal power distribution*, which is the distribution of the electrical load to normal processes of the facility via operating generators, functioning through dual fuels with the primary sources being fuel gas and the backup or secondary source being diesel. Offshore structures are usually equipped with an automatic transfer system so that the units switch to diesel upon the loss of fuel gas without affecting the platform load, which provides redundancy of fuel sources. *Emergency power distribution* refers to the designated emergency loads required for emergency power distribution, which are connected via emergency service transformers and feeds from normal and emergency generators. In the case of power loss from topside power generation resulting in an emergency, a dead bus relay picks up the power from emergency generators through emergency power distribution. The emergency power distribution ensures that the *energy storage technology* can be adapted for the uninterrupted operation of the control system, alarm management system, the initial start of emergency generators, and more.

– *Blackout prevention strategy.* A blackout in electrical power systems normally occurs due to short circuits, system overload, a fault in active and reactive load sharing between power generators, and more. The blackout condition presents significant safety hazards, as it will result in a total loss of the vessel’s propulsion system as well as the vital auxiliary systems, which may lead to catastrophe when the facility is operating in rough seas and in proximity to other vessels. In the case of an offshore supply vessel or drilling platform, this concern is magnified given the increased dependency on dynamic positioning systems during drilling operations. A loss of power during these critical operations could potentially threaten the failure of subsurface well connections.

The major risk factors or the common causes of the blackout that need to be avoided are as follows: (a) *load fluctuation*, (Hossain, et al., 2013) defined as malfunctioning in a power operation or the surging of electrical power distribution among critical equipment such as propulsion motors, thrusters, drilling equipment and more. The frequent energizing and de-energizing of the heavy load equipment causes certain changes in power demands and disturbs the steady state power flow to the electrical system. The load fluctuation ultimately contributes to the degradation of connected equipment, which may cause a breakdown in control and monitoring systems, resulting in power failure of the vessel. To prevent the effects of power surging or fluctuation, the designer of the vessel or platform needs to consider the careful application of surge protection to sensitive equipment that may be affected by sudden and transient load fluctuations. The (b) *warning or alarms failure* refers to a significant function of power management systems that increases the blackout prevention capabilities by informing power management systems, to prevent sudden engine loss. The pre-warning alarms should initiate the next available generators (backup or emergency) automatically if any conditions occur that seem to approach critical limits or will lead to the shutdown of the engine. The (c) *cascading failures*: an unstable generator can result from mechanical failures, load sharing malfunction, voltage regulator or reactive load sharing malfunction, overloading, maloperation of protective relays, or any other cause that contributes to a significant load imbalance for generators operating in parallel. One unhealthy generator prime mover may lead to cascading failures of all online generators, resulting in a blackout of the vessel. Generator prime movers, large consumers, and their associated auxiliary support systems should be properly maintained and effectively monitored to quickly isolate unhealthy generators or large consumers before the abnormal operation or failure can precipitate a blackout. The (d) *engine shutdown*: the (gas/diesel) engines are prominent machinery that provide the initial driving force for generating electrical power. The size and number of the engines, which are utilized for generating electrical power, depend on the amount of electrical power that is consumed by vessels onboard. The failure of one or more engines can cause the shortage of electrical power or even a total blackout, which can affect several parts of a dynamic positioning system such as the auxiliary machinery for main propulsion, computers, referencing systems, electromotors for driving thrusters, and more. The availability of backup generators and related parts need to be monitored and atomized to achieve safe operation by using control devices. Continuously monitoring the load demand and automatically starting the standby generators or removing operating generator(s) from service based on load demand is of vital importance (Hossain, et al., 2013). Finally, the (e) *system monitoring & automation* provide unique automated solutions to ensure the reliable and stable supply of shipboard power. They also allow integrated sets of controls, supervision, and management functions for engines, generators, switchboards, and the control system.

– *Load limit control system.* The optimum operation and control of the power distribution system are essential for safe operation and minimal fuel consumption. This load limiting control system is based on switching off the group of non-essential consumers or distributing the load to the critical equipment when there is a deficit of generated power. The load control system mainly performs the following tasks: (a) *controllable consumer*: with respect to controllability of load consumers, the manageable consumers are capable of precisely setting the load within the machine electrical/mechanical limits. These consumers with frequency converter drives are used in thrusters, along with other integrating loads, such as drilling activity loads, compressors, and more. The (b) *sheddable loads* can be used for system load limiting and optimal load management. The non-essential consumers can be regarded as sheddable. Switching-off the non-essential group of load consumers is necessary to transfer that load to critical and important equipment, such as navigational equipment, accommodation, the auxiliary machinery load, and more. (c) *Event based load* monitors the network/generating system and reacts based on unwanted events such as the tripping of the generating set by using event-based fast load reduction. For example, if any component fails or the generator breaker trips in the switchboard, the signal is hardwired to the remote I/O unit or is transmitted to the load limit controller and initiates the event based load reduction program within a short period to avoid disruptions (Lauvdal & Adnanes, 2000). Furthermore, the (d) *load forecast* must be done efficiently based on total system connections, and demand load calculations are completed based on equipment listed with special care and attention to the demand and diversity factors. A careful study must be made of the parallel operations, a system sized for the worst case operating scenario, with consideration to the worst case environmental situation, to ensure that the load forecast design is fit for the purpose (Craig & Islam, 2012).

– *Electric propulsion system.* The electric propulsion system is composed of the: (a) *dynamic positioning controller*, which uses high-level controllers to compute surge and sway, as yawing required to cancel the environmental effect in order to keep track of desired paths; (b) *integrated power automation systems* are necessary for optimal and safe operations to cut maintenance costs by protecting against faults and malfunctions; (c) *thrust controllers* are the allocated controllers which calculate the thrust set points for each propulsion unit with optimized criteria aiding in the reduction of extra power consumption; and (d) *vessel environment observer*, which defines the guidelines for the classification of environmental and climate conditions where the facility will operate, such as the vibration level of critical equipment, station keeping, mechanical conditions, chemical substances, temperature, humidity and more (Hansen & Wendt, 2015).

4.3.4.3 Maintenance

The maintenance activities include runtime maintenance and repair scheduling for the main electrical equipment and ensuring the availability of spare equipment, which will strengthen the resilience and maintainability of power system operations (Subbarao & Srinagesh, 2012). The active operational maintenance can be performed through (a) *preventive maintenance*, which is the key to any successful assets management program, and can be effectively implemented to reduce the reactive maintenance by applying standard conservation procedures for maintaining the ongoing integrity of the overall system and equipment; (b) *predictive maintenance*, meaning that high availability of the system can be accomplished by improved planning, increased predictive-reactive maintenance ratios and setting proper priority checks for maintenance activities; (c) *availability of maintenance staff* and *spare equipment* on site; and (d) *good practice guidance*, including operator training simulators which can be used to train the operational staff in normal and abnormal situations.

Table IV: Prior probabilities of basic events of proposed model for power system (Abimbola, Khan, Khakzad, & Butt, 2015; Khakzad, Khan, & Amyotte, 2011; OREDA, 2015; Sun, Kang, Gao, & Jin, 2016; Cetinkaya, 2001)

Basic events failure probability for proposed model of offshore power system					
Index	**Event Description**	**Assigned probability**	**Index**	**Event Description**	**Assigned probability**
1	Software failure	4.66E-03	26	Energy Storage Devices	1.10E-02
2	Identifying vulnerabilities	9.63E-04	27	Switchgear system	1.10E-02
3	Robust communication	2.52E-02	28	Generator failure	1.27E-05
4	System synchronization	9.15E-03	29	UPS system	7.54E-02
5	Abnormal situation awareness	2.00E-04	30	Normal power distribution	2.81E-02
6	Alarm system	3.67E-03	31	Energy storage system	7.54E-02
7	Emergency preparedness plan	9.20E-02	32	Emergency power distribution	2.58E-02
8	Environmental condition monitoring	3.00E-05	33	Power outage management Scheme	8.03E-03
9	Operator training	1.00E-03	34	System monitoring & automation	1.84E-03
10	Equipment vibration	2.01E-03	35	Engine shutdown	4.63E-03
11	Ageing infrastructure	1.93E-03	36	Load fluctuation	2.36E-03
12	Storage & backup power	2.50E-03	37	Warning failures	3.90E-02
13	Distributed energy source	3.82E-02	38	Cascaded failures	2.67E-02
14	Emergency response system	9.20E-02	39	Controllable consumer load	5.42E-03
15	Substitution	1.70E-02	40	Event based load	6.20E-03
16	System redundancy	2.50E-02	41	Load forecast	6.52E-03
17	Engineering Workstation/Toolkit training	3.82E-02	42	Automotive voltage regulator	5.42E-03
18	Onsite repair resources	1.00E-03	43	Thrust Controller	1.10E-02
19	Power outage management scheme	8.03E-03	44	Automated power system	7.24E-03
20	Early detection	7.20E-04	45	Dynamic positioning system	5.01E-04
21	Preventive maintenance	5.50E-05	46	Vessel environment observer	1.00E-05
22	Predictive maintenance	7.01E-04	47	Enhance information sharing	6.20E-03
23	Onsite expertise & resources	5.50E-04	48	Integrated alarm management system	9.01E-03
24	Good practice guidance	1.00E-03	49	Emergency shutdown system	9.20E-03
25	External supervision failure	8.30E-02	50	Autonomous smart grid	7.24E-03

3.4 Results and Discussions

The schematics of BN and the corresponding OOBN model are shown in Fig. 18 and Fig. 19. The power system involves different activities such as: electrical and electromechanical, the electronic sensors, and the communication system. Due to the complex infrastructure and integrated operating system involved, many risk factors may affect a power system. To achieve high efficiency and robustness of the system requires building resilient system, and its quantification needs to be conducted considering its relevant variables with failure probabilities adopted from different sources and using expert judgments for rare events (as shown in Table IV) to analyze and monitor system performance. All the variables used in the model are Boolean variables that measure a dichotomous response of the parent nodes, such as True/False, Present/Absent, and Yes/No. This includes system anticipation, system absorption, the integrated control system, and the categorized variables, where *True* represents a successful/positive outcome, and *False* represents a negative outcome. Similarly, (*Yes* and *No*) of *resilience improvement* represents the counterparts of true and false. For example, the blackout prevention control in a true state means that the system can be prevented from being a blackout scenario by achieving system monitoring through automation, minimizing cascaded failures, while a false state shows the system has failed to achieve blackout prevention.

The posterior probability distribution of an intermediate event is determined by the impact of the weighted sum of probabilities on its parent nodes. The weighted impact of each node represents the influence or effect on the parent node. Such weights are obtained based on the degree of belief using techniques such as an analytic hierarchy process and swing weights. The mean weight variable (W_{MEAN}) is presented in Eq. (23), where *i* represents the number of variables connected to the weight averaged child node; W_i is the weight associated with the *i*th variable.

$$\mathrm{W}_{MEAN} = \sum_{i=1}^{n} W_i X_i \quad 0 < W_i < 1\,; \quad \& \;\; X_i = 1, \ldots n\,; \quad \sum W_i = 1 \qquad (23)$$

The posterior probability distribution of an intermediate event is based on Boolean logic, as demonstrated in the main model in Fig. 17. For example, the association between the integrated control system and its sub-system, i.e. emergency shutdown, IF (*emergency shutdown system* = “True”, “True”, “False”), indicates that an emergency shutdown is performed successfully due to failure of any synchronized generators or electrical equipment, to avoid an increasingly chaotic situation that can occur at a facility by short circuits, sudden voltage drops, and more. The integrated control system can be actively achieved by providing a backup generator to start without interrupting an operation. The same interpretation can be used for other contributing elements of the resilience operation model to achieve high resilience.

The baseline scenario comprises the standard mode in which all the involved factors are working perfectly. This reflects the best design and operation of the power system, as shown in Fig. 18. For example, the probability table for the *integrated control system* includes *True* = 9.82E-01 and *False* = 1.80E-02, suggesting that integration of the control system is 98.2% successful, while 1.8% failure of an operation negatively affects system design and operational performance. Furthermore, *system vulnerability* has two states: *Present* = 5.10E-02 and *Absent* = 9.49E-01, which means the system has 5% vulnerability, which may affect the overall system or cause the failure of the operation, although there is a 95% chance that it works perfectly. This helps to calculate the overall resilience ratio of the system. It depicts a perfect system resilience with negligible power system failure and achieves a successful performance of the operation.

3.4.1 Sensitivity Analysis

One method to check the validity of the model is to perform sensitivity analysis on the specific nodes and check the impact of a set of variables on the selected nodes. In this case, the node *System Resilience* is considered as the *target node*, and the impact of its causal factors is measured in terms of conditional probability. The sensitivity of the power system resilience to the identified nodes in Table V is conducted by instantiating the individual node to a "False" state (scenario 1). From Table V and Fig. 21, the interpretation is quite clear: for one failure event such as *system absorptivity*, the negative impact on system resilience is lower than the impact of two or more failure events (scenario 2). It is not necessary that each impact has the same influence on its child node, which, again, as shown in Table V. Several scenarios are performed to analyze the result of system resilience. In the extreme right column of Table V are the observations made in terms of the number of failure events, and the second right most column, "system resilience', shows the observed consequences on the system's resilience.

Table V: Forward propagation scenarios

Sensitivity analysis of integrated control system failure using forward propagation scenarios

Scenarios	Maintenance	System Anticipation	System Absorptivity	System Adaptability	System Restoration	Integrated Control System	Power Generation System	Power Management System	System Resilience	Failure Events
1	–	–	F	–	–	–	–	–	8.525E-01	One
2	F	–	F	–	–	–	–	–	7.950E-01	Two
3	–	–	F	–	–	F	–	–	7.738E-01	Two
4	–	F	–	–	F	–	–	–	7.291E-01	Two
5	–	–	–	F	–	–	F	F	6.208E-01	Three
6	–	F	–	–	F	F	–	–	5.470E-01	Three
7	F	–	F	–	F	–	F	–	5.431E-01	Four
8	F	–	–	F	F	–	F	F	4.290E-01	Five

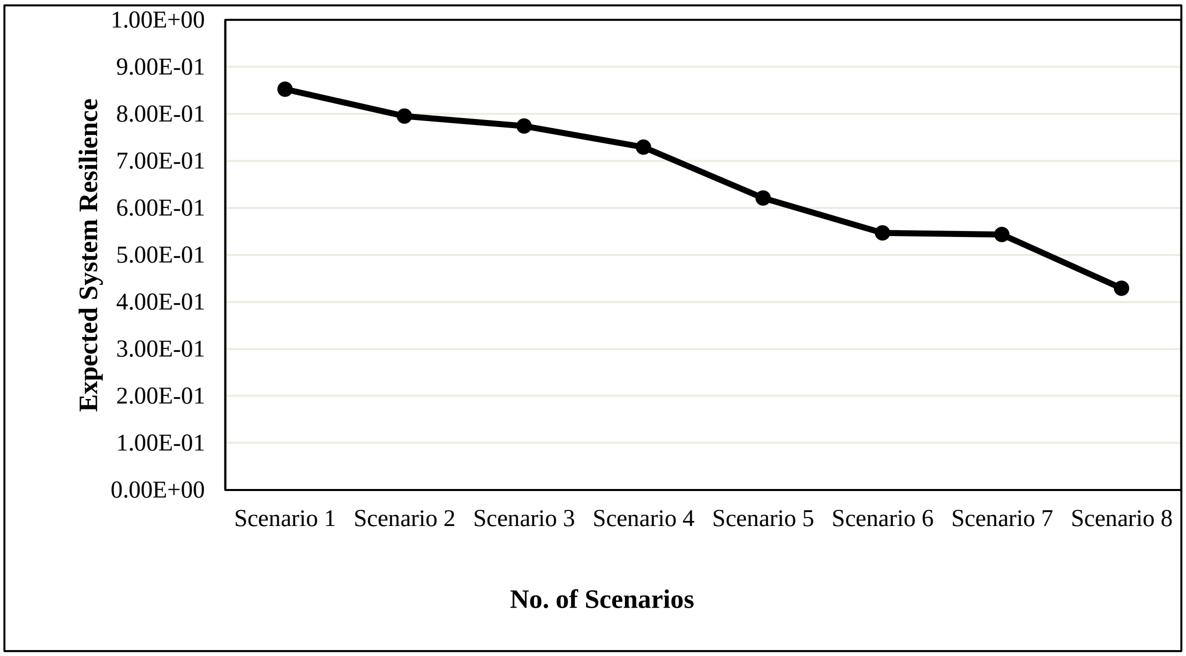

Figure 21: Resilience model sensitivity analysis

Fig. 21 depicts the graphical representation of observed scenarios and their impact on the expected system resilience. Note that the graph of expected resilience is going down from scenario 1 to scenario 8, by considering the impacts of more failure events. This signifies that the capacity of each factor contributes to the system performance.

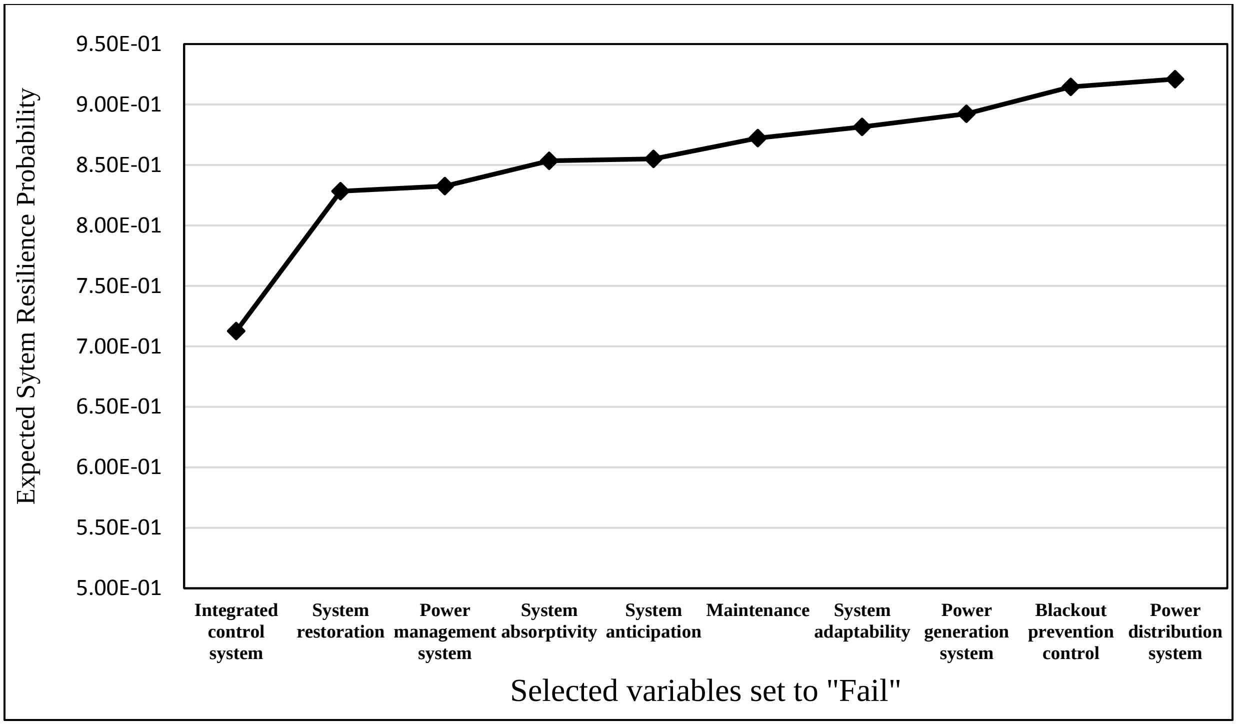

Figure 22: Impact of selected variables on system resilience, set to "Fail"

The investigation and measurement of the individual impact of a failure event on expected resilience is shown in Fig. 22. From this study, the impact of each disrupted event can be measured systematically, along with the maintainability required to achieve the desired resilience of electric power for critical infrastructure, especially systems designed for harsh environments. It can also be concluded from the given case study that the integrated control system is most sensitive and greatly affects the system performance, because it is dependent on the integrated system design and operational system. The power distribution system has less impact on system resilience. However, a combination of different failure events might have an adverse effect on system resilience.

3.4.2 Application of the Proposed Model for Major Incidents in the Offshore Oil and Gas Industry

Case 1: "*Goliat FPSO blackout incident of Barents Sea"* (Norge, 2016), occurred in an oil and gas field located in the northwest of Hammerfest, supplied with onshore hydro-generated electricity through a subsea cable. On August 26, 2016 at 22:30, production was stopped due to a complete loss of power for several hours. The production capacity was approximately 110,000 barrels per day, hence a great loss of revenue and stability of the platform. Oil fields located in harsh environments face many risk factors that can lead to blackout conditions, where the main propulsion system, associated machinery, drilling activities and more, stopped operating due to loss of power at the facility. With advanced technologies, such as load sharing, an integrated automation system, standby power and well-designed operations of the system, these losses can be avoided or overcome. The power failure halted the Barents Sea production and increased the safety risk, which resulted in economic loss. The proposed model discussed in Section 4.3 is applied to assess the impact of the power failure on system resilience where the data in Table 1 is used for the analysis due to the paucity of data from this particular incident. The model presented in this section provided possible causal factors that increased system vulnerability and control measures that could help in protecting the system from disruptions and increase the system maintainability. In the given analysis, the following factors: *system absorptive capability, blackout prevention control, and integrated control system* were considered to be unsuccessful during system design and operational activities, and the effects of the failure of these factors could be observed on the system resilience of the *Goliat* oil and gas field.

The absorptive capability of a system can be affected by its dependent features, including the backup power generation and storage and backup power capability to energize critical equipment, environmental condition monitoring, the stability of installed equipment (equipment vibration), and ageing infrastructure. Each of these factors have different effects on the disruption of the absorptive capability of the oil and gas field and their importance is determined using the weighted sum of probabilities of its parent nodes. The Noisy-OR function with a leak probability of 1.0E-02 is used to calculate the conditional probability of the factors, as discussed in Section 4.4, which suggests that if the above-mentioned factors fail, the system resilience will be reduced from 9.49E-01 to 5.73E-01, as shown in Fig. 23.

Case 2: "*Hibernia production halted by power outage"* (CBC News, 2010): an oil production platform located about 315 km southeast of St. John's, Newfoundland suspended its production due to a power outage during periodic maintenance of the main generator, which knocked out the alarm system. The emergency power restored the essential operations of the platform, but production was halted for days (CBC News, 2010). By applying the resilience model to this case study, it was observed that for the failure of the following factors: *system restorative capability*, *blackout prevention control*, and *maintenance* instantiated to a failed state as indicated in Fig. 24. The system resilience was then calculated for the Hibernia platform.

The failure of the system *restorative capacity* occurred due to the non-performance of the following factors: the *engineering workstation*, *onsite repair resources, power outage management scheme*, and retrieving *early the detection of faults*. Like Case 1, each of the factor's impact was based on its sensitivity and weight influence of its parent nodes in the system's restoration. Four causal factors were considered for system restoration, using the Noisy-OR formalism; so that if all the components failed, there was still a possibility that 1.0E-02 of the system could survive. The same criterion is applied to the *True* state, as all system restoration factors are being considered.

The model was used to investigate the result for Case 2, where the system vulnerability (chance of power loss) due to the above-mentioned factors increased from 4.0E-02 to 2.7E-01 and the overall system resilience for the degraded state was reduced from 9.49E-01 to 7.14E-01. The desired resilience of system performance can be maintained and improved upon by applying additional control measures, including: availability of stand-by generators at site, proper implementation of an energy management system, integrated power management of the complex system and its efficient power optimization, and the installation of protection relays for the critical equipment. The model quantified system resilience and its dependent features to aid designers and energy planners dealing with the shortcomings of the design and operation, as shown in Fig. 24.

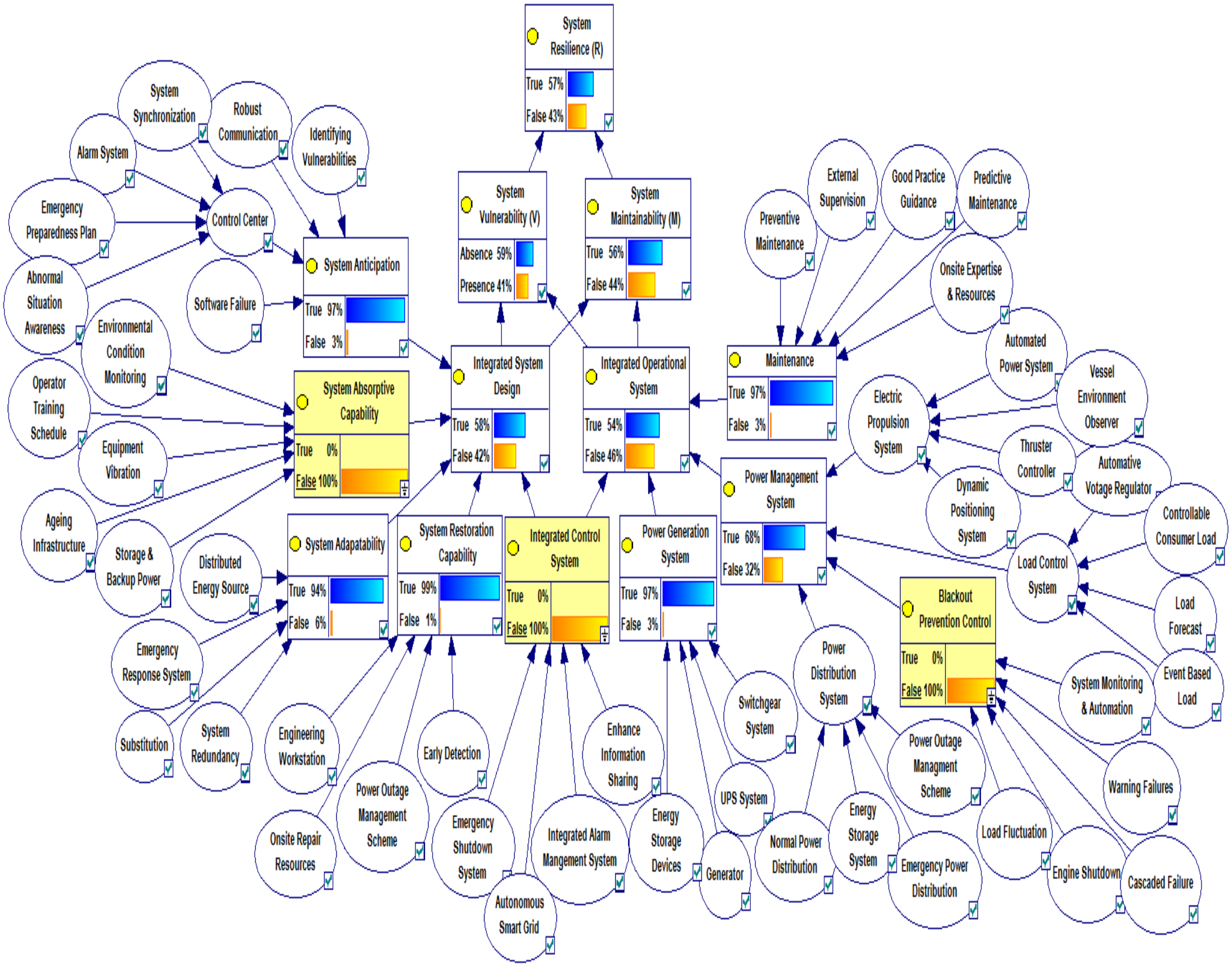

Figure 23: Bayesian simulation results for ‘Case 1’

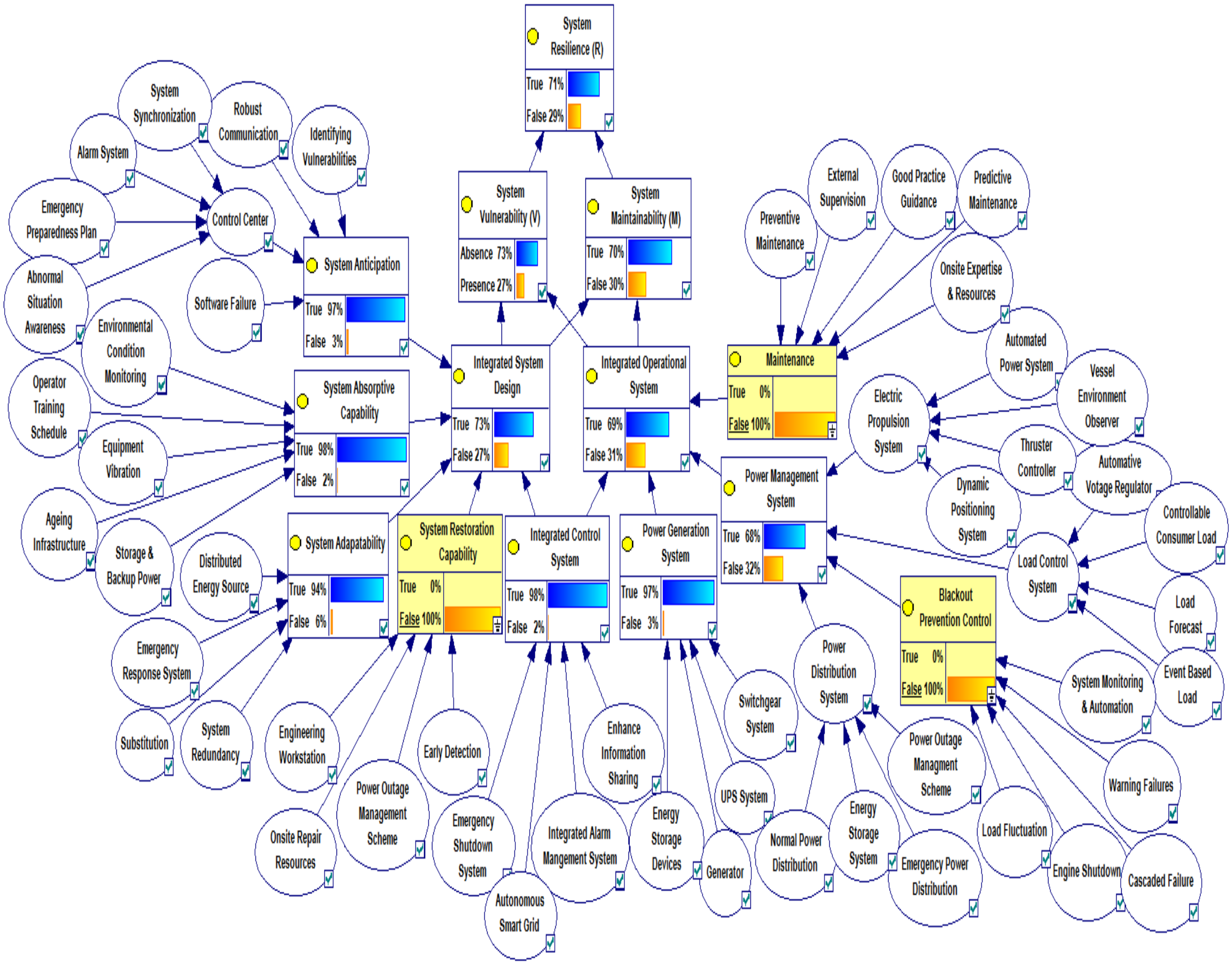

Figure 24: Bayesian simulation results for ‘Case 2’

3.5 Conclusions

This study has developed a methodology for assessing the resilience of a power management system to disruptive events using object-oriented Bayesian network formalism. This enables system designers in exploiting different strategies to assess resilience, while investigating the impact of contributing risk factors on system performance through sensitivity analysis. The sensitivity analysis has revealed that the resilience of the power management system is highly dependent on the integrated control system, system restoration system and the system absorptive capability. The resilience of offshore facilities has been discussed as a function of system vulnerability and maintainability, which can be quantified through integrated system design and its operation. Extra control measures and different scenarios have been suggested in this study to avoid the adverse effects of vulnerability and achieve higher maintainability. The Bayesian network modelling approach enables probability updating as well as conducting both predictive and diagnostic analysis.

Acknowledgments

The authors greatly acknowledge the financial support provided by the collaboration between the Norwegian University of Science and Technology (NTNU) of Trondheim, Norway, and Memorial University of Newfoundland, Canada.

References

Abimbola, M., Khan, F., Khakzad, N. & Butt, S., 2015. Safety and risk analysis of managed pressure drilling operation using Bayesian network. Safety Science, Volume 76, pp. 133-144.

Adedigba, S. A., Khan, F. & Yang, M., 2016. Dynamic safety analysis of process systems using nonlinear and non-sequential accident model. Chemical Engineering Research and Design, pp. 169-183.

Arora, K., 2004. Comprehensive production and operations management. New-Delhi: Laxmi Publication.

Arsenault, D. & Sood, A., 2007. Reslience: A systems design imperative. Arlington, VA, George Mason University.

Berkeley, A. R. & Wallace, M., 2010. A framework for establishing critical infrastructure resilience goals, s.l.: National Infrastructure Advisory Council.

Birolini, A., 2007. Reliability engineering: theory and practice. 5th ed. Berlin, Germany: Spinger.

Bobbio, A., Portinale, L., Minichino, M. & Ciancamerla, E., 2001. Improving the analysis of dependable systems by mapping fault trees into Bayesian network. Reliability Engineering and System Safety, pp. 249-260.

Cetinkaya, E. K., 2001. Reliability analysis of SCADA systems used in the offshore oil nd gas industry. Missouri-Rolla: University of Missouri-Rolla.

C. N., 2010. NL: CBC News.

Craig, C. & Islam, M., 2012. Integrated Power System Design for Offshore Energy Vessels and Deepwater Drilling Rigs. IEEE Transactions on Industry Applications, 48(4), pp. 1251-1257.

El-Gheriani, M., Khan, F. & Zuo, M. J., 2017. Rare event analysis considering data and model uncertainty. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering.

Farzin, H., Firuzabad, M. F. & Aghtaie, M. M., 2016. Enhancing power system resilience through hierarchical outage managment in multi-microgrids. IEEE Transactions on Smart Grid, pp. 2869-2879.

Fenton, N. & Neil, M., 2013. Risk assessement and decision with Bayesian networks. Boca Raton, FL: Taylor & Francis Group, LLC.

Francis, R. & Bekera, B., 2014. A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering and System Safety, Volume 121, pp. 90-103.

Gholami, A., Aminifar, F. & Shahidehpour, M., 2016. Front lines against the darkkness, enhancing the resilience of the electricity grid through microgrid facilities. IEEE Electrification Magazine, March.

Haimes, Y. Y., 2009. On the definition of resilience in systems. Risk Analysis, 29(4), pp. 498-501.

Hansen, J. F. & Wendt, F., 2015. History and state of the art in commercial electric ship propulsion, integrated power systems, and future trends. Proceedings of the IEEE, pp. 2229-2242.

Hossain, M. A., Kelly, S. J., Ahmed, M. F. & Roa, M. J., 2013. Cause and effect of catastrophic failure of shipboard and offshore vessel/platform power sources. s.l., IEEE, Industry Applications Society, 60th Annual Petroleum and Chemical Industry Conference.

Hosseini, S. & Barker, K., 2016. Modeling infrastructure reslience using Bayesian networks: A case study of inland waterway ports. Computers & industrial Engineering, pp. 252-266.

Keogh, M. & Cody, C., 2013. Resilience in regulated utilities, Washington, DC, USA: The National Association of Regulatory Utility Commissioners (NAURC).

Khakzad, N., Khan, F. & Amyotte, P., 2011. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliability Engineering and System Safety, Volume 95, pp. 925-932.

Khakzad, N., Khan, F. & Amyyotte, P., 2013. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety Science, pp. 108-117.

Khodaei, A., 2014. Resiliency-oriented microgrid optimal scheduling. IEEE Transactions on smart grid, pp. 1584-1591.

Kumar, S. A. & Suresh, N., 2008. Production and operations management (with skill development, caselets and cases). New Delhi: New Age International (P) Limited, Publishers.

Lauvdal, T. & Adnanes, A., 2000. Power management system with fast acting load reduction for DP vessels. Houston, USA, Dynamic Positioning Conference.

Lima, C., Lima, G., Quelhas, O. & Ferreira, R., 2015. Integrated operations: Value and approach in the oil industry. Brazilian Journal of Operations & Production Management, Volume 12, pp. 74-87.

Mensah, A. F., 2015. PhD. thesis: Resilience assessement of electric grids and distributed wind generation under hurricane hazards. Houston(Texas): Rice University.

Montoya, G. A., 2008. Thesis: Assessing resilience in power grids as a particular case of supply chain management, Ohio: Airforce Institute of Technology.

NIAC, 2010. A framework for establishing critical infrastructure resilience goals, Washington, D.C: National Infrastructure Advisory Council.

Nielsen, T. D. & Jensen, F. V., 2007. Bayesian networks and decision graphs. New York: Springer-Verlag.

Norge, E., 2016. Eni’s Goliat field shut down after power outage. s.l.:Offshore Energy Today Staff.

Onis´ko, A., Duzdzel, M. J. & Wasyluk, H., 2001. Learning Bayesian network parameters from small data sets: application of Noisy-OR gates. International Journal of Approximate Reasoning , pp. 165-182.

OREDA, 2015. Offshore and onshore reliability data handbook. 4th ed. Trondheim, Norway: SINTEF Participants.

Panteli, M. & Mancarella, P., 2015. Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies. Electrical power Systems Research, pp. 259-270.

Panteli, M. & Mancarella, P., 2015. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. IEEE Systems Journal, pp. 1-10.

Panteli, M. & Mancarella, P., 2015. The grid: Stronger, bigger, smarter?. IEEE Power & Energy Magazine, May/June, pp. 58-66.

Radan, D., 2008. PhD Thesis: Integrated control of marine electrical power systems, Trondheim: Department of Marine Technology, Norwegian University of Science and Technology.

Sarwar, A., Khan, F., Abimbola, M. & James, L., 2017. Resilience analysis for potential hydrocarbon release during offloading from a remote offshore oil and gas facility. Risk Analysis.(under review)..

Subbarao, M. V. & Srinagesh, Y., 2012. Integrated control system & human machine interface-Challenges for uninterrupted onshore & subsea operations. Mumbai, Society of Petroleum Engineers, pp. 1-11.

Sun, L., Kang, J., Gao, S. & Jin, P., 2016. Study on maintenance strategy for FPSO offloading system based on reliability analysis. Greece, International Society of Offshore and Polar Engineers (ISOPE).

Voltz, D. A., Islam, M. & Chaney, C. N., 2008. Diesel engine generation appliaction on ships and moored floating facilities. s.l., 55th IEEE Petroleum and Chemical Industry Technical Conference.

Vugrin, E. D., Warren, D. E. & Ehlen, M. A., 2011. A resilience assessment framework for infrastructureand economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Process Safety Progress, 3(30), pp. 280-290.

Weber, P. & Jouffe, L., 2006. Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN)*. Reliabilty Engineering & System Safety, pp. 149-162.

Weingarth, L., Manson, S., Shah, S. & Garg, K., 2009. Power management systems for offshore vessels. Houston, dynamic Positioning Conference.

Chapter 4: Conclusions and Recommendations

4.1 Conclusions

This study has developed a methodology and two models to investigate and quantify resilience. The developed models are used to study offshore facilities considering two aspects: hydrocarbon release during an offloading operation and the power management of disruptive events in offshore facilities, especially in harsh environments. To assess and quantify overall system resilience is imperative, as it is necessary to withstand inevitable difficulties, and is thus essential for the planning and execution of complex infrastructure systems. Offshore infrastructure such as drilling activities, power plants and complex facility systems are constantly dealing with natural and human-made disasters; hence, they need to be carefully designed to withstand disruptions and recover rapidly. The resilience of offshore facilities is discussed using the functions of system vulnerability and maintainability, which can be quantified through integrated system design and operation using a Bayesian network. This enables system designers to exploit different strategies to assess resilience and the underlying factors of design and operation. Investigation of the impact of each contributing factor on system performance is verified through sensitivity analysis.

To counter the negative effects of vulnerability, there is a need for a comprehensive parallel model for system maintenance and its underlying factors. The extent of vulnerability in the present model may adequately be controlled by a corresponding increase in maintainability. This study employs a feed forward network that approaches positive convergence towards system resilience. This not only ensures the strength of the model in understanding the combined effect of all underlying multi-level factors on system resilience, but also in reducing the unwanted events' probabilistic weights. The system enables engineers to predict with better accuracy the effects of any unwanted outcomes and thus manage the influence of various risk factors that inhibit normal operation within the framework. Extra control measures and different scenarios are studied and analyzed to avoid the adverse effects of a system's vulnerability and achieve higher maintainability.

The sensitivity analysis conducted helps to guide the pre-event and post-event strategies required as building blocks of resilience within the system. The generalization of this model explicitly allows researchers to further extend its use by incorporating other sets of features in the network arrangement to study the net effect of resultant factors on system resilience. The results reported from the models in case studies appear satisfactory and the built model is capable of deployment for an engineered system. The application of OOBN gives the advantage of breaking down the complex system into simplified reusable networks that can be easily combined and extended. For future work, the proposed model can be implemented for continuous variables (multi states, graphical) to improve the analysis of resilience for complex systems to minimize the design and operational risks in harsh environments. For instance, a decision support system for corrective measures and optimization of proactive design and operational systems can be studied.

4.2 Recommendations

The simulation of models is implemented using *GeNIe 2.0* and *Hugin* software, which shows the diverse and useful capability to analyze the resilience of critical infrastructure systems using a probabilistic approach. The author believes that:

- The model provides an efficient and rigorous approach to quantify resilience for any critical infrastructure based on a Bayesian network format to present quantitative risk assessment by exploring different scenarios.
- Considering the real data and reducing the assumptions in the case study will give more accurate and realistic computational results and effective implementation strategies.
- The proposed model can be implemented for continuous variables to improve the analysis of resilience for complex systems.
- The OOBN allows an effective communication between sub-networks, avoids repetition of the same node structure by enabling reusable networks, and achieves a lessened conditional probability table, which is a primary objective in dealing with a complex system.
- The generalization of this model explicitly allows researchers to further extend its use by incorporating other sets of features in correct network arrangement to study the net effect of resultant factors on either system resilience or some other outcome of high value.

- Uncertainty of the model and data needs to be investigated. A detailed uncertainty analysis combined with resilience analysis would strengthen the confidence and provide more realistic understanding of complex engineering systems.

Bibliography

American Society of Mechanical Enignеers (ASME), 2009. Innovative Technological Institute (ITI). ASME ITI, LLC, Washington, D.C.

Bakkensen, L. A., Fox-Lent, C., Read, L. K., & Linkov, I. (2016). Validating resilience and vulnerability indices in the context of natural disasters. *Risk Analysis, 37*(5), 982-1004.

Barlow, R. E., Mensing, R. W. & Smiriga, N. G., 1987. Using influence diagrams to solve a calibration problem. New York: Plenum Press.

Bensi, M., Kiueghian, A. D. & Straub, D., 2011. Bayesian network modeling of correlated random variables drawn from a Gaussian random field. Structural Safety, pp. 317-332.

Bruneau, M. et al., 2003. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra, pp. 733-752.

Dinh, L. T., Pasman, H., Gao, X. & Mannan, M. S., 2012. Resilience engineering of industrial processes: Principles and contributing factors. Journal of Loss Prevention in the Process Industries, Issue 25, pp. 233-241.

Haimes, Y. Y., 2006. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Analysis, pp. 293-296.

Haimes, Y. Y., Crother, K. & Horowitz, B. M., 2006. Homeland security preparedness: Balancing protection with resilience in emergent systems. Systems Engineering, pp. 287-308.

Hollnagel, E., Woods, D. D. & Leveson, N., 2006. Resilience engineering: concepts and precepts. Aldershot, UK: Ashgate.

Hosseini, S., & Barker, K. (2016). Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports. *Computer & Industrial Engineering, 93*, 252-266.

Hosseini, S., Barker, K. & Ramirez-Marquez, J. E., 2016. A review of definitions and measures of system resilience. Reliability Engineering and System Safety, pp. 47-61.

John, A., Yang, Z., Riahi, R. & Wang, J., 2016. A risk assessment approach to improve the resilience of a seaport system using Bayesian networks. Ocean Engineering, October.pp. 136-147.

Keogh, M. & Cody, C., 2013. Resilience in regulated utilities, Washington, DC, USA: The National Association of Regulatory Utility Commissioners (NAURC).

Langseth, H. & Jensen, F. V., 2003. Decision theoretic troubleshooting of coherent systems. Reliability Engineering & System Safety, pp. 49-62.

Langseth, H. & Portinale, L., 2007. Bayesian networks in reliability. Reliability Engineering & System Safety, pp. 92-108.

Liu, X., Shahidpour, M., Li, Z., Liu, X., Cao, Y., & Bie, Z. (2016). Microgrids for enhancing the power grid resilience in extreme conditions. *IEEE Transactions on Smart Grid*, 1-8.

Luthar, S. S., Cicchetti, D. & Becker, B., 2000. The construct of resilience: A critical evaluation and guidelines for future work. Child Development, pp. 543-562.

Mahadevan, S., Zhang, R. & Smith, N., 2001. Bayesian networks for system reliability reassessment. Structural Safety, pp. 231-251.

Rose, A., 2007. Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. Environmental Hazards, pp. 383-398.

Sheard, S., 2008. A Framework for system resilience discussion. INCOSE.

Sheffi, Y., 2005. The resilient enterprise: Overcoming vulnerability for competitive advantage. 1st ed. Cambridge: MIT Press Books.

Straub, D. & Kiureghian, A. D., 2010. Bayesian network enhanced with structural reliability methods: Methodology. Journal of Engineering Mechanics, pp. 1248-58.

Thorisson, H., Lambert, J. H., Cardenas, J. J. & Linkov, I., 2017. Resilience analytics with application to power grid of a developing region. Risk Analysis, 37(7), pp. 1268-86.

Vogus, J. T. & Sutcliffe, K. M., 2007. Organizational resilience: Towards a theory and research agenda. In: Proceedings of the IEEE international conference on systems, man and cybernetics, pp. 3418-3422.

Vugrin, E. D., Warren, D. E., Ehlen, A. M. & Camphouse, R. C., 2010. A framework for assessing the resilience of infrastructure and economic systems. K. Gopalakrishnan & S. Peeta (Eds.): Sustainable & Resilient Critical Infrastructure Systems, pp. 77-116.

Webb, C. T., 2007. What Is the role of ecology in understanding ecosystem resilience?. BioScience, pp. 470-471.