

Doctoral thesis

Doctoral theses at NTNU, 2022:40

Lin Xie

Safety barriers in complex systems with dependent failures

Modeling and assessment approaches

NTNU
Norwegian University of Science and Technology
Thesis for the Degree of
Philosophiae Doctor
Faculty of Engineering
Department of Mechanical and Industrial
Engineering



Norwegian University of
Science and Technology

Lin Xie

Safety barriers in complex systems with dependent failures

Modeling and assessment approaches

Thesis for the Degree of Philosophiae Doctor

Trondheim, January 2022

Norwegian University of Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

NTNU

Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Engineering

Department of Mechanical and Industrial Engineering

© Lin Xie

ISBN 978-82-326-6376-7 (printed ver.)

ISBN 978-82-326-6373-6 (electronic ver.)

ISSN 1503-8181 (printed ver.)

ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2022:40

Printed by NTNU Grafisk senter

Preface

This thesis is submitted to the Norwegian University of Science and Technology (NTNU) to partially fulfill the requirements for the degree of Doctor of Philosophy. The main work of the Ph.D. thesis was carried out at the Department of Mechanical and Industrial Engineering (MTP) of the Faculty of Engineering in Trondheim, Norway. The work was accomplished under the supervision of Associate professor Yiliu Liu and Professor Mary Ann Lundteigen (current affiliation: Department of engineering cybernetics at NTNU).

This work's target readers include researchers and practitioners interested in the following fields: reliability engineering, safety engineering, risk management, and oil and gas industry engineering. It is assumed that the readers have basic knowledge of reliability, preferably related to safety instrumented systems.

Trondheim, Norway

September 2021

Lin Xie

This page is intentionally left blank

Acknowledgment

Life is like a river, smoothly running along its grassy borders in silence. Yet, over four years, I can still remember the time when I was asked why I applied for a Ph.D. in the interview. Indeed, at that time, I did not know what I looked for and what I would experience while pursuing a Ph.D. Nevertheless, my heart had a voice that said I wanted to challenge myself by creating fresh knowledge and developing new skills. Looking back now, I realize that doing a Ph.D. can be intellectually challenging, physically tiring, and emotionally draining. However, it could be the best decision I ever made, both for academic research and personal development.

In the river of life, there may be many people who offer help and lead the direction. The completion of this work could not have been possible without their support. First, I would like to express my deepest appreciation to my main supervisor, Associate Professor Yiliu Liu, for providing the opportunity to do research and for the invaluable guidance and ingenious suggestions throughout this research. I appreciate all his contributions of tremendous time and tireless patience to review my work repeatedly. He has been a supportive friend over the years and always encouraged me to explore the field. In addition, I extend my heartfelt thanks to his wife and family for the invitations to dinners.

I would like to give heartfelt and special thanks to my co-supervisor, Professor Mary Ann Lundteigen. She was also the supervisor for my master's project, which opened the door of the RAMS world to me. I am profoundly grateful for her insightful advice, knowledge, supervision meetings, and inspiring discussions. I was impressed that she has never missed and delayed my requests even though she had to work late at night. From her, I have learned professionalism, writing skills, and organization techniques.

My sincere thanks are also extended to Professors Jørn Vatn and Per Schjølberg at the department for supporting my work. I would also like to thank the co-author of my article, Solfrid Håbrekke at SINTEF, who shared her knowledge and provided data for the research. Besides, I am very grateful to Professor Elias Kassa at the Civil and Environmental Engineering Department at NTNU for supporting international exchange. Many thanks to Professors Wanmin Zhai and Shengyang Zhu at Southwest Jiaotong University and Professor Yanfu Li at Tsinghua University, China, for their help during my visit.

Warm thanks to my colleagues and friends in the RAMS group for seminars, coffee breaks, and social events. To Aibo, Renny, Himanshu, Shenae, Juntao, Yun, Xingheng, Behanz, Bahareh, Michael, Federico, Jon Martin, Nanda, Ewa, Ariful, Tianqi, Yixin, Jie, and all dear others, you are acknowledged for sweat cakes, girls' meetings, ping-pong time, and lovely dinners. I am deeply thankful for visiting friends Lei, Dongming, Xinge, Xiaopeng, Yukun, and Shengnan for our happy times together. I am also grateful to the administrative staff at the department, Kari, Monica, Gabriela, Linn, and Øyvind, for being helpful whenever I needed.

I know that, in the river of life, endless time heaves like sea waves with pleasure and sorrow. People will in this river taste the joys of new life and get through grief and loss with their families. Thus, I am especially thankful to my mother and father for their unconditional love

and care. To my beloved husband Xiaobo, thanks for his relentless and unwavering support. My lovely son Zhichu and daughter Wanchu made me responsible and helped me understand life better.

In this river of life, we cannot despair even in the darkest hour because there is a new day after every night. We have only one choice that, therefore, is to keep moving on and be hopeful.

Trondheim, Norway

September 2021

Lin Xie

Hope is the thing with feathers

*“Hope” is the thing with feathers-
That perches in the soul-
And sings the tune without the words-
And never stops-at all-*

*And sweetest-in the Gale-is heard-
And sore must be the storm-
That could abash the little bird
That kept so many warm-*

*I’ve heard it in the chilliest land-
And on the strangest sea-
Yet-never-in extremity,
It asked a crumb-of me.*

--Emily Dickinson (1862)

Summary

Technical systems are becoming more and more complex. They often consist of many components with a degree of dependencies. These dependencies cannot be adequately predicted, understood, and analyzed. In addition, failures due to dependencies are often not expected to be single but multiple. As a result, in complex systems, such dependency issues can significantly reduce system reliability and cause catastrophes without proper prevention and mitigation. Therefore, a variety of control measures, such as safety barriers, are necessary to be adopted against dependent failures and ensure the safety of technical systems. They are related to implementing safety functions to avoid, prevent, control, and mitigate the effects of dependent failures.

As a type of safety barrier, safety instrumented systems (SISs) are widely installed to prevent or mitigate the consequences of accidents in the process industries and other sectors. In practice, SISs are often employed to prevent dependent failure from occurring and alleviate their severe consequences. The operation and performance of SISs are thus of great significance to ensure the safety of production systems. Although however, independence is an essential performance requirement to make SISs effective and practical, such equipment is rarely fully independent from the operational context. In many cases, SISs may inevitably suffer from dependency issues, such as dependent failures that include common cause failures (CCFs) and cascading failures (CAFs).

In the current literature, neither the effects of dependent failures within safety barriers nor the effects of SISs against dependent failures have been well studied. It seems that most attention has been directed to CCFs and in specific for SISs where redundancy is used to enhance reliability. Thus, it is desirable to analyze and model the effects of safety barriers in complex systems considering some dependency issues, such as dependency between safety barriers and the environment, dependent failures within safety barriers, and safety barriers against dependent failures.

This Ph.D. thesis bridges safety barriers and complex systems by considering the dependency issues between them. The aim is broken into four specific objectives addressed in five journal articles and three conference articles. The thesis contributes to strengthening the link between safety barriers and complex systems by proposing:

- A clarification of differences and similarities between two categories of dependent failures. Based on that, safety barrier strategies to protect against dependent failures are discussed. The research may increase the awareness and treatment of dependent failures in design and operations.
- A new framework for identifying significant influencing factors from the environment and complex systems. It is expected to present new ideas and insights to update failure rates in performance analysis of safety barriers and model the effects of dependent failures in complex systems.

- Models and approaches for assessing the performance of safety barriers considering CAFs. This thesis presents new perspectives and approaches to deal with CAFs within or between safety barriers.
- Models and approaches for assessing the performance of safety barriers to prevent CAFs. It concerns the reliability of complex systems and the durability of safety barriers during demands. Thus, it provides guidelines for efficient mitigations for a given resource situation and limited budget.

From an academic perspective, this thesis suggests models and approaches for assessing the effects of dependent failures and safety barriers against dependent failures. The proposed approaches and models serve two purposes. The first one is related to provide a holistic performance analysis of safety barriers in preventing dependent failures. The second purpose is to establish some guidelines for safety designers to improve the performance of complex systems.

From the application perspective, this thesis reminds both designers and operators to recognize the effects of dependent failures in complex systems, notably the effects of cascading failures. The thesis opens a new view of safety barriers in the context of dependent failures. It offers practical approaches to evaluate the performance of safety barriers, and they can be implemented in safety barriers and other systems with similar operational characteristics.

The work identifies many challenges that can be research lines in the future. For example, one area is implementing new approaches and models to existing industry practices or complex technical systems, such as network, hierarchical, and dynamic systems. Another area is developing and improving approaches and models to account for the operations, such as maintenance and testing.

Contents

- Preface..... I
- Acknowledgment III
- Summary V
- List of Figures VI
- List of Tables VII
- Acronyms and abbreviations..... VIII

- Part 1 Main report 1
- 1. Introduction 3
 - 1.1 Background 3
 - 1.2 Objective 5
 - 1.3 Scope and limitations 5
 - 1.4 Structure of the thesis 5
- 2 Theoretical background 7
 - 2.1 Complex system 7
 - 2.1.1 Complexity..... 7
 - 2.1.2 Dependency..... 8
 - 2.2 Dependent failure 8
 - 2.2.1 Basic concepts of dependent failure 8
 - 2.2.2 Causes and classifications of dependent failures 9
 - 2.2.3 Modeling dependent failures..... 11
 - 2.3 Safety barrier 14
 - 2.3.1 Concept of safety barrier..... 14
 - 2.3.2 Classification of safety barriers 15
 - 2.3.3 Barrier performance 16
 - 2.3.4 Barrier analysis 17
 - 2.4 Safety instrumented system..... 19
 - 2.4.1 The basic concept of SIS..... 20
 - 2.4.2 SIS operations and failures 20
 - 2.4.3 SIS performance measures..... 22
 - 2.4.4 SISs considering dependent failures 23
 - 2.5 Summary 25

3	Research questions and objectives	27
3.1	Research questions	27
3.1.1	Dependency issues	27
3.1.2	Safety barriers	28
3.2	Research objectives	29
4	Research principles and approaches	31
4.1	Research principles	31
4.2	Research approach.....	31
5	Main results	35
5.1	Overview	35
5.2	Main contributions	35
5.2.1	Contribution 1	35
5.2.2	Contribution 2	37
5.2.3	Contribution 3	38
5.2.4	Contribution 4	40
6	Conclusions and future work	43
6.1	Conclusions	43
6.2	Future work	44
6.2.1	Complex system.....	44
6.2.2	Maintenance issues	44
6.2.3	Approaches and models	44
6.2.4	Implementation	44
	Reference	45
	Part 2 Articles	53
	Article I	55
	Article II.....	65
	Article III.....	73
	Article IV	85
	Article V.....	103
	Article VI	115
	Article VII.....	123
	Article VIII.....	141

List of Figures

Figure 1 Causes of CCFs and CAFs	9
Figure 2 The risk reduction process	15
Figure 3 Classification of safety barrier	15
Figure 4 The risk reduction of a safety barrier	16
Figure 5 A general configuration of an SIS and EUC	20
Figure 6 A often used classification of SIS failures	21
Figure 7 A demand may occur while a DU failure is present in low-demand systems	21
Figure 8 Relationships between research questions and research objectives	30
Figure 9 Overall process of the Ph.D. research project	32
Figure 10 Safety barriers for CCFs and CAFs in extended bow-tie model	36
Figure 11 Illustration of the similarities and differences between CCFs and CAFs	36
Figure 12 Framework for identifying critical influences and predicting failure rates	38
Figure 13 RBD with a CAF between component i and j	38
Figure 14 Comparison of the factors for CCFs and CAFs.....	39
Figure 15 System reliability profiles for different states of SISs.....	41

List of Tables

Table 1 List of articles in part II	6
Table 2 Definition and classifications of CAFs	10
Table 3 A comparison of the models for CCFs and CAFs	12
Table 4 A comparison of some models for barrier analysis	17
Table 5 Intervals of the PFD_{avg} and PFH corresponding to the SILs	23
Table 6 A comparison of some models for SISs considering CCFs	24
Table 7 Research execution plan for the PhD project.....	33
Table 8 Overview of the contributions and relevant objectives	35
Table 9 Examples of safety barriers against CCF and CAF	37
Table 10 Approximation formulas for PFD_{avg} with CAFs after simplification	39
Table 11 PFH of various structures with CAFs	40

Acronyms and abbreviations

ALARP	As low as reasonably practicable
BORA	Barrier and operational risk analysis
CCF	Common cause failure
CAF	Cascading failure
DD	Dangerous detected
DU	Dangerous undetected
ESD	Emergency shutdown
E/E/PE	Electrical, electronic, and programmable electronic
EUC	Equipment under control
EXDIA	Safety Equipment Reliability
ETA	Event tree analysis
FDD	Failure during demand
FOD	Failure on demand
FTO	Fail to open
FTA	Fault tree analysis
IEC	International Electrotechnical Commission
ISO	International Organization for standardization
LOPA	Layer of protection analysis
OREDA	Offshore and Onshore Reliability Data
PFDavg	Average probability of failure on demand
PFH	Average frequency of dangerous failure
PSD	Process shutdown
PSV	Pressure safety valve
PDS	Reliability Data for Safety Instrumented Systems
RBD	Reliability block diagram
SD	Safe detected
SU	Safe undetected
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system

This page is intentionally left blank

Part 1

Main Report

This page is intentionally left blank

Chapter 1

1. Introduction

This chapter briefly introduces the background for this Ph.D. thesis and presents the objectives, scope and limitations, and structure.

1.1 Background

Technical systems are becoming more and more complex due to the increasing integration of communication technologies and the extensive use of digital infrastructure [1]. These complex systems often consist of many components with a degree of interrelationships and interdependencies. Such systems may not be designed but may become complex through changes and coupling [2]. The components are gradually developed to be logically or physically interactive and interdependent. Based on the current knowledge, it is challenging to understand and predict the interactions fully. Such complex systems can be found in diverse industrial systems, including, but not limited to, railway signaling systems, industrial control systems, information processing systems, and energy distribution networks.

In a complex system, failures are not expected to be single but multiple and often dependent. Dependent failures occur in more than one component, resulting in extensive damage to the entire system. Dependent failures mainly include CCFs and CAFs. CCFs refer to the failures resulting from one or more events due to shared causes, whereas CAFs are defined as the failures of an item resulting from a root cause, which then causes other failures of the same or different item [3]. Past accidents and near misses have indicated that dependent failures are significant threats to complex systems [4, 5]. For example, CCFs are essential contributors to the unavailability of safety systems in the oil and gas industry [6]. Electricity loss or attacks can lead to the cascading interruption of communications and a blackout in power systems [7, 8]. CAFs greatly impact internet systems due to the interactions and dependencies between devices in function and structure [9]. Many infrastructure systems such as water distribution networks and transportation also often suffer from CAFs [10, 11].

Dependent failures may cause catastrophes in complex technical systems without proper prevention and mitigation [12]. Therefore, safety barriers are necessary to be installed against dependent failures. Safety barriers are the physical or non-physical means to prevent, control, or mitigate undesired events or accidents [13]. The functions of safety barriers are commonly related to prevention to reduce accident probability, control deviation, and mitigation of accident developments [13]. However, safety barriers also have a significant mitigation potential in controlling the risk induced by dependent failures. A typical example of such safety barriers is applying a heat-resistant coating on process equipment to avoid its catastrophic failure due to fire exposure [4].

SISs as safety barriers are widely installed to reduce accidents in the process industries and other sectors. An SIS typically applies electrical/electronic/programmable electronic (E/E/PE) technologies to detect and act upon hazardous situations arising in the assets. The assets can be humans, equipment, or process sections, and they are called equipment under control (EUC) in

the generic standards for SISs IEC 61508 and IEC 61511 [14, 15]. An industrial facility usually is equipped with many SISs. For example, process shutdown (PSD) systems can stop production in case of process upsets, while emergency shutdown (ESD) systems are designed to reduce the escalation of uncontrolled events like leakages by depressurizing [16]. SISs can also be found in many transportation systems like railway signaling systems, where SISs provide light signals and operate switches [17].

The operation of SISs is of great significance to ensure the safety of EUC systems, and thus, the performance of SISs is particularly critical. Performance assessment is used to qualify SIS for a specific application with the given functional requirement and may have different indicators. The indicators may include specificity, functionality, reliability, response time, capacity, durability, robustness, audit-ability, and independence [18]. Reliability is the most important one guiding SIS design, construction, and operation [17]. Therefore, when an SIS is put into operation, its operational data should be collected, and the SIS must be demonstrated to meet reliability requirements.

Even though independence is also an essential requirement for SISs to ensure that safety barriers are effective and practical, they are rarely fully independent [19]. Sometimes, SISs may inevitably suffer from both CCFs and CAFs [18], even though they are used to prevent these dependent failures from occurring within EUCs. CCFs commonly exist in SISs where redundancy is used to enhance reliability actively. It is thus required to consider the contributions of CCFs in quantitative reliability analyses. Many models have been introduced for this purpose, incorporating the traditional reliability analysis approaches, such as fault tree analysis, Markov methods, and event tree analysis [1]. The defenses to CCFs are typically removing the causes and introducing measures to reduce the effects of CCFs.

SISs can also be vulnerable to CAFs originating from shared loads, shared maintenance resources, hazardous events, and dependent functions [1, 9]. However, neither the effectiveness of safety barriers protecting EUC from CAFs nor the effects of CAFs on safety barriers have been well studied in the current literature [19]. There are some challenges for this research. For example, some dependency issues in a complex system, such as influencing factors or dependent failures within the components, have not been well studied. In addition, the critical concepts related to CAFs in safety barriers are not defined and thoroughly explored. There is a lack of comprehensive comparison on CCFs and CAFs to distinguish two failures from concepts, causes, mechanisms, and consequences. Safety barrier designers still lack the guidance to set up efficient ways to prevent or mitigate the CAFs effect. Further, there seem to be insufficient attempts to analyze and model the effects of safety barriers in complex systems, considering dependent failures, particularly for CAFs.

This Ph.D. project is therefore intended to analyze safety barriers in a context with CAFs. First, it is necessary to distinguish the effects of CCFs and CAFs. The effects of CAFs in terms of safety barriers also have different impacts. The effects of CAFs can be within or between the components in safety barriers. CAFs within safety barriers mean that the barriers suffer from CAFs that reduce system safety and reliability. The effects of CAFs can also impact the functions of safety barriers that are employed to prevent CAFs. The challenging question is how to identify these safety barriers against CAFs and evaluate these effects of CAFs on safety barriers.

1.2 Objective

Based on the background for the research, the main objective of this thesis is to improve the understanding and modeling of safety barriers with dependent failures in complex systems, with a particular focus on the effects of CAFs.

To realize the overall objective, we will conduct the following specific tasks:

1. Study the effects of dependency issues in complex systems considering influences and dependent failures.
2. Discuss the differences between CCFs and CAFs, and distinguishing safety barriers strategies to protect against or mitigate the effects of the two failures.
3. Propose models and approaches for evaluating the impacts of CAFs in complex systems and investigating the effects of safety barriers against CAFs.
4. Provide new insights into the design and deployment of safety barriers to prevent CAFs.

1.3 Scope and limitations

The motivation of the thesis is to improve the basic understanding of safety barriers with dependent failures and the effects of safety barriers in protecting complex systems. The approaches and models in this thesis are applied to SISs and EUC systems, but they can also be adopted in safety barriers in other systems. The research is mainly carried out in the oil and gas and energy industry. However, the results could be relevant for other industries.

The results in this thesis are encouraging both in qualitative and quantitative analysis. However, the effectiveness of safety barriers is affected by many factors, and it is not easy to consider all the factors; thus, the relevant discussion is restricted. In addition, with the increasing complexity of systems, dependencies between the components grow exponentially. Therefore, the efficiency of the proposed approaches and models is expected to be improved.

1.4 Structure of the thesis

The thesis consists of two parts: Part I introduces the research background and research framework and highlights the research questions and contributions of the thesis. Part II is a collection of articles that represent the outcomes of the research.

The remainder of Part I is organized as follows: Chapter 2 summarizes the theoretical background of the research to understand the behaviors of safety barriers with dependent failures and reviews the models for analyzing the performance of safety barriers. Chapter 3 describes the objectives of the thesis and main research questions. Then, in Chapter 4, the research methodology and work process are elaborated. Finally, the main results and further works are discussed and summarized in Chapters 5 and 6.

Part II includes eight research articles that have been published or submitted during the Ph.D. project in international journals or conference proceedings. The articles are listed in Table 1.

Table 1 List of articles in part II

No.	Type	Article	Reference
I	Conference	Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Common cause failure and cascading failures in technical systems: similarities, differences, and barriers. <i>Proceedings of the 28th European Safety and Reliability Conference (ESREL)</i> , June 17-21, 2018, Trondheim, Norway.	[3]
II	Conference	Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Safety barriers against common cause failure and cascading failure: literature reviews and modeling strategies. <i>Proceedings of IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)</i> , December 16-19, 2018, Bangkok, Thailand.	[20]
III	Journal	Xie, Lin; Håbrekke, Solfrid; Liu, Yiliu; Lundteigen, Mary Ann. Operational data-driven prediction for failure rates of equipment in safety instrumented systems: A case study from the oil and gas industry. <i>Journal of Loss Prevention in the Process Industries</i> (2019); Volume 60. s. 96-105.	[16]
IV	Journal	Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Reliability and barrier assessment of series-parallel systems subject to cascading failures. <i>Proceedings of the Institution of Mechanical Engineers. Part O, Journal of Risk and Reliability</i> (2020); Volume 234. (3) s. 455-469.	[21]
V	Journal	Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Performance assessment of K-out-of-N safety instrumented systems subject to cascading failures. <i>ISA transitions</i> (2021); Volume 118. s. 35-43.	[22]
VI	Conference	Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Performance Assessment of Safety-instrumented Systems Subject to Cascading Failures in High-demand Mode. <i>Proceedings of the 29th European Safety and Reliability Conference (ESREL)</i> , September 22-26, 2019, Hannover, Germany.	[23]
VII	Journal	Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Performance analysis of safety instrumented systems against cascading failure during prolonged demand. <i>Reliability Engineering and Safety System</i> (2021); Volume 216. s. 107975.	[24]
VIII	Journal	Xie, Lin; Ustolin, Federico; Lundteigen, Mary Ann; Li, Tian; Liu, Yiliu. Performance analysis of safety barriers against cascading failures in a battery pack. <i>Submitted to Reliability Engineering and Safety System</i> .	[25]

Chapter 2

2 Theoretical background

This chapter reviews the theoretical literature related to complex systems, safety barriers, and dependent failures. The motivation behind this is twofold: 1) to provide highlights of concepts and methodologies that are the basis for this dissertation; 2) to establish research questions by understanding the state of the field and revealing the challenges. The review starts with discussions of the complex system perspective, followed by definitions and causes of dependent failures. Then, it continues with models of dependent failures and methodologies of safety barriers for preventing dependent failures. The last part of the review focuses on a specific safety barrier SISs.

2.1 Complex system

Over the past decade, the interest in complex systems has grown by introducing systems engineering techniques rather than separate components. However, there is no universal and concise definition of a complex system. Instead, researchers in different fields attempt to define a complex system in various ways. For example, Perrow claimed that some technical systems are characterized by high interactive complexity [26]. MIT [27] also defines complex systems as systems with numerous components and interconnections or dependencies.

Rausand and Haugen [2] classified a system into three categories: simple, complicated, and complex. Both complicated systems and complex systems have many components with a degree of interrelationships and interdependencies between components. The difference between complicated and complex systems is that the interactions in the latter are not entirely understandable using all current knowledge. As a result, the performance of a complex system cannot be adequately predicted by linear relationships. Generally, complex systems are challenging to describe, understand, predict, manage, design, and change, not only because they consist of many components but also because the interconnections among components are complex. The two terms, complicated- and complex systems, are not strictly distinguished. Therefore, we use the term complex systems, considering the two sub-categories into one group.

Complex systems may have many attributes, such as complexity, system states, functions, dependence, the realm of existence, origin, and boundary. Furthermore, due to complexity and dependencies, complex systems are likely to show their multiplicity, diversity, and interactivity [28]. Therefore, this thesis focuses on complex systems' characteristics: complexity and dependency explained in the following sections.

2.1.1 Complexity

Complexity is defined as a scientific theory that the systems that display behavioral phenomena are completely inexplicable [2]. Complexity is related to the amount of information needed to describe the system, the number of elements in the system, and the number of interconnections [27]. Sammarco [29] listed some technological or organizational attributes of complexity, e.g., the proximity of physical components, unintended feedback loops, interacting control parameters, incomplete information, and limited understanding of the system. Many technical systems are becoming more complex, and they often exhibit dynamic complexity (e.g., multi-

state of components), structural complexity (e.g., various structures), functional complexity (e.g., new functions), and complex environments (e.g., many performance influences). It is challenging to identify the influences of the environment and predict their performance considering the changes.

2.1.2 Dependency

Dependency is defined as the relationship between two elements in which a change to one element may affect or supply information needed by the other element [30]. The dependency of a complex system concerns its structure, economic factors, resources, performance, and failures. Existing literature usually distinguishes three dependencies: structural, stochastic dependence, and economic dependence [31, 32]. Structural dependence relates to the degradation of components in operation, and the lifetime distributions of components will be affected [33]. Stochastic dependence refers to the cases that one component is dependent on the state of one or more other components [32]. In addition, economic dependence applies for cases when the combined maintenance of several components leads to a different cost [32].

We mainly focus on the structural and stochastic dependence in this work, meaning that one component's deterioration process depends on the state of one or more other components. Traditional approaches cannot analyze a complex system since it is more than a sum of its components due to dependency [2]. In other words, in complex systems, the failure of two or more components interacts unexpectedly due to connections and interrelationships which involve systems and their environment.

2.2 Dependent failure

A dependent failure may arise from stochastic dependence between components and subsystems in a complex system. Dependent failures can significantly reduce the system's reliability, wherein the system often consists of many components.

2.2.1 Basic concepts of dependent failure

One observation from the literature is that there is no universal definition for dependent failures. According to the standards IEC 61511 and IEC 61508, dependent failures are defined as the failures whose probability cannot be expressed by unconditional probabilities of the individual event [14, 15]. In addition, ISO 26262 defines dependent failures as the failures that may hamper the required independence between given components [34]. Dependent failures occur in several components that are influenced or affected by either external or internal impacts, for example, hazardous events, environmental factors, shared resources, and dependent functions. On the contrary, independent failures are failures with the occurrence probabilities not affected by other components, such as an age-related failure. Even though an independent failure does not result from other failures, it can influence other components and start more dependent failures.

Generally, dependent failures may mainly be classified into negative and positive dependencies [12]. Negative dependencies refer to single failures that reduce the likelihood of failure of other components, but they are usually not relevant and are harmful to reliability applications. On the other hand, positive dependencies, including CCFs and CAFs, mean that the components are positively correlated. Hence, they are primarily relevant in the reliability analysis. That is the reason that only CCFs and CAFs are considered in this Ph.D. work.

CCFs refer to the failures resulting from one or more events, causing concurrent failures of two or more separate channels [14]. CAFs are defined as the failures of an item resulting from a

root cause, which then causes other failures of the same or different item [34]. CAFs are identified in the literature in similar terms with a different focus, such as induced failures [35], domino failures [36], propagated failures [37], escalating failures [38], and interaction failures [39]. Both CCFs and cascading failures result from some common vulnerabilities of more than one component. Furthermore, the two types of failures are interrelated in some cases. For example, CAFs could be one of the possible root causes of CCFs, but CCFs cannot be CAFs [34].

2.2.2 Causes and classifications of dependent failures

Studying the reasons for dependent failures is associated with identifying the causes and problems. Therefore, such a study can help one concentrate on the possible causes and relevant measures to avoid dependent failures. Therefore, it is required to investigate the causes of CCFs and CAFs separately.

It is common to split CCF causes into root causes and coupling factors[1]. A root cause of a failure is the most fundamental cause, whereas a coupling factor explains why several items are affected by the shared root cause. The root causes may be split into trigger events, conditioning events, and proximate causes [40]. If the root causes of CCFs are corrected, it will prevent similar failures. A coupling factor is a property that makes multiple components susceptible to failure from a single shared cause. CCFs often occur in the system with a high degree of redundancy because the components have the same properties. According to the report [41], the properties of CCFs concerns root causes and coupling factors, as illustrated in Figure 1. The root causes may be internal components, inadequate design and manufacture, human actions, maintenance, inadequate procedure, and abnormal environmental stress. Coupling factors emphasize the same properties that may overlap with root causes, e.g., same hardware design, similar operational conditions, and same maintenance staff [42] [6].

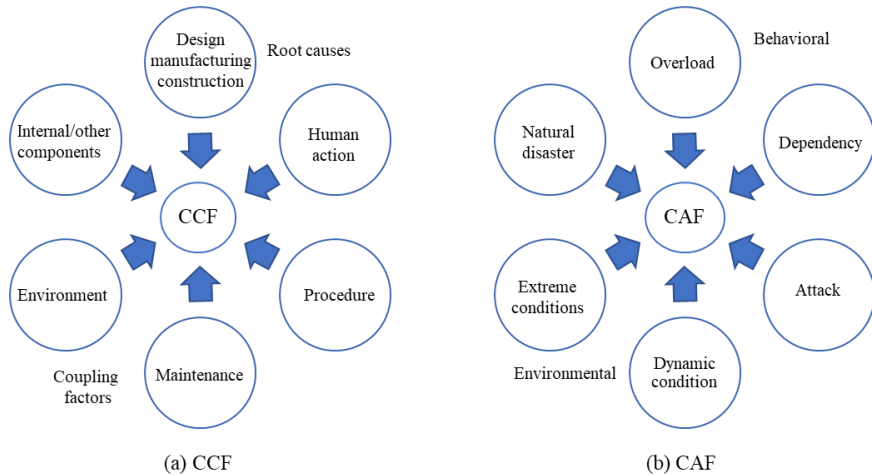


Figure 1 Causes of CCFs and CAFs

As for CAFs, the root causes can be categorized into behavioral and environmental factors [9]. The behavioral factors include overload (e.g., redistribution of loads due to one component's failure [43]), dependency (e.g., structural dependence [5]), and attacks (e.g., cyber-attacks [44]). In addition, CAFs can also be triggered due to coupling factors like environmental factors, such as natural disasters (e.g., fire and earthquake [45, 46]), extreme conditions (e.g., heat waves [47]), and dynamic conditions (e.g., elevated temperature [48]). Because of these

coupling factors in complex systems, a failure in one or more components may lead to CAFs, which may have catastrophic consequences on the system function.

Another way of classifying CAFs stems from the idea that the components are susceptible to some dependencies. From the definitions listed in Table 2, it is found that the dependencies associated with CAFs are different. Therefore, CAFs are distinguished into three types considering the dependence links: functional, hazardous event, and load-sharing. In this thesis, we focus mainly on the first two categories of CAFs.

- Functional CAFs refer to those failures that propagate between components whose functions are dependent on neighbors. For example, the state of a node depends on the state of others, which implies that a failing node will cause its neighbors to fail. This functional dependency between components could be not only direct but also indirect.
- Hazardous event CAFs correspond to hazardous events, like fire, explosion, and disease. The failures propagate within a cluster of components. The primary scenario may escalate their effect to other components, triggering one or several secondary failures spatially or temporally. Damage of hazards may be dependent on the distance between the components.
- Load-sharing CAFs are related to the flow or load in interdependent networks, like power grids, transportation networks, and traffic flow. When an overloaded node fails, the flow or load will choose an alternative path to other nodes, resulting in a redistribution of the load in the system and thereby causing the neighbors to fail.

Table 2 Definition and classifications of CAFs

Authors	Definition	Classification	Ref.
Genserik Reniers & Valerio Cozzani	An accident in which a primary unwanted event propagates within the equipment or/and to nearby equipment, sequentially or simultaneously, triggering one or more secondary unwanted events, in turn possibly triggering other unwanted events, resulting in overall consequences more severe than those of the primary event.	Hazardous event	[49]
Rausand & Øien	Cascading failures are multiple failures initiated by the failure of one component in the system that results in a chain reaction or domino effect	Hazardous event	[50]
Motter & Lai	Any failure leads to a new redistribution of loads. As a result, subsequent failures can occur. This systematic process is what we call a cascading failure.	Load-sharing	[51]
Rausand & Høyland	When several components share a common load, failure of one component may lead to increased load on the remaining components and consequently to an increased likelihood of failure	Load-sharing	[12]
Buldyrev et al.	In interdependent networks, when nodes in one network fail, they cause dependent nodes in another network to fail, which may happen recursively and lead to a cascade of failures.	Functional	[5]

Cozzani et al.	Accidental sequences have three common features: (1) a primary accidental scenario, which initiates the domino sequence; (2) propagation of the primary event, due to “an escalation vector ” generated by physical effects of the primary scenario, that results in the damage of at least one secondary equipment item; (3) one or more secondary events.	Hazardous event	[52]
Lees	An event at one unit that causes a further event at another unit	Functional	[53]
Baldick et al.	A sequence of dependent failure of individual components that successively weakens the power system	Functional	[54]
Watts & Ren	The cascade model has N identical components with random initial loads within the load limits. Components fail when their load exceeds a certain threshold. When a component fails, a fixed load is transferred to the other components, leading to a cascade of failures.	Load-sharing cascading	[55]

In sum, CCFs highlight a direct cause-effect relationship, whereas cascading failures involve the interactions or dependencies between the components. The differences between CAFs and CCFs have been discussed in [3], which is one of the objectives of this thesis.

2.2.3 Modeling dependent failures

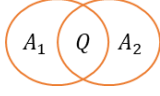
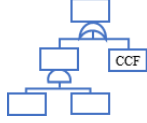
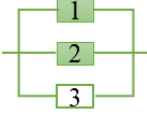
A wide range of models has been developed to study the mechanism and analyze dependent failures during the last 20 years. These models aim to include the effects of dependent failures in reliability analysis, but they are not always suitable approaches for the reliability analysis of complex systems. Moreover, it is difficult to model the dependent failures and incorporate them as basis events [17].

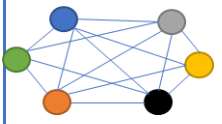
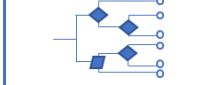
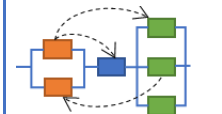
The models for CCFs can be broadly classified as direct estimate models (e.g., square root model [56]), ratio estimate models (e.g., C-factor model and β -factor model [12, 57]), and shock models (e.g., binomial failure rate model [58]). These models have been incorporated into the traditional reliability analysis approaches, such as fault tree analysis [59, 60], Markov methods [61], and Bayesian networks [62].

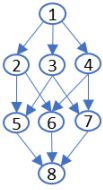
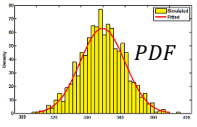
The models applied for CAFs differ from the ones for CCFs. They can be categorized as topological (e.g., complex network models [51, 63] and graph theory models [64, 65]), probabilistic (e.g., risk analysis models [66, 67] and reliability analysis models [37, 68]), state-transition (e.g., Markov processes[69], Petri nets[70], and Bayesian networks [66, 71]), and simulations (e.g., Monto Carlo simulations [72, 73]). These models focus on either the mechanism and behavior of CAFs or the effects of CAFs [9]. The effects of CAFs can also be considered from the component-level (e.g., [74, 75]), system-level (e.g., [21, 68, 76]), or their combinations (e.g., [77]).

A comparison of the models for two failures were performed based on the classifications above. Table 3 summarizes the illustrations, advantages, and disadvantages. In this Ph.D. work, the main focuses lie on the reliability analysis models considering CCFs and CAFs.

Table 3 A comparison of the models for CCFs and CAFs

Type	Category	Model	Basics	Pros	Cons
CCF	Direct estimate models	Square root model	 $q_L = P(A_1)P(A_2)$ $q_U = \min\{P(A_1), P(A_2)\}$ $Q = \sqrt{q_L q_U}$ <p> $P(A_i)$: unavailability of component i Q : unavailability of the system </p>	<ul style="list-style-type: none"> Can easily obtain the geometric mean value 	<ul style="list-style-type: none"> Cannot consider various degrees of coupling between components
	Ratio estimate models	C-factor model, β -factor model	 $\beta = \frac{\lambda^{(c)}}{\lambda}$ <p> β: common cause factor $\lambda^{(c)}$: failure rates for common causes λ: failure rates </p>	<ul style="list-style-type: none"> Can incorporate fault tree analysis, Markov models. Factor checklist can be used. 	<ul style="list-style-type: none"> Can not allow a certain fraction of the components to fail Slight conservative results
	Shock models	binomial failure rate model	 $\lambda = \lambda^{(i)} + pv$ <p> λ: failure rates $\lambda^{(i)}$: failure rates for independent failure p : failure probability due to shocks v: occurrence rate of shocks </p>	<ul style="list-style-type: none"> The components can fail independently of each other 	<ul style="list-style-type: none"> Rather complicated, difficult to define a fraction of the shocks p.

CAF	Topological models	Complex network models, graph theory models	 $P(k) = k^{-r}$ <p>k: the connection to other nodes $P(k)$: the fraction of nodes</p>	<ul style="list-style-type: none"> • Can incorporate topological features • Can incorporate network graph models and network reliability analysis 	<ul style="list-style-type: none"> • Limited capability in modeling dependent and dynamic behaviors • Limited capability in modeling repair and maintenance
	Probabilistic models	Risk analysis models, Reliability analysis models, Bayesian networks	 $\lambda = \lambda_0 P(A)P(B)P(C)$ <p>λ : end consequence frequency λ_0 : initiating event frequency $P(A)$: conditional probability of events</p>  $R_S = \sum P(F_i) \cdot P_r$ <p>R_S : system reliability $P(F_i)$: failure probability of component i P_r : cascading probability</p>	<ul style="list-style-type: none"> • Computation efficient • Can apply for some specific types of the distributions 	<ul style="list-style-type: none"> • Inefficient for large-sized systems • Limited capability in modeling repair and maintenance

State-transition	Markov models, Petri nets,	 $F = 1 - \sum P(i)$ <p>F : failure probability of the system $P(i)$: the probability of steady states</p>	<ul style="list-style-type: none"> • Flexible • Can incorporate repair and maintenance 	<ul style="list-style-type: none"> • Inefficient for large-sized systems • Limited to exponential distribution
Simulations	Monte Carlo simulations	 <p>PDF : probability density function</p>	<ul style="list-style-type: none"> • Flexible • Can apply for large-size systems 	<ul style="list-style-type: none"> • Time-consuming • Mistakes or statistical errors may be made during estimation

2.3 Safety barrier

In most technical systems, protective measures or equipment are employed to prevent or mitigate the effects of failures and protect people, the environment, and other assets. These measures or equipment can be called safety barriers. In this section, we will summarize the theories concerning safety barriers.

2.3.1 Concept of safety barrier

Although there is no universal definition of a safety barrier, they are regarded as those physical or non-physical means planned to prevent, control, or mitigate undesired events or accidents [13]. Safety barriers are also called countermeasures, defenses, layers of protection, and safeguards in the literature [2]. The basic idea of safety barriers is that the barriers are a means to avoid losses by separating or protecting vulnerable assets from hazards. In the ARAMIS project report, safety barriers are related to how to implement safety functions that can be divided into “to avoid”, “to prevent”, “to control”, and “to limit, reduce, or mitigate” [78]. Using electric, electronic, and programmable electronic technologies, SISs are regarded as specific safety barriers [14].

The concept of a safety barrier is often used in risk analysis [79]. Risk analysis is related to the probability of something going wrong, the negative consequences if it does, and the frequency of the accidents. First, one must identify the possible hazards and estimate their impacts and likelihood in the risk analysis. Then, to avoid risk, protection layers or safety barriers are added to reduce the probability and frequency of accidents and mitigate negative consequences.

In IEC 61508 [14], it is recommended to use a functional safety lifecycle to control risk. The safety lifecycle is composed of 16 steps in analysis, realization, and operation phases. The analysis phase of the lifecycle deals with identifying and specifying the safety needs for the system. Notably, in the step of overall safety requirement allocation, it is required to decide

whether SISs are needed as safety barriers and, if so, to determine the required safety integrity levels (SILs). SISs are not the only means to protect EUC from accidents. Protections may be provided by other safety barriers as well as SISs. As illustrated in Figure 2, the initial risk is defined concerning EUC and specific scenarios. The acceptable risk is a tolerable criterion, meaning that risk should be required to enter an as low as reasonably practicable (ALARP) level. The difference between EUC and acceptable risk is the necessary risk reduction that SISs or other safety barriers should allocate.

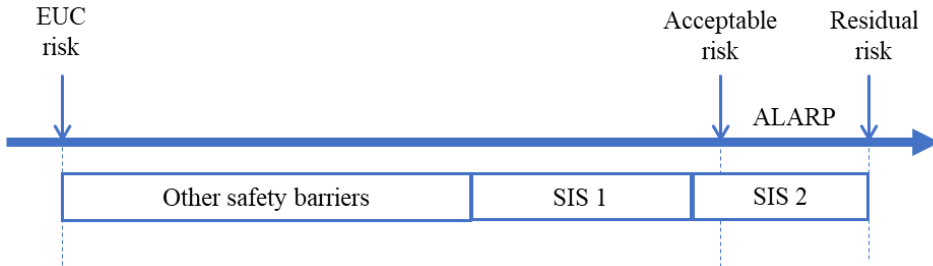


Figure 2 The risk reduction process [14]

2.3.2 Classification of safety barriers

Safety barriers can be classified in different ways. One acknowledged classification based on the bow-tie model distinguishes proactive barriers from reactive barriers [2]. Proactive barriers are applied for preventing or reducing the probability of a hazardous event, whereas reactive barriers are employed to avoid or reduce the relevant consequences. Furthermore, safety barriers can be classified as physical, technical, operational, and organizational barriers [19]. In addition, Kjellen [80] proposed two categories of barriers: add-on barriers and inherent design barriers. Apart from them, Sklet [13] provided a systematic classification of safety barriers in the literature, as shown in Figure 3.

Barrier functions are related to the functions planned to prevent, control, or mitigate accidents, which are realized by barrier systems. Generally, the barrier systems are divided into two groups: passive and active. Technical barriers can further be broken down to SIS, safety-related systems, and external risk reductions among active barriers. In this dissertation, we emphasize those technical barriers that are defined as add-on barriers. Such barriers are added to the systems or components due to safety considerations. For example, SISs are typical add-on technical barriers concerning safety issues.

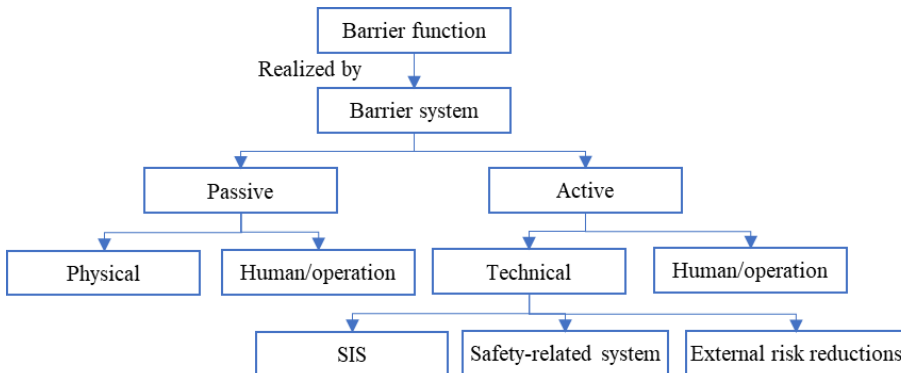


Figure 3 Classification of safety barrier [13]

2.3.3 Barrier performance

Performance assessment of safety barriers is necessary since it reflects how well safety barrier perform their functions. Scholars have proposed different performance measures to assess safety barriers. For example, Sklet [13] recommended some attributes to assess safety barriers: effectiveness, reliability (availability), response time, robustness, and triggering event. Johansen and Rausand [18] highlighted that the requirements for safety barriers include specificity, functionality, reliability, response time, capacity, durability, robustness, auditability, and independence. Rausand [1] also stated that a barrier's confidence level should be evaluated based on the following criteria: specificity, adequacy, independence, dependability, robustness, and audibility. Prashanth et al. [81] identified 17 types of variables to evaluate the performance of safety barriers.

However, not all proposed attributes or criteria are relevant for some types of barriers. Therefore, this dissertation's performance of safety barriers is delimited to the functionality/effectiveness, reliability/availability, and durability. The effectiveness is linked to the ability of a safety barrier to prevent accidents or achieve proper function [19]. For example, a safety barrier is installed to reduce a specific risk with hazardous event frequency, λ_H . The hazardous event frequency is reduced at λ_E using the safety barrier, as shown in Figure 4. A measure, the risk reduction factor (RRF), is introduced to define the effectiveness of the safety barrier:

$$RRF = \frac{\lambda_H}{\lambda_E} \quad (1)$$

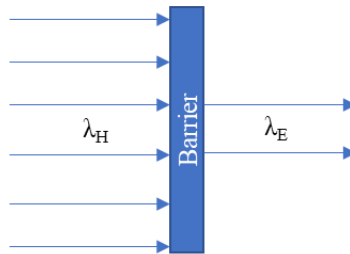


Figure 4 The risk reduction of a safety barrier [1]

Safety barriers can be classified as perfect barriers and imperfect barriers considering their performances. Perfect barriers are the barriers that can be activated if needed and prevent accidents completely once installed, which implies that RRF should be equal to infinity. However, in most cases, safety barriers are not perfectly effective and fully functional. It means that some failures may occur on safety barriers, such as response failures when needed and operational failures to stop its functions. Therefore, they can be called imperfect barriers. The purpose of such classification is to distinguish the effects of failures on safety barriers. Furthermore, imperfect barriers may also be concerned with dependent failures, namely CCFs and CAFs. That means, in some cases, it is required to consider the effects of CCFs and CAFs on imperfect barriers.

Availability (reliability) of barriers depends not only on the inherent reliability of equipment acting as barriers but also on operational and maintenance strategies. Availability expresses the ability of a safety barrier to perform its required functions at a specific time [12]. For example, IEC 61508 defines the average probability on demand of an SIS to describe the performance of an SIS [14]. The event upon which an SIS is activated is considered a demand [1]. The difference between effectiveness and availability is that effectiveness deals with how much a

barrier is expected to reduce risk, whereas availability measures how well the barrier can affect response to the demand for its safety function.

Durability is another performance measure, representing how long a safety barrier can perform its safety functions and withstand demand in this context. It is often assumed that demands are instantaneous, but this is not always the case [1]. For example, fires can last a few seconds or several days, depending on many factors. An automatic fire extinguishing system, thus, must operate for a specified period to suppress fires. Another example is an emergency shutdown valve. It must also withstand stress for an uncertain period to prevent the spread of flammable substances. Such a period is defined as a prolonged demand duration. Thus, durability is related to safety barrier performance during prolonged demands.

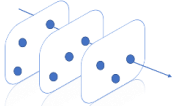

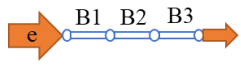
2.3.4 Barrier analysis

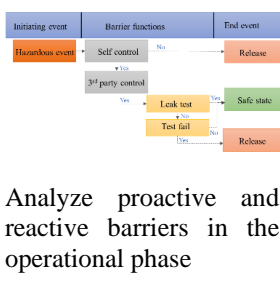
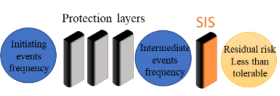
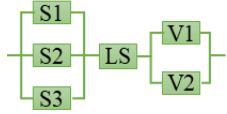
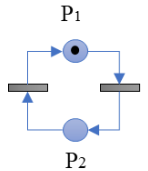
A barrier analysis aims to identify administrative, management, and physical barrier that can prevent or minimize the probability and severity of an accident [2]. Evaluating safety barriers depends on an analysis to explain why accidents occur and understand how they can be prevented. A barrier analysis is applied for preventing accidents by having proper barriers in the right place.

Numerous qualitative and quantitative models have been proposed for barrier analysis. Qualitative models for barrier analysis include hazard barrier matrices, safety barrier diagrams, Swiss cheese model, bow-tie diagram, and energy flow/barrier analysis. Quantitative models for barrier analysis include probabilistic models (e.g., event tree analysis (ETA), fault tree analysis (FTA), and reliability block diagram (RBD)) and state-transition models (e.g., Markov model, Bayesian network, and Petri net). In addition, some so-called semi-quantitative barrier models combine qualitative and quantitative analysis, such as layers of protection analysis (LOPA) and barrier and operational risk analysis (BORA), to identify risk scenarios and determine possible barriers. A comparison of these models is listed in Table 4.

Table 4 A comparison of some models for barrier analysis

Type	Models	Basics	Pros	Cons	Ref
Qualitative	Hazard barrier matrix	<p>Barrier effectiveness ■ ■ ■ ■ Most effective → Least effective</p>	<ul style="list-style-type: none"> • Simple qualitative method • Provide a degree of completeness in the identification of hazards and barriers 	<ul style="list-style-type: none"> • Limited ability to rank quantitative efficiency and effectiveness of the barriers 	[2, 82]
	Safety barrier diagram	<p>Barriers are activated on demands</p>	<ul style="list-style-type: none"> • Better for communication with non-expert • Easily illustrate the sequence and causal of accident scenario 	<ul style="list-style-type: none"> • The simplification could lead to loss of information 	[83, 84]

			<ul style="list-style-type: none"> • Logical AND/OR gates can be used in the diagram • Dependency of the barriers can be represented in the diagram 		
Swiss cheese model	 <p>Failures penetrate a series of safety barriers and lead to accidents</p>	<ul style="list-style-type: none"> • Easy to visualize the notion of the accidents • Draws upon a general, easy to remember, and adaptable graphical representation 	<ul style="list-style-type: none"> • A simplistic vision of accidents • The limited degree of generality 	[85-87]	
Bow-tie diagram	 <p>A bow-tie model is commonly used to depict the relationships between hazardous events, causes and consequences, and the barriers</p>	<ul style="list-style-type: none"> • Simple to read and understand • Structured in a division between proactive and reactive barriers • Suitable for risk management • It can be used together with fault tree and event tree 	<ul style="list-style-type: none"> • Require depth knowledge regarding systems • Barriers in the model should be independent 	[78, 88, 89]	
Energy flow/barrier analysis	 <p>Identify all possible paths from energy sources to vulnerable assets and barriers</p>	<ul style="list-style-type: none"> • Simple to understand and use • Systematic and easily recognized • Suitable in combination with other methods 	<ul style="list-style-type: none"> • Difficult to identify all the energy sources • Poor at identifying all hazards • Poor on reproducibility 	[90, 91]	

Semi-quantitative	BORA	 <p>Analyze proactive and reactive barriers in the operational phase</p>	<ul style="list-style-type: none"> • It can be used to determine the installation of specific risk • Contribute to a better understanding of the safety barrier • It gives a better insight into the risk influencing factors 	<ul style="list-style-type: none"> • Requires access to extensive data • Determine importance and weights of risk influence factors without proper justification 	[92, 93]
	LOPA	 <p>Decide whether existing safety barriers are adequate or if additional barriers are needed</p>	<ul style="list-style-type: none"> • Focus on the most critical protection layers • Reveal process safety issues • Requires less time and fewer resources • Can comply with IEC 61511 	<ul style="list-style-type: none"> • Excessive for simple or low-risk decisions • Overly simplistic for complex systems • Requires risk tolerance criteria 	[2, 79, 94]
Quantitative	Probabilistic models	 <p>Fault tree analysis, Event tree analysis, Reliability block diagram Bayesian network</p>	<ul style="list-style-type: none"> • Computationally efficient • With random variables and probability distributions 	<ul style="list-style-type: none"> • Inefficient for very large-sized systems 	[4, 95-97]
	State-transition models	 <p>Markov model, Petri net, Monte Carlo simulations</p>	<ul style="list-style-type: none"> • Flexible • Suitable for stochastic process 	<ul style="list-style-type: none"> • Inefficient for large-sized systems 	[98-100]

2.4 Safety instrumented system

As a safety barrier, a safety instrumented system is frequently deployed to reduce risk in many industries, such as oil and gas, energy, and railway industries. An SIS is characterized as a system that relies on electrical/electronic/programmable electronic technologies to detect abnormal situations.

2.4.1 The basic concept of SIS

An SIS generally consists of three main subsystems: sensors (e.g., level transmitters, gas detectors, and push buttons), logic solvers (e.g., programmable logic controller and industrial computer), and final elements (e.g., shutdown valves and circuit breakers). As showed in Figure 5, when a sensor detects possible abnormal situations, a signal is sent to the logic solver. Then, an instruction for the action of the final element is created as a response to the detected abnormal situation. Finally, a final element performs safety-instrumented functions (SIFs) according to the inputs.

A SIF refers to a function intended to achieve or maintain a safe state for the EUC against hazardous events [14]. An SIS can perform one or more SIFs, and a facility can be equipped with several SISs. For example, a process shutdown (PSD) system stops production if the process is upset. Meanwhile, an emergency shutdown (ESD) system can also be installed to reduce the escalation of uncontrolled events such as leakages by depressurizing and removing electrical ignition sources.

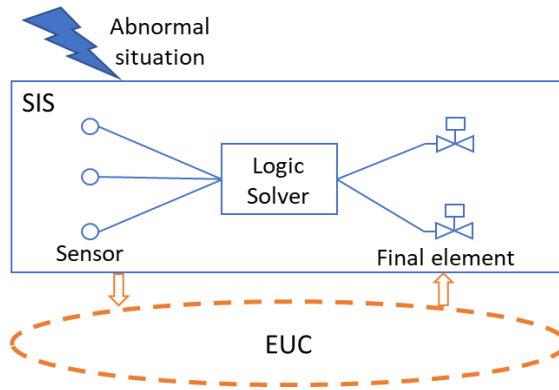


Figure 5 A general configuration of an SIS and EUC

2.4.2 SIS operation and failures

An SIS is often a passive barrier that is activated only when demand occurs. The demand is also called a process upset or process deviation [15]. According to the demand rates, SISs can be distinguished as low-demand and high-/continuous demand modes [14]:

- Low-demand mode. A safety barrier operates in low-demand mode when its function is demanded no more than once per year.
- High-/continuous-demand mode. A safety barrier is said to operate in high-/continuous-demand mode when it is demanded more often than once per year, or its function is continuously required.

Some safety barriers that operate in low-demand mode include an ESD, fire and gas detection in a process plant and an airbag system in an automobile. Safety barriers that operate in high-/continuous-demand mode can be dynamic positioning systems for ships, signaling systems for railways, and anti-lock braking systems in an automobile. Liu and Rausand have discussed the effects of distinctive demand modes for reliability analysis in the studies [101].

The reason to distinguish operational modes for SISs is that they have different performance measures due to different kinds of failures. A failure is defined as the termination of the ability of an item to perform a required function [102]. Failures of an SIS can be classified according

to numerous criteria, such as systematic and random hardware failures, critical, degraded, and incipient failures. In this thesis, we employ the classification based on the consequence and detectability according to IEC 61508. It splits the failures of SISs into four groups: dangerous detected (DD), dangerous undetected (DU), safe detected (SD), and safe undetected (SU) failures, as shown in Figure 6 [14]. DD failures are dangerous failures that are detected immediately by diagnostic testings when they occur. DU failures are dangerous failures that prevent activation on demand and are revealed only by testing or the occurrence of a demand.

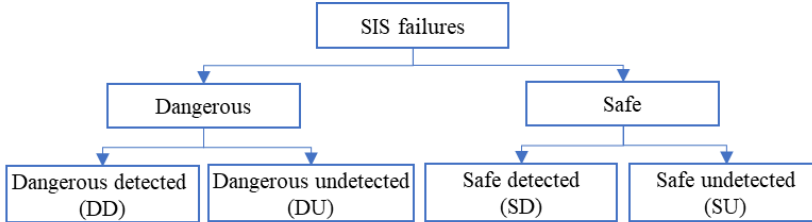


Figure 6 A often used classification of SIS failures [14]

Both DD and DU failures are dangerous failures that are critical for the functionality of the equipment. The difference between DD and DU failures lies in how the two types of failures are revealed. DU failures are latent and only occasionally revealed upon demands, periodic testings, or inspections, while automatic diagnostics reveal DD failures once they occur. Since DU failures cannot be detected immediately and cannot be fixed until the periodic testing, these failures contribute the most to the unavailability of SIS equipment.

It is noted that, for the low-demand mode of SISs, a demand may occur while a DU failure is present. As illustrated in Figure 7, for a single component, a DU failure may occur before a proof testing. There is a chance that demand occurs before a DU failure is revealed and corrected such that a hazardous event happens. Hence, DU failures are of concern in most reliability studies for the low-demand mode operating SISs.

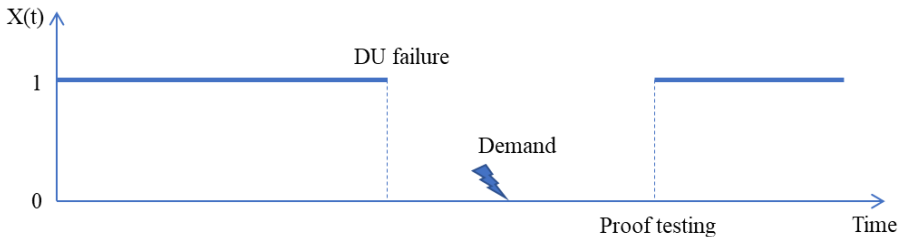


Figure 7 A demand may occur while a DU failure is present in low-demand systems [1]

Apart from failures, the concept of failure rate is also crucial for the reliability analysis of SISs. A failure rate is defined as the average failure frequency, i.e., a few failures per unit of time [103]:

$$\lambda = \frac{\text{Mean number of failures in a time interval of length } t}{t} \quad (2)$$

Failure rates can be used to reflect how SISs perform their SIFs in a specific period. Failure rates are generally classified into three groups, generic, manufacturer-provided, and user-provided failure rates, depending on how they have been derived [1]. In the oil and gas industry, generic failure rates for SIS equipment performing SIFs are presented in databases and

handbooks, such as Offshore and Onshore Reliability Data (OREDA) [104], Safety Equipment Reliability (EXDIA) [105], and Reliability Data for Safety Instrumented Systems (PDS) [106]. Databases of OREDA rely on the failures reported from multiple operating companies, while the PDS data handbook relies on a combination of data from OREDA, expert judgment, and manufacturer information. Generic failure rates are mainly applied in reliability analysis during the design phase. Manufacturer-provided data are, meanwhile, based on analyses of specific products and laboratory testing. User-provided failure rates are based on aggregated time in service and the number of reported failures at one or more specific facilities owned by the same operating company. It is often seen that manufacturer-provided failure rates are lower than what is experienced in operation.

The standards and regulations have given specific requirements concerning the failure rates. For example, IEC 61508 states that the failure rate used in a reliability analysis should have a confidence level of at least 70% [14]. Furthermore, the uncertainty of the estimated failure rates is required to be considered in OREDA, e.g., a 90% confidence level [104]. In addition, SINTEF suggests that operational time should exceed $3 \cdot 10^6$ hours, allowing it to use operational experience [107]. Therefore, many oil and gas facilities invest time and resources to record failures to estimate failure rates in this context.

Failure rates may be affected by the influencing factors. Influencing factors are the internal and external parts of a system that act on its reliability or failures. The term influencing factor is more general than failures cause, and it relates to the indirect explanatory factors, for example, equipment attributes (e.g., sizes and types), operational environment (e.g., temperature, pressure, and loads), manufacturing activities (e.g., manufacturers and procedures), facility (e.g., location), maintenance (e.g., test interval), and the activities of the end-user.

2.4.3 SIS performance measures

Performance measures of SISs are mainly linked to functionality/effectiveness and reliability/availability [19]. Functionality/effectiveness refers to the ability of an SIS to perform a specified function with a specific requirement and given conditions [13]. For example, a shutdown valve has a specific response time to be activated, reflecting the SIS's effectiveness. Reliability/availability refers to the ability of SISs to perform the required SIFs within a period [12]. This Ph.D. thesis focuses on the reliability measures involving SIS design, operation, maintenance, and testing. Several quantitative measures can be used for the reliability of an SIS, including the average probability of failure on demands (PFD_{avg}) for low-demand modes and the average frequency of dangerous failure (PFH) for high-demand modes.

SISs are a kind of system whose SIFs are only activated upon abnormal situations. Since SISs are not running in the low-demand operational mode, many DU failures cannot be detected immediately after their occurrences. Periodical proof testing, such as once per year, are conducted in many process plants to reveal DU failures of SISs but with noticeable delays. Performance assessment of SISs operated in low-demand modes thus needs specific measures, such as PFD_{avg} . PFD_{avg} is the most used reliability measure for an SIS. It is defined as the average probability that a component (i.e., SIS, subsystem, voted group, or channel) cannot perform its specified safety function if demand should occur. PFD_{avg} can also be interpreted as a mean proportion of time of which the item cannot perform its specified SIF in a certain period [14]:

$$PFD_{avg} = \frac{1}{\tau} \int_0^{\tau} PFD(t) dt \quad (3)$$

where $PFD(t)$ is the probability of failure on demand as a function of time. τ is a test interval. PFD_{avg} is related to the internal properties and the frequency of proof testing. These

particularities distinguish SISs from production or general systems and impede the adaption of the existing approaches for CAF analysis to SISs. If a component can be as good as new after each proof test, the long-term average PFD(t) is equal to the average of PFD(t) over a test interval [1].

In contrast, PFH is used as a reliability measure for SISs operated in high/continuous-demand mode. PFH at time t is defined as:

$$PFH(t) = \omega_D(t) = \lim_{\Delta t \rightarrow 0} \frac{\Pr [Dangerous failures in (t, t + \Delta t)]}{\Delta t} \quad (4)$$

where $\omega_D(t)$ is the frequency of item failures in the time interval $(t, t + \Delta t)$. IEC 61508 requires the average PFH to be used for SISs operated in high/continuous-demand modes, but it does not specify the time interval at which the average should be determined [14]. Hence, the average PFH in the time interval (t_1, t_2) is defined as:

$$PFH(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \omega_D(t) dt \quad (5)$$

An SIS's reliability requirement describes the safety integrity requirement, starting with how well the SIS is required to perform. The requirement is often assigned to each SIF. SIFs must fulfill the specified safety integrity levels (SILs) to achieve the necessary risk reduction. Safety integrity is the probability of an SIS satisfactorily performing the required SIFs under all the stated conditions within a specific period [1]. For example, in IEC 61508 and IEC 61511 [14, 15], four discrete SILs are defined, as shown in Table 5, ranging the safety integrity from SIL 1 (the lowest level) to SIL4 (the highest level).

Table 5 Intervals of the PFD_{avg} and PFH corresponding to the SILs

SILs	Low demand mode	High/continuous demand mode
4	$10^{-5} \leq \text{PFD} < 10^{-4}$	$10^{-9} \leq \text{PFH} < 10^{-8}$
3	$10^{-4} \leq \text{PFD} < 10^{-3}$	$10^{-8} \leq \text{PFH} < 10^{-7}$
2	$10^{-3} \leq \text{PFD} < 10^{-2}$	$10^{-7} \leq \text{PFH} < 10^{-6}$
1	$10^{-2} \leq \text{PFD} < 10^{-1}$	$10^{-6} \leq \text{PFH} < 10^{-5}$

In operations, SIS performance is of great significance to ensure the safety of EUC systems. Hence, it is of interest to examine whether an SIS is reliable while responding and how an SIS performs after activation. The former is related to SIS reliability, whereas the latter is related to SIS durability. SIS reliability expresses the ability of an SIS to protect EUC systems at a specific time and is related to the ability to respond on-demand as expected. SIS durability represents how long an SIS can perform its SIFs and withstand stress during prolonged demands. SISs are often exposed to high stress during prolonged demand, resulting in intensive degradations and failures before complete demand. Therefore, it is vital to examine whether a safety barrier is reliable and performs during demand.

2.4.4 SISs considering dependent failures

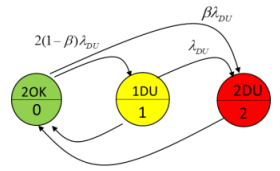
Although independence is a critical requirement for SISs, they are rarely fully independent and often subject to CCFs and CAFs [18]. The effects of CCFs in SISs have been widely studied because CCFs commonly occur in SISs with redundant structures [6]. Redundancy is a means to enhance system reliability, but meanwhile, it often leads to CCFs due to the same components, environment, or shocks in redundant structures. CCFs may reduce the effects of redundancy. It is noteworthy that CCFs are the main contributors to the unavailability of SISs [107, 108].

There have been two main strategies suggested for incorporating defenses against CCFs in design. One is to carry out analyses to identify and remove causes, and the other is to introduce measures to reduce the effects of CCFs in case they occur. The suggested approaches include cause-defense matrices, common cause analysis, and zonal analysis. The defenses to CCFs are typically identified in design. However, measures in the operational phase are also necessary [6]. Even for an excellent system design, there will always remain a risk of CCFs. It is, therefore, required to include the contribution of CCFs in quantitative analyses used to demonstrate adequate reliability.

The reliability measures, PFD_{avg} and PFH, can be calculated based on several methods: simplified formulas based on fault tree analysis, IEC 61508 formulas, PDS method, and Markov methods [1]. The effects of CCFs can be modeled and incorporated with these methods. Simplified formulas are the most time-efficient method to obtain reliability measures. However, CCFs are assumed to occur on all the redundant components simultaneously. The different effects of various voting configurations are considered in the PDS method by introducing a modification factor. IEC 61508 may give the most conservative results since the effects of DU and DD failures are considered, but this method is challenging to be understood and explained. Furthermore, Markov methods can include dynamic and multiple states of SISs, but the analysis is a time-consuming process. A comparison of these methods is listed in Table 6 that also shows their strength and weakness.

Table 6 A comparison of some models for SISs considering CCFs

Models	Basics	Pros	Cons	Ref.
Simplified formulas	$PFD_{avg} = PFD_{avg}^{(i)} + \frac{\beta\lambda_{DU}\tau}{2}$ <p>where, β: beta factor for CCFs λ_{DU}: DU failure rates τ: test interval</p>	<ul style="list-style-type: none"> • Simple method • Time-efficient • Easy to be understood 	<ul style="list-style-type: none"> • Not consider different voting configurations • CCFs are assumed to occur simultaneously 	[1, 109]
PDS method	$PFD_{avg} = PFD_{avg}^{(i)} + C_{koon} \frac{\beta\lambda_{DU}\tau}{2}$ <p>where, C_{koon}: modification factor for CCFs</p>	<ul style="list-style-type: none"> • The effects of various voting configurations are considered • Easily obtain the result 	<ul style="list-style-type: none"> • The simplification could lead to loss of information 	[107]
IEC 61508 formulas	$PFD_{avg}^{(G)} = \lambda_{D,G}t_{GE}$ <p>where, $\lambda_{D,G}$: the group failure frequency of dangerous failures, t_{GE}: the group-equivalent mean downtime</p>	<ul style="list-style-type: none"> • Provides conservative results • Can consider both DD and DU failures 	<ul style="list-style-type: none"> • It is difficult to be understood and explained the parameters in the model 	[14, 109, 110]

<p>Markov models</p>	 <p>where, State 0: two components are functioning State 1: one DU failure State 2: two DU failures, and the system is down</p>	<ul style="list-style-type: none"> • Can include dynamic and multiple states of SISs • Can consider both DD and DU failures 	<ul style="list-style-type: none"> • Time-consuming • The model complexity increases along with an increasing number of states 	<p>[111, 112]</p>
----------------------	---	---	--	-------------------

SISs may also be vulnerable to CAFs originating from the reliance on shared loads, testing and maintenance resources, hazardous events, and dependent functions [22]. For example, several components are configured in parallel in a flow transmission system sharing maintenance resources. The failure of one component may occupy the maintenance resource, decrease the possibilities of maintenances on other components, and then trigger more failures. Another example is a fire water supply system where the pumps operate in a K-out-of-N (*KooN*) configuration. When one of the pumps fails, the corresponding pipeline is closed, and other pumps must carry the whole load. The probabilities of failures-to-start of the other pumps thus increase.

CCFs are the first-in-line failures and are directly linked to the failure causes, while the propagation of CAFs follows a series of interactions. Thus, CCFs and CAFs are two types of distinctive failures. Therefore, models for assessing the performance of SISs with CCFs are not applicable for SISs with CAFs [23].

However, it seems that the most attention has been directed to CCFs. The effects of CAFs, in specific, for safety barriers are seldom explored. The current models in the literature for reliability analysis are insufficient to evaluate the overall effects of CAFs in terms of safety barriers. Hence, there is a lack of studies on the approaches and models for providing precise and holistic performance analysis of safety barriers.

2.5 Summary

To summarize, the theories reveal the basic concepts, causes, and various models for dependent failures and safety barriers in complex systems. As Tugnoli et al. pointed out, when the inherent design is not enough, safety barriers are necessary to eliminate dependent failures, such as CCFs and CAFs [113]. Both failures can coincide and influence multiple components, leading to devastating consequences. Therefore, the two kinds of failures should be equally paid attention to in the reliability analysis of safety barriers. Nevertheless, the effects CAFs among components within safety barriers have not been well studied.

This page is intentionally left blank

Chapter 3

3 Research questions and objectives

The theoretical background review in Chapter 2 reveals that dependent failures are crucial and have received increasing interest in recent years. The focus is mainly on CCFs in safety barriers. Nevertheless, in many cases, CAFs can also have a significant impact on system reliability. This chapter highlights the specific research questions to fulfill this gap and proposes the objectives of the Ph.D. project.

3.1 Research questions

The specific challenges and questions in this thesis have been identified. They are mainly related to complex systems, dependent failures, and safety barriers.

3.1.1 Dependency issues

As mentioned in Section 2.1, a complex system is challenging to describe and predict due to complexity. Moreover, with the increasing complexity of technical systems, some dependency issues arise, such as dependent failures and dependence between the system and environment.

Research gap: Definition of dependent failure categories

Dependent failures can be a significant concern in complex systems. They can coincide on multiple components quickly, resulting in devastating consequences and damages. For example, CCFs are the main contributors to failures in the safety systems of the oil and gas industry. CAFs may also propagate within the same sub-structure and between different sub-structures in a complex system. Such propagation brings multiple possibilities of CAFs in complex systems and challenges the current analysis approaches.

Although many researchers have studied CCFs and CAFs, there is little comparison between the two concepts. Indeed, one can differentiate CAFs from CCFs, covering failure causes, mechanisms, and characters. Moreover, the models that are applied to CCFs are not suitable to handle CAFs. Accordingly, safety barrier strategies to avoid or reduce the effects of the two failure categories should also be distinctive. It is thus interesting to investigate the similarities and differences between CCFs and CAFs and propose relevant barrier strategies to prevent the two failures.

Research gap: Modeling dependencies between systems and the environment

Furthermore, in a complex system, the dependency issues may also include the fact that many influencing factors directly or indirectly impact the system's performance. For example, the items within a group are assumed to have similar functions and the same performance. Nevertheless, similar components can experience different failure rates and distributions since their design (e.g., measuring principle), location, and environment can differ. For example, a review of failure data collected from six oil and gas facilities in Norway indicates that one failure mode, fail to open, is strongly affected by the temperature of the medium in the valves. The term "significant influencing factors" is thus introduced for those with the most substantial effects on performance. The significant influencing factors may include equipment attributes, the operational environment, manufacturing, maintenance, and activities.

However, it is still a question of which influencing factors are the most significant influences and how to identify them to explain the differences. Most traditional statistical models rely on data for a large group of equipment. The influencing factors can be analyzed using traditional statistical models; however, data-driven approaches could also be suitable. Therefore, it is required to address how to model dependencies between systems and the environment based on data-driven models.

Therefore, there is a need for a study on the dependency issues in complex systems:

Q1: How to distinguish between CCFs and CAFs in terms of concept, causes, mechanisms, and consequences? How to prevent and mitigate the effects of CAFs? What kind of considerations can be made to handle CAFs?

Q2: How to identify influencing factors for system performance? How to model the identified influencing factors and dependent failures between components in system performance analysis?

3.1.2 Safety barriers

In a complex system, safety barriers are vital since they can avoid accidents by protecting vulnerable assets from hazards. However, the safety functions of safety barriers are impacted by dependency issues. Such impacts stem from dependent failures, which can be different, including the effects of dependent failures within safety barriers and the effects of dependent failures when safety barriers are employed to prevent them.

Research gap: Modeling dependent failures within safety barriers

Redundancy of safety barriers is often applied in a complex system to enhance the ability to detect and respond to hazardous events. However, redundancy increases the fault tolerance and remains vulnerable to dependent failures. Therefore, reliability analysis of safety barriers involves the impact of dependent failures, including both CCFs and CAFs.

IEC 61508 and the relevant literature primarily focus on CCFs as dependent failures. However, SISs can also be vulnerable to CAFs. For example, several components are configured in parallel in a flow transmission system sharing maintenance resources. The failure of one component may occupy the maintenance resource, decrease the possibilities of maintenance on other components, and then trigger more failures. Another example is a fire water supply system where the pumps are operating in a $KooN$ configuration. When one of the pumps fails, the corresponding pipeline is closed, and other pumps must carry the whole load. The probabilities of failures-to-start of the other pumps thereby increase. Unfortunately, the used approaches mainly focus on CCFs, and the performance assessment of SISs subject to CAFs is seldom explored.

Since SISs are not always running in the low-demand operational mode and only be activated upon abnormal situations, many failures cannot be detected immediately after their occurrences. Therefore, periodical proof testing, such as once per year, are conducted in many process plants to reveal hidden failures of SISs but with noticeable delays. Performance assessment of SISs thus needs specific measures, such as PFD_{avg} for low demand modes and PFH for high/continuous demand modes. They are not only related to the internal properties of an SIS but also related to the frequency and effectiveness of proof testing. These particularities distinguish SISs from production or general systems and impede the adaption of the existing approaches for CAF analysis to SISs. Therefore, it is required to introduce approaches and models for incorporating CAFs into the performance assessment of SISs operating in low demand modes and high/continuous modes.

Research gap: Modeling safety barriers against dependent failures

Safety barriers like SISs are often installed in many industries for dependent failures, namely CCFs and CAFs, to alleviate the effects of shared failures and suspend failure propagation. However, little attention has been paid to the impacts of SISs employed to prevent cascading failures in the literature. In addition, the currently defined SIS reliability is insufficient to evaluate the overall SIS performance in preventing and mitigating CAFs. That is because the demands on SISs for preventing or mitigating CAFs may not be instantaneous. Thus, even though an SIS can respond to demands, it may fail afterward. For example, fires can last few seconds or several days, and AFESs must operate for a specified period to suppress fires. During this period, SISs are often exposed to high stress and thereby have more chances to fail. In other words, SISs that are employed against CAFs may suffer from intensive degradations and failure before demands are complete.

Therefore, it is of interest to examine whether an SIS is reliable while responding and how an SIS performs after activation. The former is related to SIS reliability, whereas the latter is related to SIS durability. The reliability is the ability to respond on-demand as expected, expressed by the failure probability on demand, PFD_{avg} . Nevertheless, durability represents how long an SIS can perform its SIFs. It lacks studies and relevant models. Furthermore, it is challenging to use straightforward approaches to evaluate SISs against CAFs considering reliability and durability. Hence, the models involving SISs to prevent against CAFs should be tailor-made.

Relevant questions regarding safety barriers suffering from CAFs include:

Q3: How to quantify the effects of CAFs within safety barriers and how to reduce or mitigate their impacts? How to evaluate the effects of CAFs within SISs operating in low demand modes and high/continuous modes?

Q4: What type of reliability modeling and calculation approaches are suitable for safety barriers that are employed to prevent against CAFs? How to apply the models and approaches to practical cases?

3.2 Research objectives

The primary objective of this thesis has been to improve the understanding of dependent failures in complex systems and model safety barriers with dependent failures, with a particular focus on the effects of cascading failures.

Based on the main objective and research questions, the specific objectives have been to:

Objective 1: Discuss the differences and similarities between CCFs and CAFs and distinguish safety barrier strategies to protect against or mitigate the effects of dependent failures, particularly for CAFs.

Objective 2: Propose approaches and models for evaluating the impacts of dependency issues in complex systems and investigate their effects.

Objective 3: Propose approaches and models for evaluating the impacts of CAFs in safety barriers, including SISs operating in high-demand and low-demand modes.

Objective 4: Provide new insights for SISs that are employed to prevent CAFs and propose models for evaluating the performance of such SISs and illustrate their applications.

The relationships between the research questions, research objectives, and research gaps are presented in Figure 8. Four specific objectives have been formulated considering the research questions regarding dependency issues and safety barriers in complex systems.

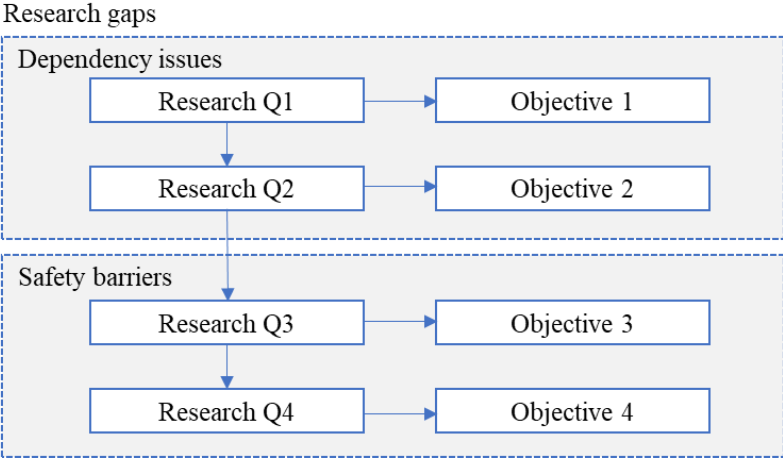


Figure 8 Relationships between research questions and research objectives

Chapter 4

4 Research principles and approaches

The rationale for pursuing this Ph.D. degree has been to acquire new knowledge and develop research skills by formulating research problems, preparing research plans, writing scientific articles, and presenting research results. The overall research process and principles, as well as research approaches, are outlined in this chapter.

4.1 Research principles

It is often the case that research makes one feel like swimming in the sea and not knowing which direction to turn [114]. Thus, the first and fundamental question for doing research is understanding what is meant by "research". Research is defined as a process of steps used to collect and analyze information to increase our understanding of a topic or issue [115]. Thus, research is finding out something one does not know. In other words, research is studying a particular topic to discover more information or reach a new understanding.

There are several dimensions to classifying research based on their applications, purposes, and methods. Traditionally, research can be classified into basic research and applied research [116, 117]. The former is theoretical or experimental work to acquire new knowledge of foundations of phenomena and observable facts, while the latter emphasizes application or practical use.

A threefold classification of research was also proposed by Phillips and Push based on research purposes, namely exploratory, testing-out, and problem-solving [118]. Exploratory research is related to studying a new problem with little knowledge and providing new insights by developing or using existing methodologies. Testing-out research is to find the limits of previously proposed generalizations and improving them. The third kind of research focuses on a particular problem in the real world and discovers solutions.

Another dimension of classification of research is related to research approaches. Research can generally be quantitative, qualitative, and a combination of the two. Quantitative research emphasizes qualification in the collection and analysis of data, whereas qualitative research emphasizes words [119].

This project should be classified as applied research since it focuses on studying the behaviors and performance of safety barriers in a complex system. As to the project's purpose, the research needs to clarify theories and concepts and develop new models for analyzing safety barriers with dependent failures in complex systems. Therefore, research is both exploratory and problem-solving. In addition, the research approaches in this project involve qualitative and quantitative research. Qualitative research in this project provides new insight into safety barriers and develops relevant theoretical models and concepts. In contrast, quantitative research is conducted to develop new models for analyzing the effects of safety barriers based on existing approaches.

4.2 Research approach

High-quality research requires systematic design and planning. A research project should answer initial questions, develop or propose new approaches, and highlight their application

areas. It may include identifying the research context and perspective, discussing research problems, identifying main assumptions, describing theoretical basis, and presenting new approaches and applications.

Generally, this Ph.D. project includes three main phases: (1) research plan, (2) theoretical study, (3) model development, and (4) research results. The Ph.D. project process and how they related to the research results are illustrated in Figure 9:

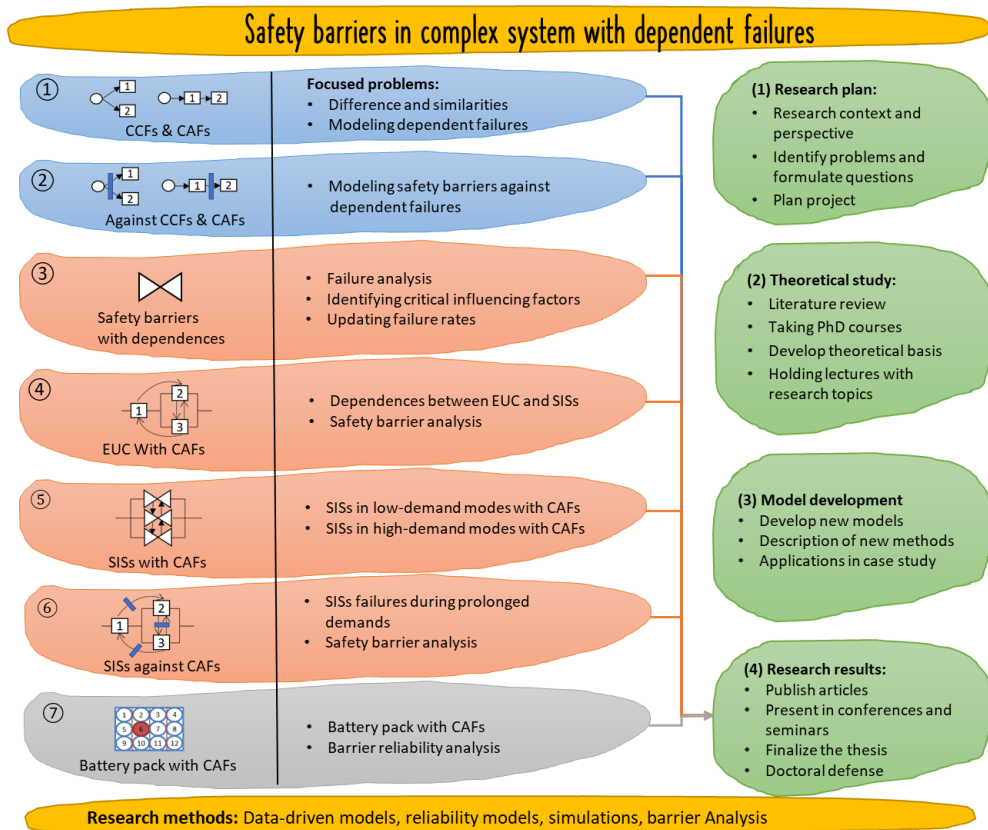


Figure 9 Overall process of the Ph.D. research project

- (1) Research plan. The project started with identifying the research context and perspectives, relating the initial research gaps, and formulating research problems and questions. Then, the activity continued with making a research plan that includes project descriptions, formulation of research questions, and research execution plan. The details of the research execution plan are presented in Table 7.
- (2) Theoretical research. The activities in this stage started with a systematic literature review, which is a fundamental task. The review is based on research material available in the NTNU database Oria, covering articles published in journals, conference papers, reports, and books. The Ph.D. courses guided conducting the research and generating a solid theoretical basis for the project, especially for achieving objective 1. Therefore, the courses related to the safety-critical system, applied statistics, system engineering, multivariate data modeling, and research methodology were undertaken during the Ph.D. period. Then, two articles that focused on the theory of dependent failures and

barriers against the failures were written for developing a theoretical basis at this stage. I was also involved in assisting and holding lectures on relevant areas, which was a way to improve the understanding of fundamental issues within safety barriers and reliability research.

- (3) Approaches and model development. One crucial part of this Ph.D. project was developing analysis approaches and models based on previous works and existing literature. Model-based and data-driven-based approaches were considered in the project. New approaches and models were developed, depending on the collected data and formulated assumptions. In addition, applications of these models and approaches were considered in a specific industry or application area, such as the battery industry. A case regarding a battery pack with CAFs and relevant safety barriers was studied.
- (4) Research results. Research results should be presented, including the developed models and approaches, discussion about constraints, suggestions for new perspectives, and new ideas for future work. The preliminary results of this project have been presented in conferences and seminars such as ESREL and IEEM. Participating in conferences and seminars allows one to open their eyes and learn the vision of new ideas in the field. The project results have also been presented to the academic world through international journals and conference proceedings. The last step of the Ph.D. project is to summarize the findings and contributions in the thesis and prepare for doctoral defense.

Table 7 Research execution plan for the PhD project

Year	2017		2018		2019		2021	
Semester: (S=Spring, F=Fall)	F	S	F	S	F	S	F	
PhD Courses								
IFEL8000 - Introduction to research methodology								
TK8116 - Multivariate data and Metamodeling								
PK8210 - System engineering								
BA8618 - Applied statistics in civil and transport								
PK8201 - System reliability								
Research process								
Research plan								
Theory study								
Model development								
Research results								
Research publications								
Conference articles								
Journal articles								
Thesis and defense								

An essential part of the quality assurance was carried out by publication in international journals and conferences. In addition, the publications have been subject to extensive peer review and have been revised based on the reviewer's suggestions and comments.

This page is intentionally left blank

Chapter 5

5 Main results

This chapter presents and describes the main results of this Ph.D. project that are documented in the form of eight articles. The purpose is to evaluate to what extent the research objectives have been met.

5.1 Overview

The research articles aim to address the research questions that have been identified in Chapter 3. Four articles were published in relevant international journals, and one is currently under review. In addition, another three articles have been presented in peer-reviewed international conferences and have been published in conference proceedings.

The overview of the contributions and relevant research objectives are listed in Table 8. There are two articles related to each research objective. Article I and II focus on the performance of complex systems with dependency issues. Articles VI and VII have highlighted the theoretical basis of CCFs and CAFs and modeled the two categories of failures. The effects of CAFs involve two levels, CAFs within safety barriers and CAFs prevented by safety barriers, which have been investigated in Articles III, VIII, VI, and V.

Table 8 Overview of the contributions and relevant objectives

Contribution	Research objective	Article	Main topic
1	Objective 1	Article I Article II	Theoretical basis and models studies regarding CCFs and CAFs
2	Objective 2	Article III Article IV	The performance analysis with dependency issues
3	Objective 3	Article V Article VI	The effects of CAFs within safety barriers
4	Objective 4	Article VII Article VIII	The effects of safety barriers against CAFs

5.2 Main contributions

5.2.1 Contribution 1

The first objective of this Ph.D. project was to compare two types of dependent failures and distinguish different safety barriers strategies to protect against or mitigate the failure effects. The two articles are related to this objective:

Article I: Common cause failure and cascading failures in technical systems: similarities, differences, and barriers.

Article II: Safety barriers against common cause failure and cascading failure: literature reviews and modeling strategies.

1. Article I investigated the similarities and differences of these two dependent failures, focusing on the conditions of initiations and propagation of such failures. This exploration facilitates one to understand the initiations, consequences, and mitigations of the failures.
2. Article II explored the functions of safety barriers against dependent failures based on extended bow-tie models. As illustrated in Figure 10, barrier B1 for CCFs separates all the components from root causes or coupling factors, whereas barrier B2 for CAFs prevents failure propagation from hazardous event 1.

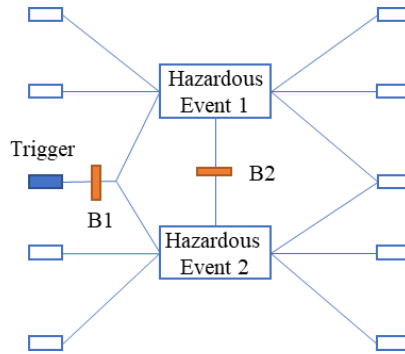


Figure 10 Safety barriers for CCFs and CAFs in extended bow-tie model

The main findings are summarized as follows:

1. By comparing the two failures, the articles have highlighted that CCFs are the "first-in-line" failures and are directly linked to the failure causes, whereas the propagation of CAFs depends on a series of interactions, as illustrated in Figure 11. In other words, CCFs are characterized by the simultaneous failures of two or more components due to a shared cause, while cascading failures reflect the multiple failures initiated by one component's failure that led to a chain reaction or a domino effect.

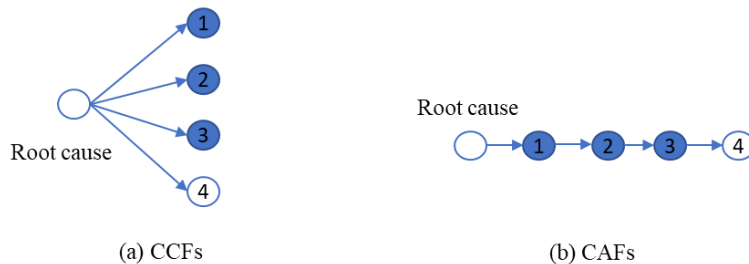


Figure 11 Illustration of the similarities and differences between CCFs and CAFs

2. Article II clarified distinctive safety barrier strategies against dependent failures and provided new insights into the barriers for reducing and mitigating the effects of dependent failures. It is required to distinguish the safety barriers against CCFs and those against CAFs. The bow-tie model is extended to illustrate the difference between these two kinds of safety barriers. Table 9 lists some examples of safety barriers that are applied for preventing CCFs and CAFs. This paper provided empirical evidence for root cause analysis for the two failures.

Table 9 Examples of safety barriers against CCF and CAF

Failure	Effect	Description	Safety barrier	Category
FTO ^a PSVs ^b	Root cause	The heating cable in the pilot line is disconnected due to a short circuit	Implement regular quality check of heating cable	B1
	Coupling factor	Same design from one supplier	Replacing the existing cables with the ones from another company	B1
Fire	Root cause	The cable is overheating due to a short circuit, which leads to the fire and explosion	Redesign and regular check	B2
	Coupling factor	Fire and explosion propagating	Firewall to prevent fire explosion	B2

^a FTO: fail to open; ^b PSV: pressure safety valves;

5.2.2 Contribution 2

The first research question is related to the dependency issues in complex systems. Quantifying the effects of these dependency issues, like the influencing factors and dependent failures between the components in a complex system, is thus the first focus of the Ph.D. project. The contributions include a framework based on data-driven approaches for identifying critical influencing factors and an approach for analyzing the impacts of CAFs on the reliability in series-parallel complex systems. These contributions are related to two articles:

Article III: Operational data-driven prediction for failure rates of equipment in SISs: A case study from the oil and gas industry

Article IV: Reliability and barrier assessment of series-parallel systems subject to cascading failures

1. Article III demonstrated the application of the proposed framework for identifying influencing factors. The main reason to investigate the effects of influencing factors is that similar types of equipment may experience different failure rates. Therefore, it is necessary to identify critical influencing factors and predict failure rates based on the reported failures. Consequently, Article I illustrated a case study with the data collected from six Norwegian onshore and offshore oil and gas facilities. As illustrated in Figure 12, the framework consists of three main steps: 1) data collection, including a selection of equipment, collection, and pre-processing data; 2) identification of significant influencing factors to find hidden correlations; and 3) failure rate prediction by determining the weights and scores of the factors.

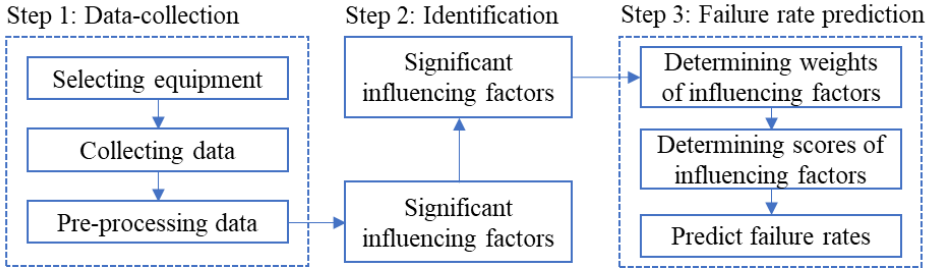


Figure 12 Framework for identifying critical influences and predicting failure rates

- Article IV presented a recursive aggregation approach based on the extended reliability block diagram models for analyzing the impacts of CAFs on the reliability of series-parallel complex systems. The fundamental idea for modeling CAFs is introducing a measure $\gamma_{ij}(t) \in [0,1]$ to denote the ease of failure propagation, as illustrated in Figure 13. It was defined as:

$$\gamma_{ij}(t) = \Pr(C_j \text{ fails} | C_i \text{ has failed by time } t) \quad (5)$$

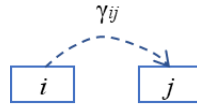


Figure 13 RBD with a CAF between component i and j

Two articles handle dependency issues in complex systems. The main findings can be found in the articles:

- The framework combines data-driven models and statistical models for predicting failure rates. It helps us identify the most significant factors on failure rates and decide the weights and scores of identified factors.
- The proposed approach to investigate the effects of CAFs can help one obtain holistic system reliability and decide the efficient way to allocate safety barriers to reduce and mitigate the consequence of CAFs.

5.2.3 Contribution 3

The third objective concerns how to quantify the effects of CAFs within safety barriers and how to reduce or mitigate their impacts. The two articles are related to this objective:

Article V: Performance assessment of $KooN$ SISs subject to cascading failures

Article VI: Performance Assessment of SISs Systems Subject to CAFs in High-demand Mode

- Article V proposed a recursive aggregation-based approach for analyzing $KooN$ SISs operating in low-demand modes considering CAFs. Based on the approach, the approximation formulas for performance assessment of most common configuration SISs have been summarized.
- Article VI proposed approximation formulas for the average frequency of dangerous failures of SISs operating in high/continuous-demand modes subject to CAFs. This article is an extension of Article V, where the focus was directed to low-demand mode systems.

The main contributions of these articles are summarized as follows:

1. Simplified formulas for PFD_{avg} considering CAFs are presented in Table 10. A general approximation based on these formulas were developed in different configurations of SISs considering CAFs.

$$\text{PFD}_{\text{avg}}^{(KooN)} = \binom{N-1}{K-1} N \gamma^{N-K} \frac{\lambda \tau}{2} \quad (6)$$

where λ denotes a failure rate of the component of SISs, γ denotes a measure of CAF propagation, and τ is a test interval.

Table 10 Approximation formulas for PFD_{avg} with CAFs after simplification

K/N	N=1	N=2	N=3	N=4
K=1	$\lambda \tau / 2$	$2\gamma \cdot \lambda \tau / 2$	$3\gamma^2 \cdot \lambda \tau / 2$	$4\gamma^3 \cdot \lambda \tau / 2$
K=2	-	$\lambda \tau$	$6\gamma \cdot \lambda \tau / 2$	$12\gamma^2 \cdot \lambda \tau / 2$
K=3	-	-	$3\lambda \tau / 2$	$12\gamma \cdot \lambda \tau / 2$
K=4	-	-	-	$2\lambda \tau$

A factor $\sigma_{KooN} = \binom{N-1}{K-1} N \gamma^{N-K}$ was introduced to distinguish the effects of CAFs on the value of PFD_{avg} among various configurations. The value of factors were also compared to those for CCFs, as illustrated in Figure 11. Again, the value for CAFs is higher than that of CCFs.

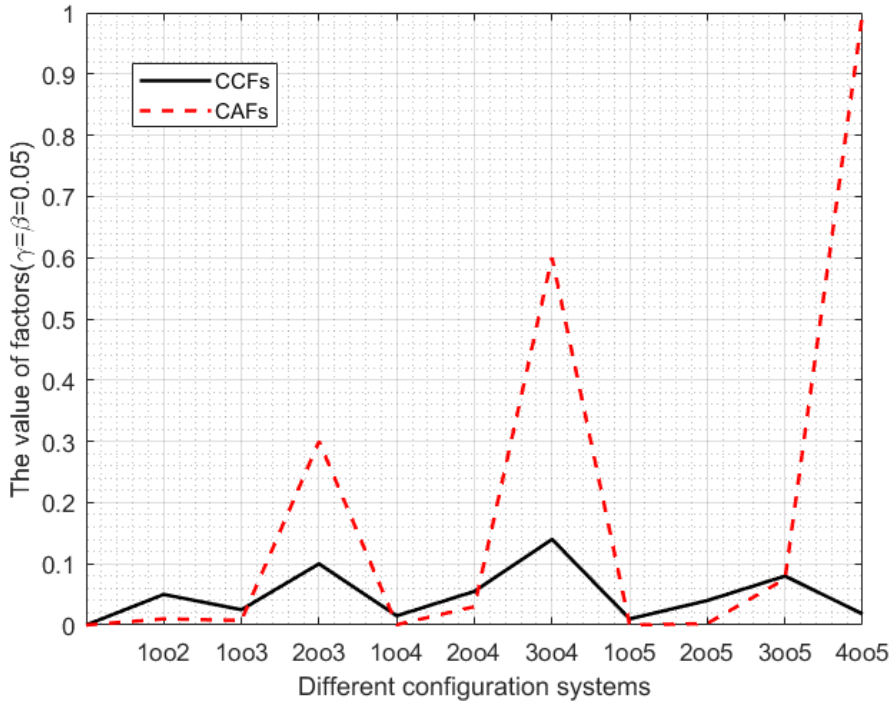


Figure 14 Comparison of the factors for CCFs and CAFs

2. Approximation formulas have been derived for PFH of SISs in high/continuous modes that are subject to CAFs, as illustrated in Table 11. λ_{DU} is a DU failure rate of the component of SISs, γ denotes a measure of CAF propagation, and τ is a test interval. The proposed formulas can be applied to other industrial systems that are susceptible to cascading failures. The article was also demonstrated that the contribution of CAFs towards PFH relies on the CAFs and may lead to unacceptable SIL.

Table 11 PFH of various structures with CAFs

System	PFH
1oo2	$\lambda_{DU}^2 \tau + 2 \lambda_{DU} \gamma$
1oo3	$\lambda_{DU}^3 \tau^2 + 6 \lambda_{DU}^2 \tau \gamma + 3 \lambda_{DU} \gamma^2$
2oo3	$3 \lambda_{DU}^2 \tau + 6 \lambda_{DU} \gamma$
1oo4	$\lambda_{DU}^4 \tau^3 + 12 \lambda_{DU}^3 \tau^2 \gamma + 12 \lambda_{DU}^2 \tau \gamma^2 + 4 \lambda_{DU} \gamma^3$
2oo4	$4 \lambda_{DU}^3 \tau^2 + 24 \lambda_{DU}^2 \tau \gamma + 12 \lambda_{DU} \gamma^2$
3oo4	$6 \lambda_{DU}^2 \tau + 12 \lambda_{DU} \gamma$

5.2.4 Contribution 4

The last objective addresses the problem of how SISs are employed to prevent CAFs. Unlike the previous ones focused on CAFs within safety barriers, these research questions are associated with safety barriers used to prevent CAFs. Therefore, the two articles are relevant:

Article VII: Performance analysis of SISs protecting against cascading failure during prolonged demand

Article VIII: Performance analysis of safety barriers against cascading failures in a battery pack.

1. Article VII proposed an approach for analyzing how the performance of SISs influences the protection against and mitigation of CAFs. In addition, it considers SIS reliability and SIS durability in the mitigation of CAFs if demands on SIS are prolonged.
2. Article VIII investigated the effects of CAFs in a specific application area regarding batteries. It studied battery reliability and analyzed the effects of safety barriers against CAFs from a modeling battery pack perspective

The main contributions of these articles are summarized as follows:

1. Article VII developed a new approach to model SISs against CAFs and evaluated their effectiveness. The approach considered the failures of SISs in responding and after activation; thus, it analyzed SIS reliability and durability in performance analysis. The proposed approach can provide designers and operators with information for SIS design and deployment, thereby improving the safety and reliability of the EUC system.
2. It was demonstrated that, in some cases, it was reasonable to pay more attention to the effects of failure during demand when considering the high stress from CAFs, as illustrated in Figure 15.

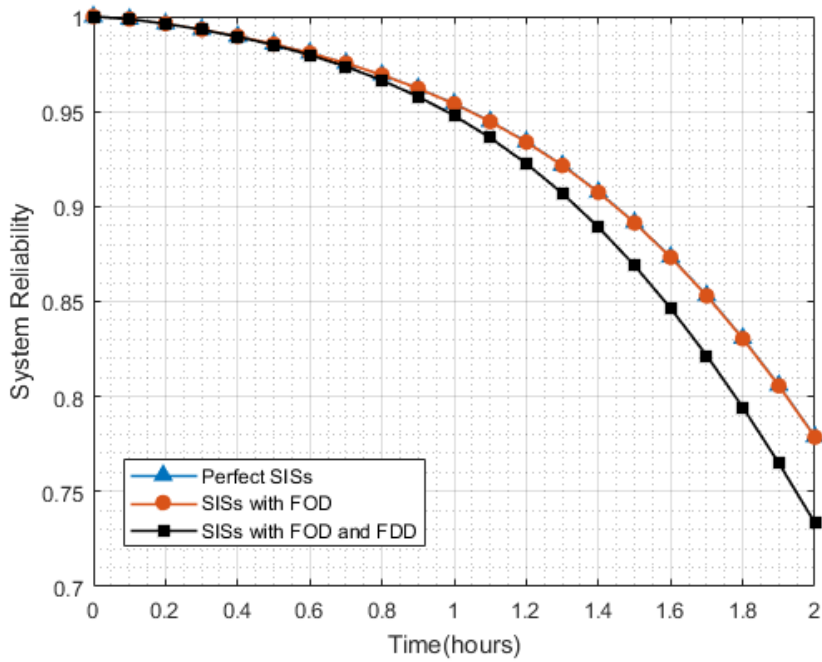


Figure 15 System reliability profiles for different states of SISs

That means the effects of failure during demand (FDD) are relatively higher than failures on demand (FOD) on the system reliability.

3. The proposed models for evaluating the performance of safety barriers against CAFs illustrated in their applications with a practical case study in the battery industry in Article VIII.

This page is intentionally left blank

Chapter 6

6 Conclusions and future work

This chapter highlights the main contributions of the Ph.D. works. Because the research regarding safety barriers with dependent failures is still under-explored, this chapter also presents several open research problems and opportunities for the future.

6.1 Conclusions

The overall objective of this Ph.D. thesis was to explore a new approach for analyzing safety barriers with dependent failure in complex systems, with a particular focus on the effects of CAFs. This objective was decomposed into four sub-objectives addressed through the eight articles in Part II of the thesis. Four articles investigated dependent failures, while four aimed to model the effects of safety barriers considering CAFs.

The contributions of individual objectives have been elaborated in Chapter 5. Here, it emphasized that the contributions fulfilled the objectives and are summarized as follows:

1. A clarification of the differences and similarities between CCFs and CAFs was explored. Meanwhile, safety barrier strategies to protect against the dependent failures have been discussed and clarified. This research may increase the awareness, competence, and treatment of CAFs. It is expected that defense against CAFs can be considered in design as well as in operations.
2. A new framework for identifying significant influencing factors was proposed, presenting new ideas and insights to update failure rates in performance analysis of safety barriers. In addition, the models for evaluating the effects of CAFs in complex systems have been investigated and developed. Although the framework and models need further development, the contributions fulfill the intent of the objective.
3. Models and formulas for evaluating the performance of safety barriers considering the impacts of CAFs were proposed and developed. Traditionally, CCFs in safety barriers have been a significant contributor to system unavailability and have been intensively studied. However, little attention has been paid to the effects of CAFs within safety barriers, particularly for SISs operating in high- and low-demand modes. A special challenge is related to modeling dependencies that are within or between components of SISs. The contributions of this Ph.D. project represented new perspectives and approaches to deal with CAFs within or between SISs.
4. While safety barriers prevent CAFs during prolonged demands, models for evaluating their performance are desirable. The project addressed this question and considered the EUC reliabilities and SIS durability during demand. They allow one to provide guidelines for a cost-efficient mitigation plan for a given resource situation and limited budget.

In conclusion, this Ph.D. thesis contributed to recognizing the effects of safety barriers with dependent failures in complex systems, promoting systematic and holistic approaches to evaluate the performance of the systems. The benefits of the proposed approaches and models in this thesis were as follows: 1) providing precise and holistic performance analysis of safety barriers, and 2) offering the guidelines for SIS or barrier design and deployment to improve the performance of complex systems.

The thesis applied the proposed models and approaches to SISs and safety barriers in the oil and gas industry, but they can also be adapted to other sectors, such as the energy and railway fields. The proposed models have been employed in SISs and EUC systems, but they can also be generalized to other industrial complex systems with dependent failures.

6.2 Future work

This section gives open questions and recommendations for further research concerning complex systems, maintenance, approaches and models, and verification.

6.2.1 Complex system

Complex systems discussed in this thesis mainly focus on systems comprising many components and are associated with interactions and dependency issues, like numerous influences or dependent failures. However, as mentioned in Chapter 1, complex systems can be various and more complicated. Therefore, efforts can be made to find more numerical solutions for complex systems, e.g., network systems, hierarchical systems, and dynamic systems. The effects of CAFs in these complex systems can thus be different, which can be interesting research questions.

6.2.2 Maintenance issues

The thesis is dedicated to the performance analysis and reliability analysis of safety barriers. The work can be extended to testing and maintenance issues as they are vital activities to ensure that safety barriers achieve and maintain the desired performance. The activities may include several factors but may not be limited to repair time, proof testing, response time for SIF, inspection intervals, testing coverage, testing schedules, and maintenance strategies. Involving these activities impacts the models for analyzing the performance of safety barriers. Therefore, it is necessary to improve the models and approaches for analyzing safety barriers considering maintenance activities.

6.2.3 Approaches and models

The adequate models and approaches are determined by the simplification and assumptions that are made. Simplification of the reality in the models raises uncertainty of the approaches. The approaches and models in this Ph.D. work still need future development, and their numerical efficiency must also be improved. Some assumptions in the models are somewhat restrictive. For example, the statistical dependency between CAFs, e.g., time-dependent, or jointing cascading probability, has not been considered in the analysis. Additionally, performance indicators, such as response time, capacity, and robustness, can also be included in the models.

6.2.4 Implementation

Monto Carlo simulations have verified the approaches and models proposed in this Ph.D. project. However, it is also required to accumulate and develop available cascading failure data to verify the models. High-quality data are then essential for accurate modeling reliability and performance analysis. The models have been applied to a specific industry in the battery cascading cases, but more efforts should be encouraged, and the models should be expanded to various applications.

Reference

- [1] Rausand M. "Reliability of safety-critical systems: theory and applications." Hoboken, New Jersey, USA, John Wiley & Sons,2014.
- [2] Rausand M, Haugen S. "Risk assessment: theory, methods, and applications," John Wiley & Sons,2020.
- [3] Xie L, Lundteigen MA, Liu Y. "Common cause failures and cascading failures in technical systems: Similarities, differences and barriers," In: European Safety and Reliability Conference, Trondheim, Norway, pp.2401-2407, June 17-21.2018.
- [4] Landucci G, Argenti F, Spadoni G, Cozzani V. "Domino effect frequency assessment: The role of safety barriers," Journal of Loss Prevention in the Process Industries, vol. 44, pp. 706-717, 2016.
- [5] Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, pp. 1025-1028, 2010.
- [6] Lundteigen MA, Rausand M. "Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing," Journal of Loss Prevention in the process industries, vol. 20, pp. 218-229, 2007.
- [7] Haes Alhelou H, Hamedani-Golshan ME, Njenda TC, Siano P. "A survey on power system blackout and cascading events: Research motivations and challenges," Energies, vol. 12, pp. 682, 2019.
- [8] Liao W, Salinas S, Li M, Li P, Loparo KA. "Cascading failure attacks in the power system: A stochastic game perspective," IEEE Internet of Things Journal, vol. 4, pp. 2247-2259, 2017.
- [9] Xing L. "Cascading failures in internet of things: review and perspectives on reliability and resilience," IEEE Internet of Things Journal, vol. 8, pp. 44-64, 2020.
- [10] Ouyang M. "Review on modeling and simulation of interdependent critical infrastructure systems," Reliability engineering & System safety, vol. 121, pp. 43-60, 2014.
- [11] Shuang Q, Zhang M, Yuan Y. "Node vulnerability of water distribution networks under cascading failures," Reliability Engineering & System Safety, vol. 124, pp. 132-141, 2014.
- [12] Rausand M, Høyland A. "System reliability theory: models, statistical methods, and applications."2nd. Hoboken, New Jersey, USA, John Wiley & Sons,2004.
- [13] Sklet S. "Safety barriers: Definition, classification, and performance," Journal of loss prevention in the process industries, vol. 19, pp. 494-506, 2006.
- [14] IEC61508. "Functional safety of electrical/electronic/programmable electronic safety-related systems." Geneva. International Electrotechnical Commission, 2010.
- [15] IEC61511. "Functional safety-safety instrumented systems for the process industry sector." Geneva. International Electrotechnical Commission, 2016.
- [16] Xie L, Håbrekke S, Liu Y, Lundteigen MA. "Operational data-driven prediction for failure rates of equipment in safety instrumented systems: A case study from the oil and gas industry," Journal of Loss Prevention in the Process Industries, vol. 60, pp. 96-105, 2019.
- [17] Lundteigen MA. "Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation," 2009
- [18] Johansen IL, Rausand M. "Barrier management in the offshore oil and gas industry," Journal of Loss Prevention in the Process Industries, vol. 34, pp. 49-55, 2015.

- [19] Liu Y. "Safety barriers: Research advances and new thoughts on theory, engineering and management," *Journal of Loss Prevention in the Process Industries*, vol. pp. 104260, 2020.
- [20] Xie L, Lundteigen MA, Liu Y. "Safety barriers against common cause failure and cascading failure: literature reviews and modeling strategies," In: 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, pp.122-127, December 16-19.2018.
- [21] Xie L, Lundteigen MA, Liu Y. "Reliability and barrier assessment of series-parallel systems subject to cascading failures," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 234, pp. 455-469, 2020.
- [22] Xie L, Lundteigen MA, Liu Y. "Performance assessment of K-out-of-N safety instrumented systems subject to cascading failures," *ISA transactions*, vol. 118, pp.35-43.2021.
- [23] Xie L, Lundteigen MA, Liu Y, Kassa E, Zhu S. "Performance Assessment of Safety-instrumented Systems Subject to Cascading Failures in High-demand Mode," In: *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*. 22–26 September 2019 Hannover, Germany, Hannover, Germany, September 22-26.2019.
- [24] Xie L, Lundteigen MA, Liu Y. "Performance analysis of safety instrumented systems against cascading failures during prolonged demands," *Reliability Engineering & System Safety*, vol. 216, pp. 107975, 2021.
- [25] Xie L, Ustolin F, Lundteigen MA, Li T, Liu Y. "Performance analysis of safety barriers against cascading failures in a battery pack," Submitted to *Reliability Engineering and Safety System*.
- [26] Perrow C. "Normal Accidents: Living with High-Risk Technologies." New York, Princeton University Press,1999.
- [27] Magee C, De Weck O. "An attempt at complex system classification."Massachusetts Institute of Technology Engineering Systems Division, 2002.
- [28] Magee C, De Weck O. "Complex system classification."International Council On Systems Engineering (INCOSE), 2004.
- [29] Sammarco JJ. "A normal accident theory-based complexity assessment methodology for safety-related embedded computer systems," West Virginia University,2003.
- [30] 14776-414 II. "Information technology -- Small Computer System Interface (SCSI) -- Part 414: SCSI Architecture Model-4 (SAM-4)." Geneva. International Organization for Standardization, 2009.
- [31] Nicolai RP, Dekker R. "Optimal maintenance of multi-component systems: a review," *Complex system maintenance handbook*, vol. pp. 263-286, 2008.
- [32] Keizer MCAO, Flapper SDP, Teunter RH. "Condition-based maintenance policies for systems with multiple dependent components: A review," *European Journal of Operational Research*, vol. 261, pp. 405-420, 2017.
- [33] Dao CD, Zuo MJ. "Selective maintenance of multi-state systems with structural dependence," *Reliability engineering & system safety*, vol. 159, pp. 184-195, 2017.
- [34] ISO26262. "Road vehicles Road vehicles — Functional safety." Switzerland. International Standard, 2018.
- [35] Murthy D, Nguyen D. "Study of two - component system with failure interaction," *Naval Research Logistics Quarterly* vol. 32, pp. 239-247, 1985.
- [36] Cozzani V, Gubinelli G, Antonioni G, Spadoni G, Zanelli S. "The assessment of risk caused by domino effect in quantitative area risk analysis," *Journal of hazardous Materials*, vol. 127, pp. 14-30, 2005.

- [37] Levitin G, Xing L. "Reliability and performance of multi-state systems with propagated failures having selective effect," *Reliability Engineering & System Safety*, vol. 95, pp. 655-661, 2010.
- [38] Hauge S, Hoem A, Hokstad P, Habrekke S, Lundteigen MA. "Common Cause Failures in Safety Instrumented Systems." SINTEF, 2015.
- [39] Liu B, Wu J, Xie M. "Cost analysis for multi-component system with failure interaction under renewing free-replacement warranty," *European Journal of Operational Research*, vol. 243, pp. 874-882, 2015.
- [40] Mosleh A, Parry G, Zikria A. "An approach to the analysis of common cause failure data for plant-specific application," *Nuclear Engineering and Design*, vol. 150, pp. 25-47, 1994.
- [41] NEA. "International Common Cause Failure Data Exchange (ICDE) General Coding Guidelines - Updated Version," 2012.
- [42] Paula HM, Campbell DJ, Rasmuson DM. "Qualitative cause-defense matrices: Engineering tools to support the analysis and prevention of common cause failures," *Reliability Engineering & System Safety*, vol. 34, pp. 389-415, 1991.
- [43] Daqing L, Yinan J, Rui K, Havlin S. "Spatial correlation analysis of cascading failures: congestions and blackouts," *Scientific reports*, vol. 4, pp. 1-6, 2014.
- [44] Timashev S. "Cyber reliability, resilience, and safety of physical infrastructures," In: *IOP Conference Series: Materials Science and Engineering*, pp.012009,2019.
- [45] Chen Y, Wen L, Ji C. "A cascading failure during the 24 May 2013 great Okhotsk deep earthquake," *Journal of Geophysical Research: Solid Earth*, vol. 119, pp. 3035-3049, 2014.
- [46] Zuccaro G, De Gregorio D, Leone MF. "Theoretical model for cascading effects analyses," *International journal of disaster risk reduction*, vol. 30, pp. 199-215, 2018.
- [47] McEvoy D, Ahmed I, Mullett J. "The impact of the 2009 heat wave on Melbourne's critical infrastructure," *Local environment*, vol. 17, pp. 783-796, 2012.
- [48] Said AO, Lee C, Stolarov SI, Marshall AW. "Comprehensive analysis of dynamics and hazards associated with cascading failure in 18650 lithium ion cell arrays," *Applied Energy*, vol. 248, pp. 415-428, 2019.
- [49] Reniers G, Cozzani V. "Domino effects in the process industries: modelling, prevention and managing," Newnes,2013.
- [50] Rausand M, Øien K. "The basic concepts of failure analysis," *Reliability Engineering & System Safety*, vol. 53, pp. 73-83, 1996.
- [51] Motter AE, Lai Y-C. "Cascade-based attacks on complex networks," *Physical Review*, vol. 66, pp. 065102, 2002.
- [52] Cozzani V, Gubinelli G, Salzano E. "Escalation thresholds in the assessment of domino accidental events," *Journal of hazardous materials*, vol. 129, pp. 1-21, 2006.
- [53] Lees F. "Lees' Loss prevention in the process industries: Hazard identification, assessment and control," Butterworth-Heinemann,2012.
- [54] Baldick R, Chowdhury B, Dobson I, Dong Z, Gou B, Hawkins D, et al. "Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures," In: *2008 IEEE Power and Energy Society General Meeting- Conversion and Delivery of Electrical Energy in the 21st Century*, pp.1-8,2008.
- [55] Watts D, Ren H. "Classification and discussion on methods for cascading failure analysis in transmission system," In: *2008 IEEE International Conference on Sustainable Energy Technologies*, pp.1200-1205,2008.
- [56] Edwards G, Watson I. "A study of common-mode failures." UKAEA Risley Nuclear Power Development Establishment, 1979.

- [57] Fleming KN. "Reliability model for common mode failures in redundant safety systems." General Atomics, 1974.
- [58] Vesely WE. "Estimating common cause failure probabilities in reliability and risk analysis: Marshall-Olkin specializations," In: Nuclear systems reliability engineering and risk assessment, ed. J.B.B. Fussell, G.R, pp.314-341,1977.
- [59] Vaurio JK. "Common cause failure probabilities in standby safety system fault tree analysis with testing—scheme and timing dependencies," Reliability Engineering & System Safety, vol. 79, pp. 43-57, 2003.
- [60] Kančev D, Čepin M. "A new method for explicit modelling of single failure event within different common cause failure groups," Reliability Engineering & System Safety, vol. 103, pp. 84-93, 2012.
- [61] Vaurio JK. "Uncertainties and quantification of common cause failure rates and probabilities for system analyses," Reliability Engineering & System Safety, vol. 90, pp. 186-195, 2005.
- [62] Mi J, Li Y-F, Peng W, Huang H-Z. "Reliability analysis of complex multi-state system with common cause failure based on evidential networks," Reliability Engineering & System Safety, vol. 174, pp. 71-81, 2018.
- [63] Albert R, Barabási A-L. "Statistical mechanics of complex networks," Reviews of modern physics, vol. 74, pp. 47-97, 2002.
- [64] Khakzad N, Landucci G, Reniers G. "Application of Graph Theory to Cost - Effective Fire Protection of Chemical Plants During Domino Effects," Risk analysis, vol. 37, pp. 1652-1667, 2017.
- [65] Khakzad N, Reniers G. "Using graph theory to analyze the vulnerability of process plants in the context of cascading effects," Reliability Engineering & System Safety, vol. 143, pp. 63-73, 2015.
- [66] Khakzad N, Khan F, Amyotte P, Cozzani V. "Risk management of domino effects considering dynamic consequence analysis," Risk Analysis, vol. 34, pp. 1128-1138, 2014.
- [67] Khan FI, Abbasi S. "Models for domino effect analysis in chemical process industries," Process Safety Progress, vol. 17, pp. 107-123, 1998.
- [68] Levitin G. "A universal generating function approach for the analysis of multi-state systems with dependent elements," Reliability Engineering & System Safety, vol. 84, pp. 285-292, 2004.
- [69] Iyer SM, Nakayama MK, Gerbessiotis AV. "A Markovian dependability model with cascading failures," IEEE Transactions on Computers, vol. 58, pp. 1238-1249, 2009.
- [70] Fricks RM, Trivedi KS. "Modeling failure dependencies in reliability analysis using stochastic petri nets," In: Proceedings of European Simulation Multiconference (ESM 97), Istanbul, Turkey, pp.355-368,1997.
- [71] Khakzad N, Khan F, Amyotte P, Cozzani V. "Domino effect analysis using Bayesian networks," Risk Analysis, vol. 33, pp. 292-306, 2013.
- [72] Abdolhamidzadeh B, Abbasi T, Rashtchian D, Abbasi SA. "A new method for assessing domino effect in chemical process industry," Journal of hazardous materials, vol. 182, pp. 416-426, 2010.
- [73] Abdolhamidzadeh B, Rashtchian D, Ashuri E. "A new methodology for frequency estimation of second or higher level domino accidents in chemical and petrochemical plants using monte carlo simulation," Iranian Journal of Chemistry and Chemical Engineering (IJCCE), vol. 28, pp. 21-28, 2009.
- [74] Chen X, Qiu J, Reedman L, Dong ZY. "A statistical risk assessment framework for distribution network resilience," IEEE Transactions on Power Systems, vol. 34, pp. 4773-4783, 2019.

- [75] Shunkun Y, Jiaquan Z, Dan L. "Prediction of cascading failures in spatial networks," *PloS one*, vol. 11, pp. e0153904, 2016.
- [76] Xing L, Levitin G. "Combinatorial analysis of systems with competing failures subject to failure isolation and propagation effects," *Reliability Engineering & System Safety*, vol. 95, pp. 1210-1215, 2010.
- [77] Fan D, Zhang A, Feng Q, Cai B, Liu Y, Ren Y. "Group maintenance optimization of subsea Xmas trees with stochastic dependency," *Reliability Engineering & System Safety*, vol. 209, pp. 107450, 2021.
- [78] De Dianous V, Fievez C. "ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance," *Journal of Hazardous Materials*, vol. 130, pp. 220-233, 2006.
- [79] Willey RJ. "Layer of protection analysis," *Procedia Engineering*, vol. 84, pp. 12-22, 2014.
- [80] Kjellén U. "Safety in the design of offshore platforms: Integrated safety versus safety as an add-on characteristic," *Safety science*, vol. 45, pp. 107-127, 2007.
- [81] Prashanth I, Fernandez GJ, Sunder RG, Boardman B. "Factors influencing safety barrier performance for onshore gas drilling operations," *Journal of Loss Prevention in the Process Industries*, vol. 49, pp. 291-298, 2017.
- [82] DOE. "Hazard and barrier analysis guidance document." Department of energy, 1996.
- [83] Duijm NJ. "Safety-barrier diagrams as a safety management tool," *Reliability Engineering & System Safety*, vol. 94, pp. 332-341, 2009.
- [84] Duijm NJ, Markert F. "Safety-barrier diagrams as a tool for modelling safety of hydrogen applications," *International Journal of Hydrogen Energy*, vol. 34, pp. 5862-5868, 2009.
- [85] Reason J, Hollnagel E, Paries J. "Revisiting the Swiss cheese model of accidents," *Journal of Clinical Engineering*, vol. 27, pp. 110-115, 2006.
- [86] Perneger TV. "The Swiss cheese model of safety incidents: are there holes in the metaphor?," *BMC health services research*, vol. 5, pp. 1-7, 2005.
- [87] Larouzee J, Le Coze J-C. "Good and bad reasons: The Swiss cheese model and its critics," *Safety science*, vol. 126, pp. 104660, 2020.
- [88] Jacinto C, Silva C. "A semi-quantitative assessment of occupational risks using bow-tie representation," *Safety Science*, vol. 48, pp. 973-979, 2010.
- [89] De Ruijter A, Guldenmund F. "The bowtie method: A review," *Safety science*, vol. 88, pp. 211-218, 2016.
- [90] Harms-Ringdahl L. "Assessing safety functions—results from a case study at an industrial workplace," *Safety Science*, vol. 41, pp. 701-720, 2003.
- [91] Shahrokhi M, Bernard A. "A development in energy flow/barrier analysis," *Safety science*, vol. 48, pp. 598-606, 2010.
- [92] Aven T, Sklet S, Vinnem JE. "Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part I. Method description," *Journal of hazardous Materials*, vol. 137, pp. 681-691, 2006.
- [93] Sklet S, Vinnem JE, Aven T. "Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part II: Results from a case study," *Journal of hazardous materials*, vol. 137, pp. 692-708, 2006.
- [94] Gowland R. "The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment?," *Journal of hazardous materials*, vol. 130, pp. 307-310, 2006.
- [95] Guo H, Yang X. "A simple reliability block diagram method for safety integrity verification," *Reliability Engineering & System Safety*, vol. 92, pp. 1267-1273, 2007.

- [96] Tsunemi K, Kihara T, Kato E, Kawamoto A, Saburi T. "Quantitative risk assessment of the interior of a hydrogen refueling station considering safety barrier systems," *International Journal of Hydrogen Energy*, vol. 44, pp. 23522-23531, 2019.
- [97] Cai B, Liu Y, Liu Z, Tian X, Zhang Y, Ji R. "Application of Bayesian networks in quantitative risk assessment of subsea blowout preventer operations," *Risk Analysis*, vol. 33, pp. 1293-1311, 2013.
- [98] Innal F, Cacheux P-J, Collas S, Dutuit Y, Folleau C, Signoret J-P, et al. "Probability and frequency calculations related to protection layers revisited," *Journal of Loss Prevention in the Process Industries*, vol. 31, pp. 56-69, 2014.
- [99] Liu Y, Rausand M. "Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems," *Reliability Engineering & System Safety*, vol. 145, pp. 366-372, 2016.
- [100] Kaczor G, Młynarski S, Szkoda M. "Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams," *Journal of Loss Prevention in the Process Industries*, vol. 41, pp. 31-39, 2016.
- [101] Liu Y, Rausand M. "Reliability assessment of safety instrumented systems subject to different demand modes," *Journal of Loss Prevention in the Process Industries*, vol. 24, pp. 49-56, 2011.
- [102] IEC60050. "International Electrotechnical Vocabulary." Geneva. International Electrotechnical Commission, 1990.
- [103] ISO14224. "Petroleum, petrochemical and natural gas industries: Collection and exchange of reliability and maintenance data for equipment." Geneva. International Organization for Standardization, 2006.
- [104] OREDA. "Offshore and onshore reliability data ". Høvik, Norway. OREDA Participants, 2015.
- [105] EXDIA. "Safety Equipment Reliability Handbook." Sellersville, PA. EXIDA, 2007.
- [106] SINTEF. "Reliability data for safety instrumented systems, PDS data handbook." Trondheim, Norway. SINTEF, 2013.
- [107] SINTEF. "Reliability prediction method for safety instrumented systems, PDS method handbook." Trondheim, Norway. SINTEF, 2013.
- [108] Hasani F. "Calculation and Analysis of Reliability with Consideration of Common Cause Failures (CCF)(Case Study: The Input of the Dynamic Positioning System of a Submarine)," *International Journal of Industrial Engineering & Production Research*, vol. 28, pp. 175-187, 2017.
- [109] Jin H, Rausand M. "Reliability of safety-instrumented systems subject to partial testing and common-cause failures," *Reliability Engineering & System Safety*, vol. 121, pp. 146-151, 2014.
- [110] Jahanian H. "Generalizing PFD formulas of IEC 61508 for KooN configurations," *ISA transactions*, vol. 55, pp. 168-174, 2015.
- [111] Chebila M, Innal F. "Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH," *Journal of loss Prevention in the process industries*, vol. 34, pp. 167-176, 2015.
- [112] Guo H, Yang X. "Automatic creation of Markov models for reliability assessment of safety instrumented systems," *Reliability Engineering & System Safety*, vol. 93, pp. 829-837, 2008.
- [113] Tugnoli A, Cozzani V, Di Padova A, Barbaresi T, Tallone F. "Mitigation of fire damage and escalation by fireproofing: A risk-based strategy," *Reliability Engineering & System Safety*, vol. 105, pp. 25-35, 2012.
- [114] Blaxter L, Hughes C, Tight M. "How to research," McGraw-Hill Education (UK),2010.

- [115] Creswell JW. "Educational research: Planning, conducting, and evaluating quantitative," Prentice Hall Upper Saddle River, NJ,2002.
- [116] Fisher WW, Mazur JE. "Basic and applied research on choice responding," Journal of applied behavior analysis, vol. 30, pp. 387-410, 1997.
- [117] Bentley PJ, Gulbrandsen M, Kyvik S. "The relationship between basic and applied research in universities," Higher Education, vol. 70, pp. 689-709, 2015.
- [118] Phillips E, Pugh D. "How to get a PhD: A handbook for students and their supervisors," McGraw-Hill Education (UK),2015.
- [119] Bryman A. "Social research methods," Oxford university press,2016.

This page is intentionally left blank

Part 2

Articles

This page is intentionally left blank

Article I

Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Common cause failure and cascading failures in technical systems: similarities, differences, and barriers. *Proceedings of the 28th European Safety and Reliability Conference (ESREL)*, June 17-21, 2018, Trondheim, Norway.

This page is intentionally left blank

Common cause failures and cascading failures in technical systems: Similarities, differences and barriers

L. Xie, M.A. Lundteigen & Y.L. Liu
NTNU, Trondheim, Norway

ABSTRACT: Many technical systems continue to increase in size and complexity, with more interactions and interdependencies between components. Dependent failures, such as common cause failures and cascading failures, are becoming important concerns to system reliability. Both failure types may lead to the unavailability of multiple components at the same time or within a short time interval. Although many researchers have studied common cause failures and cascading failures respectively, there is little comparison of the two concepts. This paper investigates the similarities and differences of these two failure groups, with focus on the conditions and nature of initiations and propagation of such failures. Moreover, a comparison is also made about suitable barrier strategies that can either prevent or reduce the consequences of failure. The paper concludes the study with a demonstration of reliability modeling for common cause- and cascading failures.

1 INTRODUCTION

Technical systems, such like railway systems, processing systems in chemical and petroleum plants, and power grids, are becoming increasingly complex. These systems include many physical components, with a huge number of interaction and interdependencies. Sometimes, those failures occurring in multiple components are resulted from the interconnections. We refer to such failures as dependent failures. Within the category of dependent failures, there are two sub-categories that are of specific interest: common cause failures (CCFs) and cascading failures (Rausand and Lundteigen, 2014). In the chemical and process industry, cascading processes are called as domino effects (Abdolhamidzadeh et al., 2010, Abdolhamidzadeh et al., 2009, Landucci et al., 2016).

Past accidents and near misses have shown that dependent failures are one of main threats to a complex system. For example, CCFs are main contributors of failures in safety systems of the oil and gas industry (Smith and Simpson, 2004, Lundteigen and Rausand, 2007). Fires in the chemical and process industry highlight the severe cascading consequences (Landucci et al., 2016, Cozzani and Reniers, 2013). The blackouts in United States, Canada in 2003, and Europe in 2006 are also the examples of cascading failures (Kotzanikolaou et al., 2013, Andersson et al., 2005). Many other infrastructure systems, like water distribution networks, transportation, also often suffer from cascading failures (Lin et al., 2014, Shuang et al., 2014, Ouyang, 2014).

So far, it seems like most attention has directed to CCFs and in specific for safety-critical systems where redundancy is used actively to enhance reliability (Paula et al., 1991, Humphreys and Jenkins, 1991, Lundteigen and Rausand, 2007, IEC61508, 2010, A. Mosleh, 1998). There have been two main strategies suggested for incorporating defenses against CCFs in design. One is to carry out analyses to identify and remove causes, and the other is to introduce measures to reduce the effects of CCFs in case they occur. Suggested methods include cause-defense matrices, common cause analysis, and zonal analysis (Humphreys and Jenkins, 1991, Paula et al., 1991).

The defenses to CCFs are typically identified in design, however, measures in the operational phase are also important (Lundteigen and Rausand, 2007). Even for an excellent system design, there will always remain a risk of CCFs. It is therefore required to include the contribution of CCFs in quantitative analyses used to demonstrate adequate reliability. A high number of models has been introduced for this purpose (Vesely, 1977, Fleming, 1975, Evans et al., 1984, Mosleh and Siu, 1987). The standard beta factor model is perhaps the most widely adopted, due to its simplicity (Fleming, 1975, IEC61508, 2010). The PDS method (Hauge et al., 2015) is an extension of the standard beta factor, where a second parameter is added to account for voting, e.g. 2-out-of-3 and 1-out-of-3.

As for cascading failures, it is of interest to consider efficient means to avoid or reduce the vulnerability of the failures in the system design, and to quantify cascading failures. An important

task in these analyses is to study interdependencies, and many analyzing approaches in literature are based the topology of complex network (Motter and Lai, 2002, Wang, 2012, Albert and Barabási, 2002). One kind of cascading failures are the failures when a heavily load component fails, and its load is redistributed to other components, resulting in loads on that exceed their capacities. State-based approaches, such as Markovian process, approaches based on the Bayesian network models, and Monte Carlo Simulation have been used to analyze cascading failures (Iyer et al., 2009, Calviño et al., 2016, Erp et al., 2017).

In fact, many technical systems can be subject to both CCFs and cascading failures, thus it is important to consider both failure categories in reliability analysis. Unfortunately, very limited attention has been directed comparing the two types of dependent failures, and their corresponding defense strategies. Kotzanikolaou et al. (2013) highlight that CCFs may have cascading effects, but do not go into much detail.

The objective of this paper is therefore to make a comprehensive comparison on the concepts, causes, and mechanisms of the two failures, and provide some suggestions on the analysis and defense strategies. In this paper, we use the term of barrier to denote a specific defense measure.

The rest of the paper is organized as follows: In [section 2](#), we discuss the definitions and interpretations of CCFs and cascading failures. [Sections 3](#) and [4](#) present the similarities and distinctions of the two failures. In [section 5](#), we clarify the barriers against the two failures. A small example is then employed in [section 6](#), to illustrate that the effects of CCFs and cascading failures. Conclusions and discussions occur in [section 7](#).

2 DEFINITIONS AND INTERPRETATIONS

According to Humphreys and Jenkins (Humphreys and Jenkins, 1991), *dependent failures refer to the failures whose probability cannot be expressed by unconditional probability of the individual event*. Dependencies in a technical system may derive from the sameness of the types of components, exposure from the same environment, the use of shared resources, functionality, the common shocks and the incapability to resist certain hazardous events (Rausand, 2013).

People in different industrial sectors define CCFs in their own ways. Nuclear sector defines it as *two or more component fault states exist at the same time, or with a short interval, because of a shared cause* (Mosleh et al., 1988). The generic standard on design and operation of electric, electronic, and programmable electronic safety-related

systems, IEC 61508, defines a CCF as *a failure that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure* (IEC61508, 2010). Both definitions emphasize that CCFs involve at least two failures that are due to a shared or common cause.

Cascading failure may be *multiple failures, where initiated by the failure of one component in the system that results in a chain reaction, the so-called domino effect* (Rausand and Øien, 1996). In power systems, cascading failure is referred to *a sequence of dependent failures of individual components that successively weakens the systems* (Baldick et al., 2008). It differs from the definition in infrastructures that limit the cascading failure to the propagation of failures between components (Rinaldi et al., 2001). Generally, we can find some same elements in the definitions that cascading failures are multiple failures initiated by one, and a sequential effect occurs.

From the perspective of failure causes, both CCFs and cascading failures result from some common vulnerabilities of more than one component. These two types of failures are interrelated in some cases (Laprie et al., 2007, Kotzanikolaou et al., 2013). However, they are still two distinctive categories of dependent failures. As Smith and Watson explained, CCFs emphasize that failures are located in ‘first in line’, which means that the failure are only dependent on the causes, but not on each.

In the following sections, we try to elaborate similarities and difference between the two failures.

3 SIMILARITIES

We categorize the similarities between CCFs and cascading failures into three: *multiplicity, timeliness and classification of causes*.

3.1 Multiplicity

Both CCFs and cascading failures obviously involve more than one components. We are concerned with the *effect of failure* of several components and *functions* for two categories of failures.

3.2 Timeliness

For both CCFs and cascading failures, the time from the first failure to the existence of multiple failures is often short. In case of insufficient mitigation measures, the collapse of an entire system may occur very soon. For example, in the Three Mile Island accident caused by CCFs in 1979, the radiation level in the primary coolant water

was around 300 times of the expected level after only 2 hours (Hasani, 2017). The power blackout in India in 2012 due to cascading failures, spread across 22 states within 12 hours and affected more than 620 million people (Russel, 2012).

3.3 Root causes

Root causes of both CCFs and cascading failures are the common vulnerability of more than one components in a system. Coupling factors between components can explain why multiple components are destroyed by a common hazardous event, e.g. cold temperature, extreme snowfall or electrical failure. Meanwhile, for cascading failures, couplings also can explain why multiple components are affected by the faults of relevant components. For example, the unavailability of one processing unit increases the workload of another unit.

from shared causes, may be simultaneous failures or failures with some time apart. A cascading failure always starts with a single preceding component failure, as the effect of an initiating event.

Table 1. Differences between CCFs and cascading failures.

Difference	Characteristics	CCFs	Cascading failures
Initiation	Triggering condition	Shared causes	Conditional on preceding failures
	Occurrence	Simultaneously or during a critical time of interest	Sequence
Propagation	Sequence	First in line	Series
	Consequence	Finite	Possibly infinite
	Pathway	Cause-components	Connected/dependent components

4 DIFFERENCES

For differences between two types of failures, we categorize them into two: *initiation* and *propagation* of failures, as shown in Table 1. Initiation of failures.

As seen in Table 1, the initiating event of a CCF can be either replicated or occur simultaneously for several components. The effect of CCFs arises

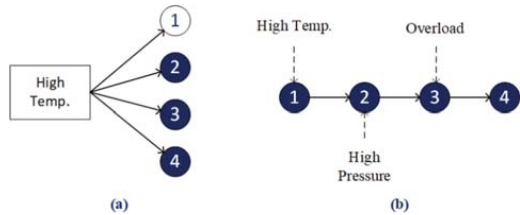


Figure 1. CCF and cascading failures.

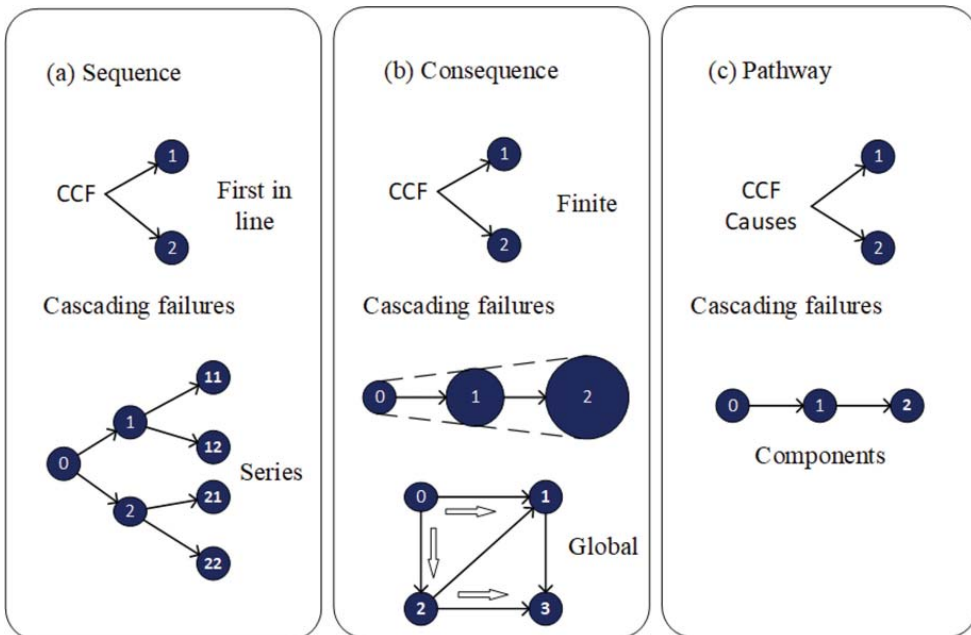


Figure 2. Comparisons of CCFs and cascading failures in terms of impact and effect.

To illustrate these differences, we introduce two small examples, as shown in Figure 1. High temperature is the initiating event of both a CCF and a cascading failure in this case. In Figure 1(a), all the four components expose themselves to high temperature, and so all or some of the components fail simultaneously or in a short interval. However, in the case of a cascading failure of Figure 1(b), only component 1 is exposed to high temperature, and fails due to this initiating event. Then, the failure of component 1 triggers the failures of other components due to diverse reasons. Even in the same cascading sequence, the failure causes can be different for the different components.

4.1 Propagation of failures

Propagation of failure means in this context the involvement of multiple failures, with the initiating event already manifested. Figure 2 illustrates the differences in the propagation of CCFs and cascading failures. CCFs are *first in line* failures that delineate the exclusion of dependent failures from CCF definition (Smith and Watson, 1980), which implies that CCFs are directly linked to the failure causes. On the contrary, the propagation of a cascading failure follows a series of interactions. CCFs are most different from cascading failures in terms of the approaches of propagation. As shown in Figure 2(a), for CCFs, the first in line failure only occurs on component 1 and 2. For the consequence of failure propagation, as shown in Figure 2(b), a cascading failure can escalate and result in worse impacts on the other parts of a system, such as more serious disruptions, overload to neighbors and longer recovery time etc. CCFs highlight a direct cause-effect relationship between the cause and the failed components (Rausand and Lundteigen, 2014), whereas the pathway of cascading failures involve the interactions or dependencies between relevant components, see in Figure 2(c).

5 BARRIERS

Barriers are employed to prevent, control or mitigate undesired events or accident (Sklet, 2006). Sometimes, barriers are also called defenses, protection layers or countermeasures. In general, a barrier function can be realized by many different means, such as by a technical or physical system, human actions and procedural deficiencies.

In the design phase of a system, it is possible to introduce barriers against potential failures, like separation, diversity, quality control, simplicity of design etc. Some of them are effective to reduce the probability of CCFs, and some of them are

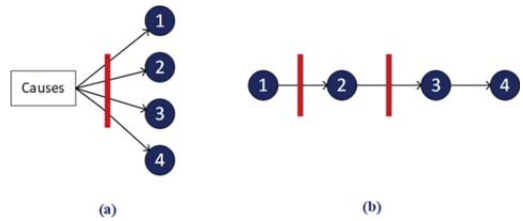


Figure 3. Barriers for CCF and cascading failures.

more functional for protecting the system from cascading failures. Considering the similarities and differences of CCFs and cascading failures, we can categorize barriers into three groups: *barriers against both failures*, *barriers against CCFs* and *barriers against cascading failures*.

- **Barriers efficient for both failures:** Such kind of barriers should be designed in consideration of the similarities of CCFs and cascading failures, such like their root causes and coupling factors. One way of barrier design is therefore to mitigate and reduce the vulnerability to root causes. Simplicity can be regarded as a barrier, for example, to reduce system complexity that is one important source of vulnerability. Another way of barrier design is to decrease the coupling degrees among components. Spatial and temporal separations are examples of decreasing coupling degrees. In practices, we can find that firewalls in a process plant are effective barriers to prevent fire disasters.
- **Barriers against CCFs:** The effectiveness of such barriers is to isolate failure causes and components, as shown in Figure 3(a). One example is diversity of the design. Diverse components will often have different failure modes, and are therefore less likely to be affected by the common cause. However, diversity is not effective to mitigate cascading failures. When the failure of one component brings higher workload to its neighbors and their failure probabilities, no matter the components are identical or not.
- **Barriers against cascading failures:** The main purposes of this kind of barriers are to stop or slow down failure propagation, as shown in Figure 3(b). An example for this class of barriers is a process shutdown valve that can isolate related process segments. In case abnormal events have occurred in the upstream facility, the shutdown valve can stop or limit the flow between two facilities, and thereby cease the failure propagation.

In the next section, we will use a small example to illustrate the quantitative analyses for CCFs and cascading failures, and the effects of barriers.

6 CASE STUDY

Suppose a system comprising two parallel components. The effects of failures and corresponding barriers for the two dependent failures are studied separately, as illustrated in Figure 4.

For modeling CCFs, a new *independent* “CCF” event is added in the standard beta model with beta-factor β . The parameter β can be interpreted as the conditional probability that a failure of a channel is in fact a common-cause failure:

$$\beta = \Pr(\text{CCF} | \text{Failure of channels}) \quad (1)$$

With inclusion of CCFs, the total system reliability can be obtain as:

$$R(t) = 2R - R^{(2-\beta)} \quad (2)$$

where $R = 0.8$ and $\beta = 0.1$.

For modeling cascading failures, it is necessary to consider the effects of functional dependency between the two components, and Bayesian network model is an approach we used here. The conditional failure probability is a measure of dependency that differ from the conditional probability β for CCFs. The conditional probability for cascading failures can be defined as:

$$\Pr(\text{Comp. B fails} | \text{comp. A fails}) = \frac{F_D}{F_A} \quad (3)$$

Here, F_A and F_B denote the individual failure probability for component A and B. F_D denotes the failure probability for component A on the condition of component A has failed. The total system reliability with cascading failures can be obtained as:

$$R(t) = 1 - F_A(F_B + F_D - F_B F_D) \\ = 1 - (1 - R)^2 - (1 - R)^2 R P_r \quad (4)$$

where P_r denotes conditional probability between component A and B and is assigned as 0.1 ($\Pr = 0.1$).

As shown in Figure 5, the total system reliability with CCFs becomes 0.946, but it is 0.957 with the effects of cascading failures at that time. This

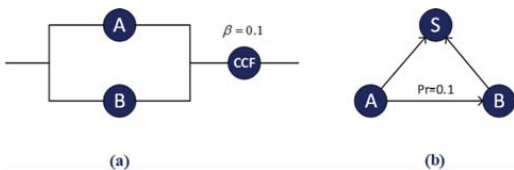


Figure 4. Case study for CCF and cascading failures.

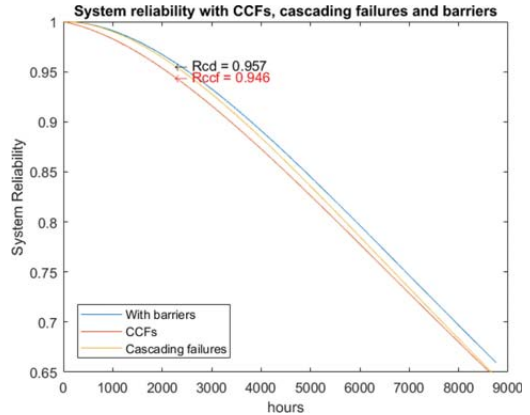


Figure 5. Reliability with cascading failures & CCFs.

implies that CCFs may have more influence on the reliability performance than cascading failures in this case, when using similar assumptions about the probability of having additional failures, when a first failure has occurred.

We now introduce time-dependent probabilities for reliability analysis, and assume that the time to failure is exponentially distributed, with failure rate of $1E-04$ per hour for each component. For the system with CCFs, the total system reliability can be obtain as:

$$R(t) = [2e^{-(1-\beta)\lambda t} - e^{-2(1-\beta)\lambda t}] e^{-\beta\lambda t} \quad (5)$$

For the system with cascading failures, the total system reliability can be obtain as:

$$R(t) = 1 - (1 - e^{-\lambda t})^2 - (1 - e^{-\lambda t})^2 e^{-\lambda t} P_r \quad (6)$$

Figure 5 illustrates calculated system reliability considering the effects of the two failures as a function of time. We can see that, in this case, the two failures seems to have comparable effects on the system reliability.

For CCFs, the function of barriers is to separate shared root causes from the components. The function of the barriers against cascading failures is to prevent propagation of the failures between component A and B. Reliability of the system with barriers is illustrated in the blue line in Figure 5, implying that the system reliability will increase when performing barriers function against the failures.

7 CONCLUSION AND FURTHER WORK

Exploring similarities and difference between CCFs and cascading failures facilitate us to answer

the following questions: 1) why such dependent failures initiate, 2) how dependent failures contribute to disruptions in the systems, and 3) what kind of barriers are needed and how they should be implemented. In this paper, we find that CCFs and cascading failures may have comparable influences on the performance of a simple system. More probabilistic and quantitative analyses are required, to evaluate the impacts of cascading failures in a larger and more complex system (Erp et al., 2017).

Our further work will involve modeling the interdependent systems with cascading failures and CCFs, and developing tools to evaluate reliability for complex systems. It is also of interest to identify different failure modes and perform barrier analysis for both of the failures, which can help to allocate barriers and thereby optimize barrier functions.

REFERENCES

- Abdolhamidzadeh, B., Abbasi, T., Rashtchian, D. & Abbasi, S.A. (2010) A new method for assessing domino effect in chemical process industry. *Journal of hazardous materials*, 182, 416–426.
- Abdolhamidzadeh, B., Rashtchian, D. & Ashuri, E. (2009) A new methodology for frequency estimation of second or higher level domino accidents in chemical and petrochemical plants using monte carlo simulation. *Iranian Journal of Chemistry and Chemical Engineering (IJCCE)*, 28, 21–28.
- Albert, R. & Barabási, A.-L. (2002) Statistical mechanics of complex networks. *Reviews of modern physics*, 74, 47.
- Andersson, G., Donalek, P., Farmer, R., Hatziaargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P. & Sanchez-Gasca, J. (2005) Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems*, 20, 1922–1928.
- Baldick, R., Chowdhury, B., Dobson, I., Dong, Z., Gou, B., Hawkins, D., Huang, H., Joung, M., Kirschen, D. & Li, F. (2008) Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures. *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*. IEEE.
- Calviño, A., Grande, Z., Sánchez-Cambronero, S., Gallego, I., Rivas, A. & Menéndez, J.M. (2016) A Markovian-Bayesian network for risk analysis of high speed and conventional railway lines integrating human errors. *Computer-Aided Civil and Infrastructure Engineering*, 31, 193–218.
- Cozzani, V. & Reniers, G. (2013) Historical background and state of the art on domino effect assessment. *Domino Effects in the Process Industries: Modelling, Prevention and Managing*. Elsevier, Amsterdam, The Netherlands.
- Erp, N.V., Linger, R., Khakzad, N. & Gelder, P.V. (2017) Report on risk analysis framework for collateral impacts of cascading effects. *RAIN—Risk Analysis of Infrastructure Networks in Response to Extreme Weather*. TU Delft.
- Evans, M., Parry, G. & Wreathall, J. (1984) On the treatment of common-cause failures in system analysis. *Reliability engineering*, 9, 107–115.
- Fleming, K. (1975) Reliability model for common mode failures in redundant safety systems. *Modeling and simulation. Volume 6, Part 1*.
- Hasani, F. (2017) Calculation and Analysis of Reliability with Consideration of Common Cause Failures (CCF)(Case Study: The Input of the Dynamic Positioning System of a Submarine). *International Journal of Industrial Engineering & Production Research*, 28, 175–187.
- Hauge, S., Hoem, A., Hokstad, P., Habrekke, S. & Lundteigen, M.A. (2015) Common Cause Failures in Safety Instrumented Systems. SINTEF Technology and Society Trondheim.
- Humphreys, P. & Jenkins, A.M. (1991) Dependent failures developments. *Reliability Engineering & System Safety*, 34, 417–427.
- Iec61508 (2010) Functional safety of electrical/electronic/programmable electronic safety related systems. *International Electrotechnical Commission*.
- Iyer, S.M., Nakayama, M.K. & Gerbessiotis, A.V. (2009) A Markovian dependability model with cascading failures. *IEEE Transactions on Computers*, 58, 1238–1249.
- Kotzanikolaou, P., Theoharidou, M. & Gritzalis, D. (2013) Cascading effects of common-cause failures in critical infrastructures. *International Conference on Critical Infrastructure Protection*. Springer.
- Landucci, G., Argenti, F., Spadoni, G. & Cozzani, V. (2016) Domino effect frequency assessment: The role of safety barriers. *Journal of Loss Prevention in the Process Industries*, 44, 706–717.
- Laprie, J.-C., Kanoun, K. & Kaâniche, M. (2007) Modelling interdependencies between the electricity and information infrastructures. *Computer Safety, Reliability, and Security*, 54–67.
- Lin, Y., Li, D., Liu, C. & Kang, R. (2014) Framework design for reliability engineering of complex systems. *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2014 IEEE 4th Annual International Conference on*. IEEE.
- Lundteigen, M.A. & Rausand, M. (2007) Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *Journal of Loss Prevention in the process industries*, 20, 218–229.
- Mosleh, A., D.M. Rasmuson & F.M. Marshall (1998) Guidelines on modeling common cause failures in probabilistic risk assessment.
- Mosleh, A., Fleming, K., Parry, G., Paula, H., Worledge, D. & Rasmuson, D.M. (1988) Procedures for treating common cause failures in safety and reliability studies: Volume 1, Procedural framework and examples. Pickard, Lowe and Garrick, Inc., Newport Beach, CA (USA).

- Mosleh, A. & Siu, N. (1987) A multi-parameter common cause failure model. *Transactions of the 9th international conference on structural mechanics in reactor technology. Vol. M.*
- Motter, A.E. & Lai, Y.-C. (2002) Cascade-based attacks on complex networks. *Physical Review E*, 66, 065102.
- Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability engineering & System safety*, 121, 43–60.
- Paula, H.M., Campbell, D.J. & Rasmuson, D.M. (1991) Qualitative cause-defense matrices: Engineering tools to support the analysis and prevention of common cause failures. *Reliability Engineering & System Safety*, 34, 389–415.
- Rausand, M. (2013) *Risk assessment: theory, methods, and applications*, John Wiley & Sons.
- Rausand, M. & Lundteigen, M.A. (2014) *Reliability of safety-critical systems: theory and applications*, John Wiley & Sons.
- Rausand, M. & Øien, K. (1996) The basic concepts of failure analysis. *Reliability Engineering & System Safety*, 53, 73–83.
- Rinaldi, S.M., Peerenboom, J.P. & Kelly, T.K. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21, 11–25.
- Russel, H.S. a. R. (2012) 620 million without power in India after 3 power grids fail.
- Shuang, Q., Zhang, M. & Yuan, Y. (2014) Node vulnerability of water distribution networks under cascading failures. *Reliability Engineering & System Safety*, 124, 132–141.
- Sklet, S. (2006) Safety barriers: Definition, classification, and performance. *Journal of loss prevention in the process industries*, 19, 494–506.
- Smith, A.M. & Watson, I.A. (1980) Common cause failures—a dilemma in perspective. *Reliability Engineering*, 1, 127–142.
- Smith, D.J. & Simpson, K.G. (2004) *Functional Safety: A straightforward guide to applying IEC 61508 and related standards*, Routledge.
- Vesely, W. (1977) Estimating common cause failure probabilities in reliability and risk analysis: Marshall-Olkin specializations. *Nuclear systems reliability engineering and risk assessment*, 2.
- Wang, J. (2012) Mitigation of cascading failures on complex networks. *Nonlinear Dynamics*, 70, 1959–1967.

This page is intentionally left blank

Article II

Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Safety barriers against common cause failure and cascading failure: literature reviews and modeling strategies. *Proceedings of IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, December 16-19, 2018, Bangkok, Thailand.

This paper is not included due to IEEE copyright

This page is intentionally left blank

Article III

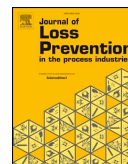
Xie, Lin; Håbrekke, Solfrid; Liu, Yiliu; Lundteigen, Mary Ann. Operational data-driven prediction for failure rates of equipment in safety instrumented systems: A case study from the oil and gas industry. *Journal of Loss Prevention in the Process Industries* (2019); Volume 60. s. 96-105.

This page is intentionally left blank



Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Operational data-driven prediction for failure rates of equipment in safety instrumented systems: A case study from the oil and gas industry

Lin Xie^a, Solfrid Håbrekke^b, Yiliu Liu^a, Mary Ann Lundteigen^{a,*}^aNorwegian University of Science and Technology, Trondheim, Norway^bSINTEF Digital, Trondheim, Norway

ARTICLE INFO

Keywords:

Safety instrumented system
Data collection
Failure rates
Data-driven models

ABSTRACT

Safety instrumented systems are frequently deployed to reduce the risk associated with industrial activities, such as those in the oil and gas industry. A key requirement for safety-instrumented systems in standards like IEC 61508 and IEC 61511, is that the safety functions and their equipment must fulfill the requirements of a given safety integrity level. A safety integrity level formulates a maximum tolerated probability of failure on demand, which must be confirmed in design as well as follow-up phases. The equipment's failure rates are important inputs to this analysis, and these figures assumed from design must be re-estimated and verified based on the operational experiences with the equipment at the specific facility. A thorough review of reported failures from six Norwegian onshore and offshore oil and gas facilities indicates that equipment of similar type experience different failure rates and different distribution of the occurrence of failure modes. Some attempts have been made to identify the underlying influencing factors that can explain the differences, however, so far the utilization of data-driven methods have not been fully explored. The purpose of this paper is two-fold: 1) demonstrate how data-driven methods, i.e. principal component analysis and partial least squares regression, can be used to identify important influencing factors, and 2) propose a framework for predicting the failure rates based on the reported failures. The framework is illustrated with a case study based on the data collected from the six facilities.

1. Introduction

Safety instrumented systems (SISs) are frequently used to reduce the risks associated with industrial activities in many industries, e.g. at process and nuclear power plants, and at oil and gas facilities (Rausand, 2014). A SIS is characterized as a system that relies on electrical/electronic/programmable electronic (E/E/PE) technologies to detect abnormal situations. SISs perform one or more safety instrumented functions (SIFs) to protect the equipment under control (EUC) against the occurrence of hazardous events (IEC61511, 2016). An industrial facility usually is equipped with several SISs, such as process shutdown (PSD) system to stop production in case of process upsets, and emergency shutdown (ESD) system to reduce the escalation of uncontrolled events like leakages by depressurizing and removing electrical ignition sources. A SIS generally consists of three main subsystems: sensor(s) (e.g. level transmitters, gas detectors, and push buttons), logic solver(s) (e.g. programmable logic controller and industrial computer) and final element(s) (e.g. shutdown valves, and circuit breakers). As illustrated in Fig. 1, the sensors detect possible abnormal situations, and the logic

solvers activate, and the final elements take actions according to the sensor inputs.

The standards for SISs, e.g. IEC 61508 and IEC 61511, state that the SIFs performed by SISs must fulfill the requirements of specified safety integrity levels (SILs) (IEC61508, 2010; IEC61511, 2016). Each SIL defines the maximum tolerated (average) probability of failure on demands (PFD). The PFD of a SIF must be estimated in design, using generic (often field-based) failure rates or those provided by manufacturers, and then re-estimated in operation using reported failures from the facilities where the SIF is installed (Rausand, 2014). A failure rate is defined as an average frequency of failure, i.e. a number of failures per unit of time (ISO14224, 2006). Failure rates can generally be classified into three groups: generic, manufacturer-provided and user-provided failure rates, depending on how they have been derived (Rausand, 2014).

In oil and gas industry, *Generic failure rates* for SIS equipment performing SIFs are presented in databases and handbooks, like Offshore and Onshore Reliability Data (OREDA, 2015), Safety Equipment Reliability (EXDIA, 2007) and Reliability Data for Safety Instrumented

* Corresponding author.

E-mail address: mary.a.lundteigen@ntnu.no (M.A. Lundteigen).<https://doi.org/10.1016/j.jlp.2019.04.004>

Received 26 November 2018; Received in revised form 14 March 2019; Accepted 4 April 2019

Available online 09 April 2019

0950-4230/© 2019 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

Nomenclature			
SIS	safety instrumented system	P, Q	loading matrix
PSD	process shutdown	X	explanatory variable
ESD	emergency shutdown	V	eigen value
FTO	fail to open	Y	response variable
LCP	leakage in closed position	$\bar{E}, \bar{F}, \bar{F}^*$	residuals from decomposition
DOP	delayed operation	NIPALS	nonlinear iterative PLS algorithm
OTH	other	$\lambda_{DU,i}$	failure rate of DU failure, corresponding to failure mode i
PCA	principal component analysis	θ_{ij}	weight of influencing factor j , corresponding to failure mode i
PLSR	partial least squares regression	σ_{ij}	score of influencing factor j , corresponding to failure mode i
DD	dangerous detected	λ_{DU}^*	predicted failure rate
DU	dangerous undetected	LT	level transmitter
PC	principal component	PSV	pressure safety valve
SIF	safety instrumented function	DU_YES	revealed DU failure
SIL	safety integrity level	DU_NO	no revealed DU failure
GLM	generalized linear model	PDS	reliability data for safety instrumented system
Cox	proportional hazards model	SAR	safety analysis report
HC	hydrocarbon	P&ID	process and instrument diagram
T	score matrix	SRS	safety requirement specification

Systems (PDS data handbook¹) (SINTEF, 2013a). OREDA databases and handbooks rely on failures reported in operation from multiple operating companies, while e.g. PDS data handbook relies on a combination of OREDA data, expert judgment, and manufacturer information. Generic failure rates are mainly applied in reliability analysis during the design phase before the designers have decided on what equipment to purchase. *Manufacturer-provided data* is meanwhile based on analyses of specific products, laboratory testing and collected data, typically during the warranty period. It is often seen that manufacturer-provided failure rates are lower than what is experienced in operation (SINTEF, 2013b). *User-provided failure rates* are based on aggregated time in service and the number of reported failures at one or more specific facilities owned by the same operating company. The standards and regulations, such as IEC61508, IEC 61511, ISO 14224 and GL070, have given certain requirements with respect to the failure rates (GL070, 2004; IEC61508, 2010; IEC61511, 2016; ISO14224, 2006). IEC 61508 states that the failure rates used in a reliability analysis should have at least a confidence level of 70% (IEC61508, 2010). The uncertainty of the estimated failure rates is required in OREDA to be presented as a 90% confidence interval with a lower limit and an upper limit (OREDA, 2015). In order to fulfill 90% confidence, a guideline proposed by SINTEF² suggests that operational hours times the number of failures should exceed $3 \cdot 10^6$ hours (Hauge and Lundteigen, 2008). In addition, when the upper 95% percentile is approximately three times the mean value or lower, we may use the estimated failure rates based on operational experience (Hauge and Lundteigen, 2008). In this context, many oil and gas facilities invest time and resources to record failures to obtain estimated failure rates.

A number of methods can be applied to estimate failure rates. In many applications, failure rates are estimated as the maximum likelihood estimators (i.e. the total number of failures divided by the aggregated time in service) (OREDA, 2015). Estimation of the failure rates should also consider specific operational conditions (IEC61508, 2010). Different models are suggested to analyze the impact of various operational conditions from one facility to another. Physical models considering physical laws like Arrhenius's law, Voltage acceleration and

Gunn's law, are used to estimate failure rates (Foucher et al., 2002; Ratkowsky et al., 1982). MIL-HDBK-217 (MIL-HDBK-217F, 1995), Telcordia SR-332 (TelcordiaSR-332, 2001) and IEC 61709 (IEC61709, 2017) propose analytical failure functions of parameters, e.g. temperature, humidity, stress, voltage or electrical intensity. Statistical models can use operational data to investigate the trends of failure rates, such as Cox models (proportional hazards model) and Bayesian models (Becker and Camarinopoulos, 1990; Cox, 1972; Elsayed and Chan, 1990; Kutylowska, 2015; Newby, 1994). Brissaud suggests a way to predict failure rates with consideration of the influences from design, manufacture or installation etc. (Brissaud et al., 2010). A similar method is suggested by Vatn, taking into account the effects of implementation of risk reduction measures in the prediction (Vatn, 2006). It is noticed that the physical models for estimating failure rates require well-known knowledge about physical mechanism leading to the failures. In this paper, in order to develop a general model, the prediction of failure rates is only based on statistical models.

Most statistical models mentioned above rely on the data for a large group of equipment. The items within a group are assumed to have similar functions and the same failure rates, however, their design (e.g. measuring principle), location, and environment can be different. SINTEF has previously performed a study where it was documented that similar equipment experienced varied failure rates even if the operating environment is the same (Håbrekke et al., 2017). The study has shown that shutdown valves with flow medium gas and hydrocarbon (HC) liquid experience different failure rates. It was also showed that the failure mode, i.e. the type of failure, was influenced by certain parameters. For example, the occurrence of the failure mode "fail to

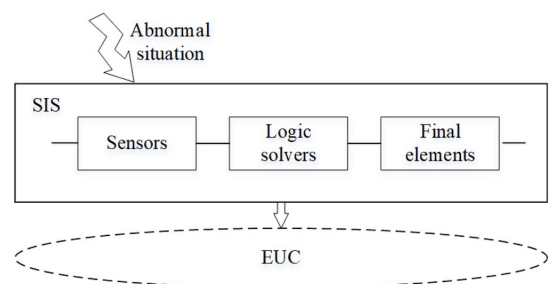


Fig. 1. Role and general configuration of SIFs.

¹ PDS forum is a co-operation between 20 participating companies, including oil companies, drilling contractors, engineering companies, consultants, safety system manufacturers and researchers, with a special interest in SISs, see www.sintef.no/pds.

² SINTEF: An independent Norwegian research organization (<https://www.sintef.no/en/>).

open” (FTO) for the same valves were strongly affected by the temperature of the medium flowing through the valves. The term significant influencing factors were thus introduced for those factors (e.g. design, operating environment, failure mode) with the strongest effects on the failure rates. These factors have been analyzed by using traditional statistical models, however, data-driven methods could also be suitable (Håbrekke et al., 2018). In this paper, data-driven methods refer to the quantitative methods of identifying the correlations based on amounts of data, such as principal component analysis (PCA) and partial least squares regression (PLSR). Those data-driven models based on experienced data are now proposed to be incorporated with the traditional statistical models to predict failure failures of SIS equipment for new facilities in the design phase.

The purpose of this paper is to study the application of data-driven models for failure rate estimation. More specifically, the objectives are to: 1) demonstrate how data-driven methods, i.e. PCA and PLSR, can be used to identify significant influencing factors for the specific failures of SISs, and 2) propose a framework for predicting the failure rates based on the identified factors. The framework is illustrated with a case study from data collected at six Norwegian onshore and offshore oil and gas facilities. The framework is developed for SIS equipment, but can also be applied for other systems or equipment.

The rest of the paper is organized as follows: Section 2 gives some theoretical basis related to predictions of failure rates. Section 3 depicts a framework for prediction of failure rates. Section 4 illustrates the application of the proposed framework based on the data from six different oil and gas facilities. Finally, some conclusions and ideas for further work are discussed.

2. Theoretical basis

This section presents some selected definitions and concepts relating to failures as well as failure rate prediction and elaborates the basic principles of data-driven methods for identifying influencing factors.

2.1. Definitions of the failures

According to IEC 50(191), a failure is defined as “the termination of the ability of an item to perform a required function” (IEC60050, 1990). An item may refer to a system, subsystem, voted group or channel and component. IEC 61508 splits the failures of SISs into four groups (IEC61508, 2010): dangerous detected (DD) failures, dangerous undetected (DU), safe and no part/no effect failures. Both DD and DU failures are dangerous failures that are critical for the functionality of equipment. The difference between DD and DU failures lies in how the two types of failures are revealed. DU failures are latent and only revealed upon real demands, periodic tests, or inspections occasionally, while DD failures are revealed by automatic diagnostics once they occur. Since DU failures cannot be detected immediately and may not be fixed until e.g. the next periodic test, these failures contribute the most to the unavailability of SIS equipment. Hence, DU failures are of concern in most reliability studies and also in this paper.

Other important terms in this paper include “time to failure”, “failure cause”, “detection methods” and “failure mode”. Time to failure is often

referred to as the time elapsing from when the item is put into operation until it fails for the first time (Rausand and Hoyland, 2004). By time to DU failure we mean the time when the item is put into operation until a DU failure on it is revealed. Failure causes include circumstances associated with design, manufacture installation, use and maintenance that have led to a failure (IEC60050, 1990). Detection methods are used to describe how the failures are discovered (IEC61508, 2010). A failure mode is a possible state description of a faulty item, which tells how the inability is observed (Rausand, 2014).

2.2. Influencing factors

Estimation of DU failure rates from operation are often based on generic data and/or user-provided data. In addition, influencing factors that may affect the failure rates should be considered for prediction of failure rates, but it is not mandatory in all generic and user-provided data. Influencing factors are defined as the internal and external parts of a system which act on its reliability or failures (Brissaud et al., 2010). The term of influencing factor is more general than failures causes, and it relates to the indirect explanatory factors, for example, equipment attributes (e.g. sizes, types), operational environment (e.g. temperature, pressure, loads), manufacture activities (e.g. manufacturers, procedures), facility (e.g. location) and maintenance (e.g. test interval) and the activities of the end-user (e.g. general safety culture) (Brissaud et al., 2010; Rausand, 2014). Significant influencing factors are the factors whose effects are the most influencing on the failure rates. Each influencing factor can be broken down into several subcategories. The effects of influencing factors may relate to failure rates. For example, high temperature may lead to a higher frequency of the failures compared to low temperatures.

2.3. Data-driven models for identifying significant influencing factors

In previous analyses of influencing factors, Cox models and generalized linear model (GLM) have been used (Håbrekke et al., 2018). Both of the two models assume underlying failure distributions. For example, GLM is based on binomial distributions, where only two possible states of equipment are considered. A major advantage of these models is the ability to describe the analytical correlations between influencing factors and failure probability. However, both models require high quality data for representing simple statistical correlations, and they are sensitive to the number of factors. When a number of influencing factors are involved with complex interaction and non-linearity, Cox and GLM models may not be suitable.

More flexible models, such as those data-driven models, can be alternatives. PCA and PLSR are therefore introduced to investigate the correlation between many factors simultaneously. These models enable us to extract the most important information in order to understand the correlations that may exist between factors. PCA and PLSR have been applied for root cause identification, fault detection, and quality monitoring in many cases (Li et al., 2016; Qin, 2012; Tidriri et al., 2016). Here we will adopt them for understanding the essential relationships between the influencing factors and DU failures. Details regarding PCA and PLSR are found in the Appendix.

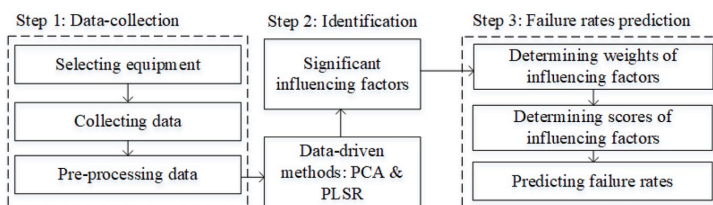


Fig. 2. Framework for predicting failure rates.

3. Framework of failure rate prediction

In this section, we propose a framework to predict failure rates of SIS equipment at a new facility based on experiences from comparable facilities. The framework clarifies the correlations between operational data and influencing factors, and thereby provides more preciseness in failure rates prediction for selected equipment. As illustrated in Fig. 2, the framework consists of three main steps: 1) data-collection, including a selection of equipment, collection, and pre-processing data; 2) identification of significant influencing factors to find out hidden correlations; and 3) failure rates prediction by determining the weights and scores of the factors.

3.1. Step 1: data-collection

The purpose of this step is to collect and interpret, classify and clean data. It is required to collect data concerning both failures and influencing factors. The failure data were obtained from failure notifications and maintenance records, ranging from time to DU failure, failure causes, and failure modes to detection methods. The data reflecting the states of influencing factors were related to equipment attributes, operational environment and maintenance activities, etc. Equipment attributes are used to describe equipment relating to manufacturer's data and design characteristics.

To limit the scope of the analysis, experts from manufacturers, oil and gas facilities and engineering companies within the PDS project have suggested some typical types of SIS equipment relevant for analysis. The selected groups of equipment should be accompanied by sufficient data to obtain the required statistical confidence. The recommendation is limited to four groups: shutdown valves (i.e. ESD and PSD valves), process safety valves (PSVs³), level transmitters (LTs), and gas detectors. In terms of their safety functions, shutdown valves can close and isolate related segments on demands, PSVs can be open on a predefined setpoint to relief pressure, LTs measure the level in a vessel or tank, and gas detectors discover the presence of gas and initiate an alarm at specified concentrations.

To assure the quality of the data, pre-processing of data is needed. Each failure maintenance notifications is reviewed and classified according to failure causes, failure modes, and detection methods. The failures were registered by operators and maintenance personnel, including both random hardware failures and systematic failures. It is suggested that systematic failures can be in failure rates estimations (SINTEF, 2013a). However, some reoccurring failures due to specific problems, such as icing problems and hydrate design problems have been removed to avoid invalid the impacts on the overall results. Such problems at one facility may not necessarily occur at other facilities. The classifications of equipment are predefined according to the suggestions of the experts. For example, the valves whose diameters are less than one inch are categorized into a separated group, since they are normally water-based and low-risk valves. Some assumptions are necessary in case of lack of data, for example, the valves installed in one particular system are assumed to share the same medium as the flow medium within the valves is not given.

3.2. Step 2: identification of significant influencing factors

The purpose of this step is to investigate the correlations between failures and influencing factors, and to identify significant influencing factors based on the data-driven models. Significant influencing factors are referred to as the factors that highly affect the performance of equipment.

³ PSVs are non-instrumented equipment, but they are considered for the data collection since some reliability handbooks for SIS include data for such equipment.

PCA has been selected to identify gross correlations in data, and give an overview of the distribution of the DU failures, correlations between DU failures (e.g. occurrence of DU failures, failure modes) and influencing factors (e.g. equipment attributes, maintenance, environmental factors). As shown in Fig. 3, PLSR is applied to find quantitative correlations between equipment performances (e.g. time to DU failure) and the same influencing factors. PCA models are concerned with the occurrence of DU failures and failure modes, while PLSR models are mainly related to time to DU failure. Both models contribute to the identification of significant influencing factors, and investigate more on the correlations between failures and factors.

3.3. Step 3: failure rates prediction

The purpose of this step is to predict failure rates of SIS equipment at a new facility based on experiences from comparable facilities. A user-provided failure rate for DU failures is denoted as λ_{DU} . This failure rate can be split into i groups according to different failure modes:

$$\lambda_{DU} = \lambda_{DU,1} + \lambda_{DU,2} + \dots + \lambda_{DU,i} \quad (1)$$

where $\lambda_{DU,i}$ is the failure rate according to the failure mode i . θ_j ($j = 1, 2, \dots, k$) denotes the weight of the significant influencing factor j , meaning its importance to the failure rates $\lambda_{DU,i}$. The weight θ_j can be determined based on either the analysis in step 2, such as regression coefficients and correlation analysis or the experience from the experts.

Then, the score σ_j for the influencing factors can be determined by comparing the new conditions and existing conditions. The scores represent the impact of the significant influencing factors. For example, when $\sigma_j = 1$, the influencing factor j is supposed to be in the medium state according to failure rates $\lambda_{DU,i}$. When $\sigma_j > 1$, the impact from influencing factor j is more hostile than the existing condition. When $\sigma_j < 1$, the impact is considered more benign than the existing condition. Similar studies have been discussed by many authors (Brissaud et al., 2010; Rausand, 2014; Vatn, 2006). The predicted failure rates are then estimated by:

$$\lambda_{DU}^* = \sum \theta_j \cdot \sigma_j \cdot \lambda_{DU,i} \quad (2)$$

Failure rates are then obtained by using Equations (1) and (2).

4. Case study

In this section, a case study is used to illustrate the proposed framework for the prediction of failure rates. The content of this paper is based on the works of the PDS project. We focus on the shutdown valves and use the analysis of equipment attributes as examples. Other influencing factors like the operational activities of the end-user or maintenances, may also have important influences on the failure rates.

4.1. Step 1: data-collection

The data stem from the six offshore and onshore facilities in the Norwegian oil and gas industry, involving 12788 equipment items and more than 13000 failures. A number of influencing factors can be taken into account, but we mainly focus on equipment attributes here since they are demonstrated important in explaining the variance of experienced reliability performance of the SIS equipment.

The data regarding the failures and equipment attributes is derived from maintenance notifications, work orders and relevant documentation, such as safety requirement specifications (SRs), process and instrument diagrams (P&IDs), safety manuals and safety analysis reports (SARs) and manufacturer specifications. Discussions with technical advisors and process engineers have also been included. For example, the flow medium for shutdown valves in the separation and stabilization system has been checked in P&ID manually and discussed with the experts. Some failure records are illustrated in Table 1. Shutdown

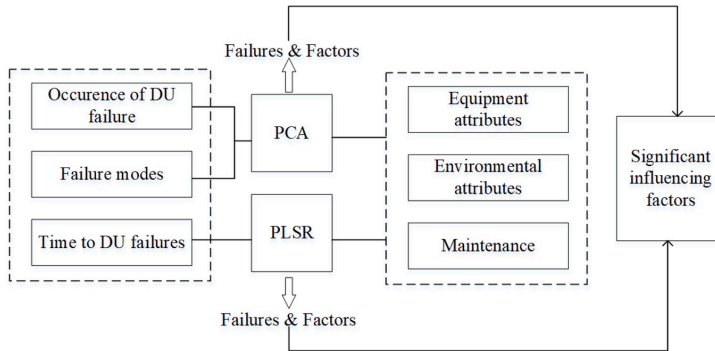


Fig. 3. Flowchart for identifying significant influencing factors.

Table 1
Examples of failure notifications.

Comp.	Notification	Functional loc.	Failure mode	Detection method	Description	Comments
PSD valve	*	*	FTC	Proof test	The valve fails under function test	Valve went to 40% opening at closing. Rust actuator and spring.
ESD valve	*	*	DOP	On-demand	Error of feedback	The too long closing time during the function test
PSD valve	*	*	DOP	Proof test	Check opening and closing time for valve	Closing time is 56 s
...

valves mainly have three types of DU failure: fail to close (FTC), leakage in closed position (LCP), and delayed operation (DOP) (ISO14224, 2006).

Table 2 and Table 3 present a summary of the failure data and equipment attributes. The equipment attributes, i.e. manufacturers, size, flow medium and type of the shutdown valves, are included in the analysis.

Table 4 illustrates an example of the shutdown valves used in data analysis. For example, No. 1 valve has survived and No. 4 valve has failed during the surveillance time.

4.2. Step 2: identification of significant influencing factors

PCA and PLSR are possible methods to identify significant influencing factors for shutdown valves in this section. The results are visualized by the software called “The Unscrambler X”, but it should be noted that similar analyses can also be realized in Matlab or R.

Each possible influencing factor is defined as a variable. The samples here are shutdown valves, which are distributed in the variable space. By application of PCA, a set of possibly correlated variables are converted into a set of linear uncorrelated variables. Then, the dimension of the multivariate variables is reduced to principal components (PCs) with a minimal loss of information. The samples are projected by using PCs with the largest explained variance. Fig. 4 shows the correction loadings plot. The explained variance now tells us how much information attribute to each of the PCs when high dimensional space is converted to low dimensional space. In Fig. 4, PC1 contains 12% of the variance and the PC2 contains 10% of the variance. The loading plot is used to understand the correlation between the variables, as illustrated in Fig. 4. “DU_NO” stands for a situation where DU failures are not

revealed, while “DU_YES” stands for a situation where DU failures are revealed during surveillance time. There is a distinction between “DU_NO” and “DU_YES” along PC2. The valves with DU failures are allocated in third and fourth quadrants, illustrating the distribution of DU failures. The score plot indicates how the samples are distributed along with PCs. By comparing Figs. 4 and 5, we can recognize the correlation between the grouped influencing factors and DU failures. In Fig. 5, the extremely large and large valves are also distributed in the third and fourth quadrants, meaning they are more likely to be subject to DU failures than the rest of the valves. The valves with gas and chemical flow medium are more exposed to DU failures compared to the other valves.

By introducing failure modes, e.g. DOP, FTC, LCP, in the analysis, the variance of PC1 and PC2 rises to 17% and 14% respectively. As shown in Fig. 6, failure mode DOP is close to “extreme” and “gas”, meaning that the failure mode DOP and extreme large-sized valves with gas flow medium are clustered. This implies that these valves are more exposed to DU failures with the failure mode DOP.

Fig. 7 and Fig. 8 show the analysis results from the PLSR analysis. The predicted plot is used to describe the correlations between time to DU failure and the influencing factors. R-squared gives the goodness-of-fit of the model. Time to DU failure is poorly predicted in Fig. 7 since R-squared is rather small and there is a big deviance between predicted regression lines (red validation line and blue calibration line) and target line (black reference line). Fig. 8 illustrates the weight regression coefficients providing information about the importance of the influencing factors. The influencing factors with a large regression coefficient play an important role in the regression model. In this case, some influencing factors like size (e.g. extremely large), flow medium (e.g. water, multiphase) and type of valves (e.g. ball and gate) can still be

Table 2
Failure data for the four groups of equipment.

Equipment Group	No. of equipment	Total operational time (hours)	No. of DU failures	Experienced failure rates (per 10 ⁶ hours)
Shutdown valves	1646	3.7·10 ⁷	292	7.9

Table 3
Equipment attributes for the shutdown valves.

Type	Ball	Controls flow by rotating a perforated and pivoting ball, poor methanol resistance in O-rings and deposits.
	Gate	Opens and closes by lifting or putting a gate out/down of the path of the fluid. Precipitation and abrasion are typical problems.
	Butterfly	Regulates or isolates flow by a damper.
	Others	Other types, e.g. globe valves
Size	Small-sized	0–1 inch
	Medium-sized	1–3 inches
	Large-sized	3–18 inches
	Extreme large-sized	> 18 inches
Flow medium	HC liquid	Oil and condensate (hydrocarbon) liquid
	Diesel	Diesel fuel.
	Chemical	Chemical medium in chemical injection system e.g. H ₂ S, Oxygen and some in methanol injection system e.g. 90% MEG with 10% water
	Multiphase	A mixture of different flow medium, e.g. a mixture of hydrocarbon, water, and sand
	Water	Freshwater with normal temperature and produced water with high temperature
	Seawater	Used for a fire water system and is characterized by salt
	Gas	HC gas or HC vapor in gas compression and re-injection systems, gas treatment systems, gas export metering systems, heating medium systems, etc.
Manufacturer	Manufacturers	E.g. P, B ... (anonymized)

Table 4
Examples for the analyses.

No.	Time (hours)	DU Failures	Type	Dimension	Flow Medium	Manufacturer
1	96456	DU_NO	Ball	Large	HC Liquid	P
2	96456	DU_NO	Ball	Medium	Others	P
3	96456	DU_NO	Ball	Large	Others	B
4	624	DU_YES	Ball	Large	Others	P
5	96456	DU_NO	Ball	Medium	Gas	B
...

Note: "DU_YES" – DU failures are revealed and "DU_NO" – No DU failure is revealed.

found as significant with respect to the failure rates.

To sum up, we conclude that in our case study DU failures are correlated with the most significant influencing factors, e.g. size and flow medium. Extremely large-size and flow medium (i.e. gas) are critical for some particular failure modes like DOP. That is why the two influencing factors, i.e. size and flow medium are mainly concerned in the following subsection.

4.3. Step 3: failure rates prediction

Based on operational experiences, we intend to predict failure rates of the shutdown valves installed a new facility. The user-provided failure rates in our case study are based on 1646 shutdown valves and 292 DU failures in total. The failures rate is estimated as the maximum likelihood estimator by $7.9 \cdot 10^{-6}$. The corresponding confidence interval is given by $[7.2 \cdot 10^{-6}, 8.9 \cdot 10^{-6}]$. Table 5 lists the DU failures and associated rates λ_j per failure mode for the shutdown valves.

As discussed in the previous section, two significant influencing factors need to be taken into account in predicting failure rates, i.e. size and flow medium of the valves. The weight θ_{ij} reflects the influence on failure rates from each influencing factor according to the failure modes, which is determined by experts based on the analysis results from PCA and PLSR. The score σ_{ij} is determined by comparing new conditions and existing conditions. The relevant assumptions and prediction results are shown in Table 6. Due to changes in operational conditions, the failure rate can be calculated by Eq. (1) and Eq. (2) and the predicted failure rate decrease by 5% to 8.8 per 10^6 hour, lower than the predicted result by using Brissaud's method (9.3 per 10^6 hour) under the same assumptions. The difference between the two predicted results can be explained by obtaining more information about correlations between significant influencing factors and the failure modes from the

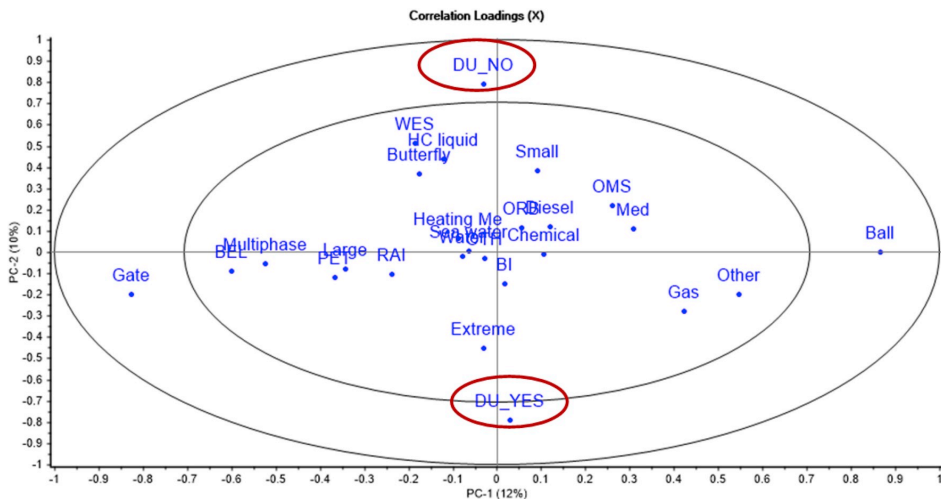


Fig. 4. Correlation loading plot for the first and second PCs in PCA.

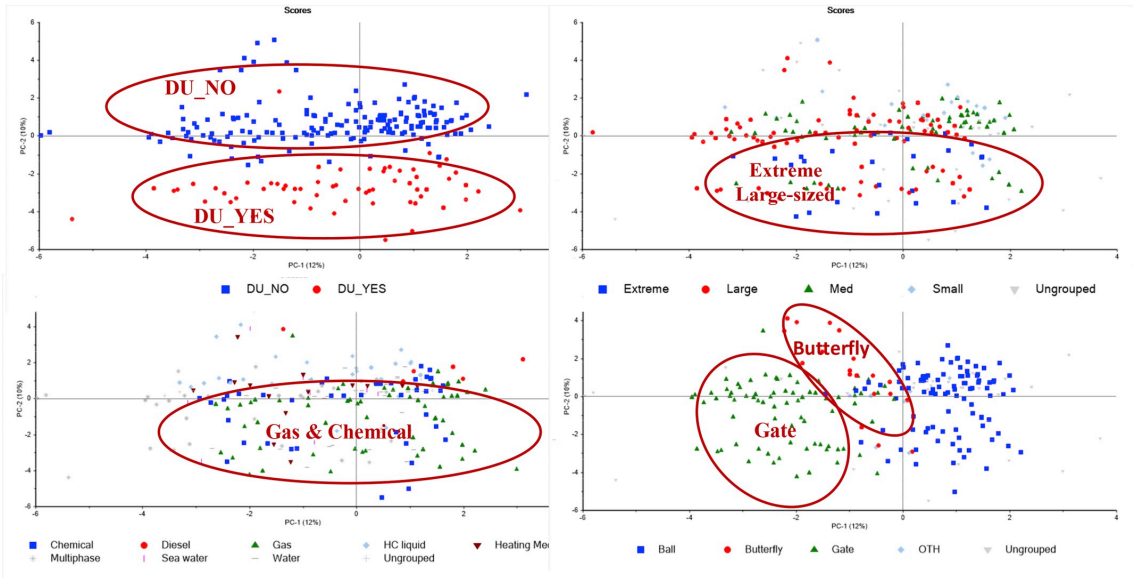


Fig. 5. Score plot of the first and second PCs in PCA.

PCA and PLSR analysis. It is illustrated that changes in the influencing factors may affect some specific failure modes, rather than all failure modes. Thus, it is more reasonably to predict failure rates for the specific failure modes of the shutdown valves.

5. Conclusions, discussions and further work

The main contribution of this paper is the proposed framework for identifying influencing factors and predicting failure rates of SIS equipment. The framework combines data-driven models i.e. PCA and

PLSR, and statistical models for predictions of failure rates. The methods help us to identify the most important significant influencing factors on failure rates, and to decide on the weights and scores of identified influencing factors based on the analysis results from PCA and PLSR.

Such a framework has been illustrated with a case study involving operational experiences reported for the shutdown valves at six oil and gas facilities. The results suggest that the size and the flow medium through the valves are the most significant influencing factors. The case study also illustrates how the framework is utilized to predict the failure

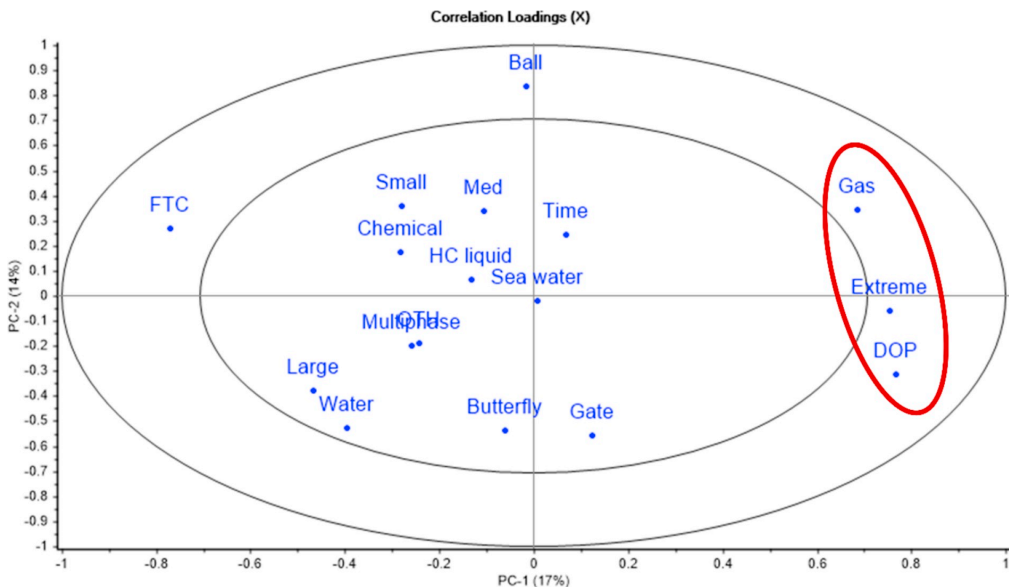


Fig. 6. Correlation loading plot of the valves in PCA with failure modes.

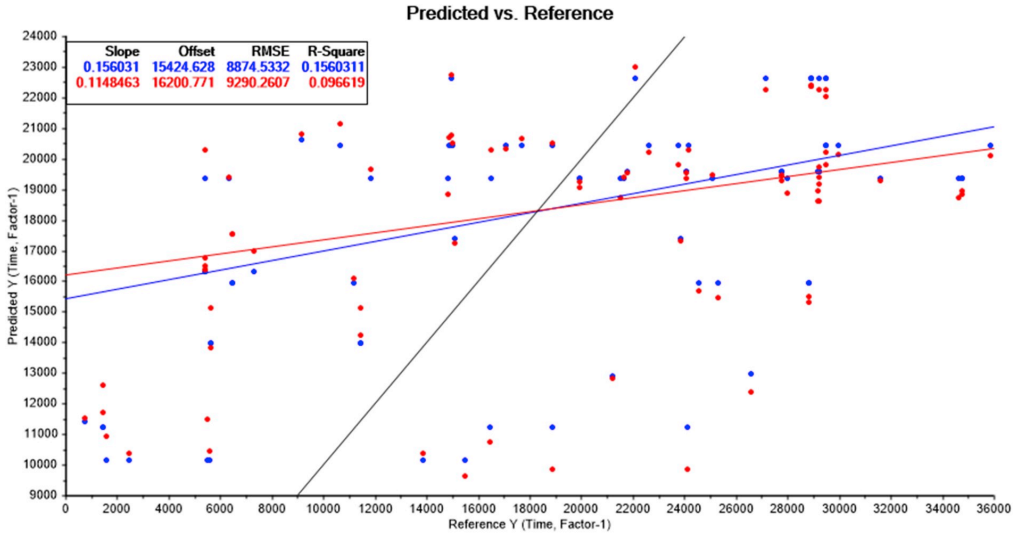


Fig. 7. Predicted plot of the shutdown valves in PLSR.

rates for equipment at a new facility. It can be the basis for reliability improvement programs, optimizing maintenance programs and suggesting subcategories within equipment groups. Prediction of failure rates is the start of risk assessment and the calculation of PFD (Famuyiro, 2018).

Many factors will affect the accuracy of the analysis. The biggest challenge comes from the quality of data, such as lack of data, missing information. Another limitation is the choice of predefined categories for equipment (i.e. attributes) and failures (e.g. failure modes). The selection of these categories strongly depends on the experts' opinion and the information available in the data. The data applied in the case study to identify significant influencing factors is restricted to time to DU failure. This time may be underestimated since DU failures are not revealed immediately. Constant failure rates are also assumed in this paper, which only applies to the failures during the useful life period of operation. Thus, we have disregarded any changes in failure rates

Table 5

Failure distributions and corresponding failure rates.

Failure mode	No. of DU	Weights	Failure rates $\lambda_{DU,i}$ (per 10^6 hour)
DOP	152	52.0%	4.1
FTC	101	34.6%	2.7
LCP	16	5.5%	0.4
OTH*	23	7.9%	0.6
Total	292	100%	7.9

Note*: OTH represents other failure modes and unknown failure modes.

during early life and end-of-life.

Further research should involve the comparisons of the effects of different significant influencing factors on various SIS equipment groups to mitigate DU failures. It is relevant to study other influences,

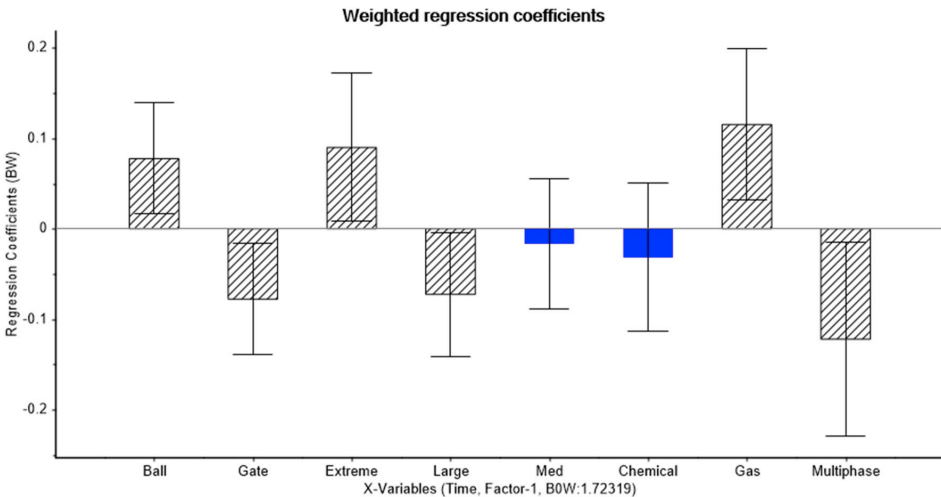


Fig. 8. Weighted regression coefficients of the influencing factors in PLSR.

Table 6
Comparison of the distribution for subcategories.

Brissaud's method				Proposed method in this paper						
λ_{DU} (per 10 ⁶ hours)	Significant Influencing factors	$\hat{\theta}_j$	σ_j	$\lambda_{DU,i}^*$ (per 10 ⁶ hours)	Failure mode	$\lambda_{DU,i}$ (per 10 ⁶ hours)	Significant influencing factors	$\hat{\theta}_{ij}$	σ_{ij}	$\lambda_{DU,i}^*$ (per 10 ⁶ hours)
7.9	Size	0.6	1.5	7.1	FTC	4.1	–	–	–	4.1
	Flow medium	0.4	0.7	2.2	DOP	2.7	Size	0.6	1.5	3.2
								Flow medium	0.4	0.7
					LCP	0.4	–	–	–	0.4
					OTH	0.6	–	–	–	0.6
Prediction			9.3							8.8

such as installation, maintenance and general safety culture, on the prediction of failure rates. Root cause analysis could also be incorporated in the proposed framework from the beginning of the quantification of influencing factors. Other alternative methods, like dynamic principal component analysis and or machine learning, can be considered and their effectiveness needs to be analyzed. Development of a guide for failure rate prediction is also required from an end-users perspective, including validation of predicted values with experienced failure rates. Another issue to be considered is to perform analyses to predict dynamic failure rates in the operation.

Acknowledgment

Thanks to all the participants of the PDS forum (www.sintef.no/pds) that have contributed with data, valuable information, operational experience, expert judgments, and suggestions. Particularly, thanks to SINTEF that have contributed with their knowledge, comments, and discussions. The authors are also pleased to thank the anonymous reviewers for their thoughtful, constructive comments.

Appendix

PCA

PCA is based on the statistic model proposed by Pearson and Hotelling (Hotelling, 1933; Jolliffe, 2011; Pearson, 1901). Such a method can reduce the dimensionality of multivariate to principal components (PCs) with minimal loss of information. In the context of this paper, PCA is used to reduce the dimensionality of the influencing factors, so that significant influencing factors are retained and essential correlation is analyzed more easily.

Influencing factors are defined as the explanatory variables and expressed as $X = [X_1, X_2, \dots, X_n]^T$. Assume m samples of equipment that describe the observed situation relating to various influencing factors and the states of DU failures. ‘1’ represents a situation where a DU failure is detected, whereas ‘0’ represents that there is no DU failures. The matrix X is decomposed into a score matrix $T = [t_1, t_2, \dots, t_n]$ and a loading matrix P :

$$X = TP^T + \bar{E} \tag{3}$$

where \bar{E} denotes the residual matrix. The score T shows how the DU failures are distributed and how they project along the orthogonal PCs. The loading P reflects the correlations between PCs. Then, the covariance matrix can be expressed as:

$$S = \frac{1}{N - 1} X^T X \tag{4}$$

The Eigen-decomposition is performed on S to obtain loading matrix P . The Eigenvalues V are denoted as:

$$V = [v_1, v_2, \dots, v_l] \tag{5}$$

Then, the i th eigenvalue v_i , relates to the i th column of the score matrix T :

$$v_i = \frac{1}{n - 1} t_i^T t_i \tag{6}$$

The highest eigenvalues represent the PCs with the most information and the measurement of the residuals is conducted to contain less covariance.

PLSR

Similarly, PLSR decomposes X and Y matrices into bilinear structure models consisting of scores and loading matrices. The influencing factors are defined as the explanatory variable expressed by $X = [X_1, X_2, \dots, X_n]^T$. The response variables $Y = [Y_1, Y_2, \dots, Y_n]^T$ represents here the time to DU failures. X and Y project from high dimensional spaces to low-dimensional spaces as follows:

$$X = TP^T + \bar{E} \tag{7}$$

$$Y = TQ^T + \bar{F} \tag{8}$$

where $T = [t_1, t_2, \dots, t_l]$ are the score vectors, $P = [p_1, p_2, \dots, p_l]$ and $Q = [q_1, q_2, \dots, q_l]$ are the loading for X and Y . \bar{E} and \bar{F} are PLS residuals corresponding to X and Y . The loading weights of P and Q reflect the correlations between X and Y with the purpose of prediction. Then, the PLSR mode can be rewritten as:

$$U = f(T) + \bar{F}^* \tag{9}$$

where U is a matrix that represents score vectors when Y projects to T . \tilde{F}^* denotes the combined residuals from the decomposition. In this study, the nonlinear iterative PLS (NIPALS) algorithm is used. Once all significant components are extracted, the model can then be used to predict new data using the following relationship:

$$Y = TQ^T + \tilde{F} = XB + \tilde{F}^* \quad (10)$$

where B denotes a matrix of regression coefficients. More details of PLS algorithms can be found in the studies introduced by Geladi and Kowalski (1986) and Hoskuldsson (Höskuldsson, 1988).

References


- Becker, G., Camarinopoulos, L., 1990. A Bayesian estimation method for the failure rate of a possibly correct program. *IEEE Trans. Softw. Eng.* (11), 1307–1310.
- Brissaud, F., Charpentier, D., Fouladirad, M., Barros, A., Bérenguer, C., 2010. Failure rate evaluation with influencing factors. *J. Loss Prev. Process. Ind.* 23 (2), 187–193.
- Cox, D.R., 1972. Regression models and life-tables. *The Royal Statistical Society: Ser. Biolog.* 34 (2), 187–202.
- Elsayed, E., Chan, C., 1990. Estimation of thin-oxide reliability using proportional hazards models. *IEEE Trans. Reliab.* 39 (3), 329–335.
- EXDIA, 2007. Safety Equipment Reliability Handbook. exdia.com, Sellersville, PA.
- Famuyiro, S., 2018. Use of combustible gas detectors in Safety Instrumented Systems—A practical application case study. *J. Loss Prev. Process. Ind.* 54, 333–339.
- Foucher, B., Boullie, J., Meslet, B., Das, D., 2002. A review of reliability prediction methods for electronic devices. *Microelectron. Reliab.* 42 (8), 1155–1162.
- Geladi, P., Kowalski, B.R., 1986. Partial least-squares regression: a tutorial. *Anal. Chim. Acta* 185, 1–17.
- GL070, 2004. Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry. Stavanger, Norway. Norwegian Oil Industry Association.
- Håbrekke, S., Hauge, S., Hoem, Å.S., Lundteigen, M.A., Xie, L., 2017. Modified generic failure rates for safety instrumented systems based on operational experience from the oil and gas industry. In: *European Safety and Reliability Conference Proceedings, Portorož, Slovenia*.
- Håbrekke, S., Hauge, S., Xie, L., Lundteigen, M.A., 2018. Failure rates of safety critical equipment based on inventory attributes. In: *European Safety and Reliability Conference Proceedings, Trondheim, Norway*.
- Hauge, S., Lundteigen, M.A., 2008. Guidelines for Follow-Up of Safety Instrumented Systems (SIS) in the Operating Phase. SINTEF, Trondheim, Norway.
- Höskuldsson, A., 1988. PLS regression methods. *J. Chemom.* 2 (3), 211–228.
- Hotelling, H., 1933. Analysis of a complex of statistical variables into principal components. *J. Educ. Psychol.* 24 (6), 417.
- IEC60050, 1990. International Electrotechnical Vocabulary. International Electrotechnical Commission, Geneva.
- IEC61508, 2010. Functional Safety of Electrical/electronic/programmable Electronic Safety-Related Systems. International Electrotechnical Commission, Geneva.
- IEC61511, 2016. Functional Safety-Safety Instrumented Systems for the Process Industry Sector. International Electrotechnical Commission, Geneva.
- IEC61709, 2017. Electronic Components—Reliability—Reference Conditions for Failure Rates and Stress Models for Conversion. International Electrotechnical Commission, Geneva.
- ISO14224, 2006. Petroleum, Petrochemical and Natural Gas Industries: Collection and Exchange of Reliability and Maintenance Data for Equipment. International Organization for Standardization, Geneva.
- Jolliffe, I., 2011. Principal component analysis. In: *International Encyclopedia of Statistical Science*. Springer, Berlin, Heidelberg, pp. 1094–1096.
- Kutyłowska, M., 2015. Neural network approach for failure rate prediction. *Eng. Fail. Anal.* 47, 41–48.
- Li, G., Qin, S.J., Yuan, T., 2016. Data-driven root cause diagnosis of faults in process industries. *Chemometr. Intell. Lab. Syst.* 159, 1–11.
- MIL-HDBK-217F, 1995. Reliability Prediction of Electronic Equipment. U.S. Department of Defense, Washington, DC.
- Newby, M., 1994. Perspective on Weibull proportional-hazards models. *IEEE Trans. Reliab.* 43 (2), 217–223.
- OREDA, 2015. Offshore and Onshore Reliability Data Høvik, Norway: OREDA Participants.
- Pearson, K., 1901. LIII. On lines and planes of closest fit to systems of points in space. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 2 (11), 559–572.
- Qin, S.J., 2012. Survey on data-driven industrial process monitoring and diagnosis. *Annu. Rev. Contr.* 36 (2), 220–234.
- Ratkowsky, D., Olley, J., McMeekin, T., Ball, A., 1982. Relationship between temperature and growth rate of bacterial cultures. *J. Bacteriol.* 149 (1), 1–5.
- Rausand, M., 2014. Reliability of Safety-Critical Systems: Theory and Applications. John Wiley & Sons, Hoboken, New Jersey, USA.
- Rausand, M., Høyland, A., 2004. second ed. *System Reliability Theory: Models, Statistical Methods, and Applications*, vol. 396 John Wiley & Sons, Hoboken, New Jersey, USA.
- SINTEF, 2013a. Reliability Data for Safety Instrumented Systems, PDS Data Handbook. SINTEF, Trondheim, Norway.
- SINTEF, 2013b. Reliability Prediction Method for Safety Instrumented Systems, PDS Method Handbook. SINTEF, Trondheim, Norway.
- TelcordiaSR-332, 2001. Reliability Prediction Procedure for Electronic Equipment. Piscataway, N. J: Telcordia.
- Tidiri, K., Chatti, N., Verron, S., Tiplica, T., 2016. Bridging data-driven and model-based approaches for process fault diagnosis and health monitoring: a review of researches and future challenges. *Annu. Rev. Contr.* 42, 63–81.
- Vatn, J., 2006. Procedures for updating test intervals based on experience data. In: *The 30th ESReDA Proceedings, Ispra, Italy*.

Article IV

Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Reliability and barrier assessment of series-parallel systems subject to cascading failures. *Proceedings of the Institution of Mechanical Engineers. Part O, Journal of risk and reliability* (2020); Volume 234. (3) s. 455-469.

This page is intentionally left blank

Reliability and barrier assessment of series–parallel systems subject to cascading failures

Proc IMechE Part O:
J Risk and Reliability
2020, Vol. 234(3) 455–469
© IMechE 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1748006X19899235
journals.sagepub.com/home/pio


Lin Xie, Mary Ann Lundteigen and Yiliu Liu 

Abstract

Cascading failures can occur in many technical systems where the components are organized as in series–parallel structures. The failures in these systems may propagate from one component to the other, not only within the same parallel sub-structure but also between different sub-structures. This article presents a recursive aggregation method based on the extended models of reliability block diagram, for analyzing the impacts of cascading failures on the reliability of series–parallel systems. Based on the reliability analysis, the effects of safety barriers on preventing cascading failures are studied, and the importance of safety barriers at different locations is evaluated. One simple example of three components and one practical case from an oil production system are presented. The findings in these case studies illustrate how system designers and safety managers can identify the effective and reasonable ways of installing safety barriers by using the proposed approaches, for the mitigation of cascading failures in series–parallel technical systems.

Keywords

Cascading failure, series–parallel system, system reliability, reliability block diagram, safety barrier

Date received: 1 July 2019; accepted: 9 December 2019

Introduction

Dependent failures (DFs) often occur in technical systems, such as in railway signaling, in flow transmission, and in process plants.^{1–5} DFs refer to those failures occurring in more than one component, influenced or affected by either external or internal impacts, for example, hazardous events, environmental factors, shared resources, and dependent functions of different components.⁶ The term “DF” reflects a relationship between the state of one component and the states of other associated subsets or components in a system.

Two sub-categories of DFs are of specific interest: common cause failures (CCFs) and cascading failures (CAFs). The similarities and difference between CCFs and CAFs have been studied in Xie et al.⁷ Both failures can occur simultaneously and influence multiple components, leading to devastating consequences. However, CCFs are the multiple failures due to a shared cause, while CAFs are characterized by a chain reaction or a domino effect initiated by the failure of one component.³ Neither CCFs nor CAFs can straightforwardly be modeled by traditional reliability analysis approaches like fault tree or Markov method,^{8–11} and considerable researches have recently been devoted to

modeling and analyzing these failures with complexity. The models for CCFs can be broadly classified as: direct estimate models (e.g. square-root model^{8,9}), ratio models (e.g. β -factor model,¹⁰ C-factor model¹¹), and shock models (e.g. binomial failure rate model¹²). These models have been incorporated to the traditional reliability analysis approaches, such as fault tree analysis, Markov methods, and event tree analysis.

The mentioned approaches for CCFs are unfortunately not fully applicable for modeling CAFs, because the interdependence and propagation mechanisms in CCFs and CAFs are not the same.⁷ CAFs have been widely studied by using sequential and network-based approaches from risk-based assessment, complex network theory, and reliability analysis perspective. Since late 1990s, Khan and Abbasi have provided conceptual frameworks based on sets of models and computer-automated tools to assess CAFs as domino effect.^{13–16}

Norwegian University of Science and Technology, Trondheim, Norway

Corresponding author:

Yiliu Liu, Norwegian University of Science and Technology, 7491 Trondheim, Norway.
Email: yiliu.liu@ntnu.no

Based on these works, domino effect is lately described by the physics of cascaded process like escalation probability or domino effect frequency related to distance,¹⁷ threshold values,¹⁸ and probit methodology.¹⁹ Risk analysis associated with Markovian model,^{20–22} Bayesian network (BN),^{23,24} graph theory,^{25,26} and Monte Carlo (MC) simulation,^{27,28} have been used to quantify the impacts of CAFs or domino effect. Topological approaches motivated by the complex network theory have been utilized to analyze the impacts of CAFs on system connectedness and robustness.^{29–32} In the context of reliability analysis, numerous algorithms have been proposed for analyzing the effects of CAFs in redundant systems, for example, parallel systems and *k*-out-of-*n* (*koon*) systems. For example, Murthy and Nguyen have studied three types of relevant failures on parallel systems in stochastic models: induced failure, shock failure, and their combinations.^{1,33} Redistribution of loads that can result in CAFs is also discussed in consideration of *koon* systems,^{34,35} where the functioning of *k* channels in *n* parallel ones can ensure the system functioning. Recently, some approaches like stochastic filtering and fault tree analysis have been proposed to address stochastic dependency issues including degradation dependencies and structural redundancy.^{36,37} In addition, CAFs in multistate or network systems are paid more attention. Levitin and Xing have analyzed the performance of discrete multistate systems considering the global and selective effects of CAFs.^{5,38–41} In Fricks and Trivedi,⁴² stochastic Petri nets and continuous time Markov chains are adopted to study the effects of CAFs on reliability. Tsilipanos has developed a system of systems framework for analyzing CAFs of telecommunication networks based on Bayesian network model.⁴³

In a short, the existing literatures on CAFs have analyzed the sequence-based, network, redundant and multistate systems. However, in practices, it is very common that technical systems are designed for functionality. The realization of system function is through those sub-functions in series–parallel structures, which can be described as a success-oriented model, namely reliability block diagram (RBD). The reliability of a technical system is concerned with the probability that system functionality can be performed well within a specified period of time. Therefore, system reliability is not only determined by the number of survival components in the system, but also related to functional structure of the system.³

It is also noteworthy that, in a series–parallel system, failures may propagate not only within the same parallel sub-structure but also between different sub-structures in series. Such a kind of propagation brings multiple possibilities of cascading failures in series–parallel systems, and challenges the current analysis approaches. Therefore, the first objective of this study is to develop an approach for evaluating the impacts of CAFs on the reliability of series–parallel systems with certain functionality.

Moreover, given that CAFs can endanger a system, it makes senses to explore how to protect the system and enhance the reliability of series–parallel systems. Safety barriers are necessary to be installed against CAFs to avoid accidents.³⁷ In the accidental risk assessment methodology for industries (ARAMIS) project report, safety barriers have been considered in risk assessment of domino effect, including identification, frequency assessment, consequence assessment, and risk calculation.^{44,45} Similar efforts have also been devoted to introduce safety barriers in cascading control and mitigation in complex networks.^{46–49} A framework proposed by Reniers and Cozzani²¹ has been used to allocate protective safety barriers. A decision model has been proposed to allocate protective safety barriers and mitigate domino effect in Janssens et al.⁵⁰ Chen et al.⁵¹ also suggested a sequence-based method considering economic losses, casualties, and pollution to allocate security measures and safety barriers for reducing the risk of intentional attacks. Quantitative assessment of safety barrier performances, such as time to failure and activation time, has been developed in the prevention of fire escalation.¹⁷

Despite the above researches, few of them has focused on the effects of barriers against CAFs in the context of the system reliability analysis. The second objective of this article is thus to propose reliability-based approach for investigating the effects of barriers against CAFs. It is expected that the approaches presented in this article can support the designers and operators to determine the effective and reasonable ways of deploying safety barriers. Especially when the resources are limited, the mitigation of cascading failures should be conducted in a cost-effective way.

The rest of the article is organized as follows. Section “Definitions, assumptions and specifications” presents the definitions and the assumptions in terms of CAFs and safety barriers. In section “RBD-based recursive aggregation approach,” we elaborate the reliability analysis and barrier analysis approaches considering CAFs in series–parallel systems. Section “An illustrative example” and section “Case studies for preventing CAFs in oil and gas production” introduce two examples to illustrate the approaches in analyzing the effects of CAFs and safety barriers. Conclusions and further works are discussed in section “Conclusion and future works.”

Definitions, assumptions, and specifications

Definitions of CAF and safety barrier

It is helpful to clarify the concepts of CAFs and safety barriers for further quantitative analysis, in consideration of the existence of arguments on these topics. From the perspective of probability theory, DFs have been regarded as the failures whose probability cannot be expressed by the simple unconditional failure

probabilities of the individual events.⁵² On the contrary, independent failures, or self failures are the failures with the occurrence probabilities not affected by other components.¹¹ For example, an age-related failure occurs on a component itself, irrelevant with whether other components fail or not. Meanwhile, even though an independent/self failure of one component is not a result of other failures, it can influence other components and act as a starting point of more failures.

CAFs are referred to as a subcategory of DFs but are identified in literature by the similar terms with a different focus, such as induced failures, domino failures, propagated failures and interaction failures.^{1,22,53} For example, Murthy and Nguyen¹ have called them as induced failures and emphasized the failure probability caused by the other components within the systems. Rausand and Høyland³ have regarded CAFs as multiple failures associated with a chain reaction or domino effect. CAFs have been called as escalating failures in the SINTEF report, that is, failure mode of one or more component initiates failure in other components.⁵⁴ The term CAFs (or domino effect) has also been used to denote a chain of accidents or situations when a fire/explosion/missile/toxic load generated by an accident in one unit causes secondary and higher order accidents in other units.^{13,14}

Despite of the differences existing in defining CAFs, we keep this article in the commonly accepted area, where CAFs are regarded as multiple failures that originate from independent failures of some components and then propagate to the other components. In Figure 1(a), dotted curves with arrows are used to denote the propagation paths of CAFs. For example, the curve from component 1 to component 3 means the failure of the former can result in the failure of the latter, or at least increase its failure probability.

In terms of safety barriers, they are known as countermeasures, defenses, lines of defense, layers of protection, and safeguards in different regulations, standards, and literature.⁶ Safety barriers are defined as the physical or non-physical means to prevent, control, or mitigate undesired events or accidents.⁵⁵ In this article, we

emphasize those physical means installed to stop or mitigate the effects of CAFs. Such barriers are a kind of add-on barriers that refer to the added systems or components because of their safety considerations.⁵⁶ They are introduced on the logical or physical paths of failure propagations to intervene in to the interdependencies between components, as the crosses are shown in Figure 1(b).

It is noted that the safety barriers considered here do not perform the main or essential system functions, but they carry out protective functions. Take a separation system of process fluids as an example: firewalls are added to section the process area in case of a fire, which can prevent fires from spreading from one part to another. Shutdown valves can play a similar role, that is, to prevent the propagation of fire in one area to the next.

Delimitations and assumptions in the CAF analysis

We will analyze the impacts of CAFs and safety barriers on the reliability of series-parallel systems, based on the definitions given in the last subsection. It is necessary to mention the delimitation of analysis, and the assumptions to be noted:

1. For any components in a system, only two states are taken into account: functioning or completely failed.
2. Independent/self failures and CAFs are considered. All components are subject to both types of failures.
3. Independent/self failure of any component can trigger one or multiple CAFs, but second-order or higher order effects of CAFs can be ignored considering the extremely low occurring likelihood and small impacts on the system reliability.
4. Time to an independent/self failure on any component follows the exponential distribution, with a probability of $F_{T_i}(t)$, and a constant failure rate λ . It should be noted that other distributions like Weibull distribution, can also be considered.

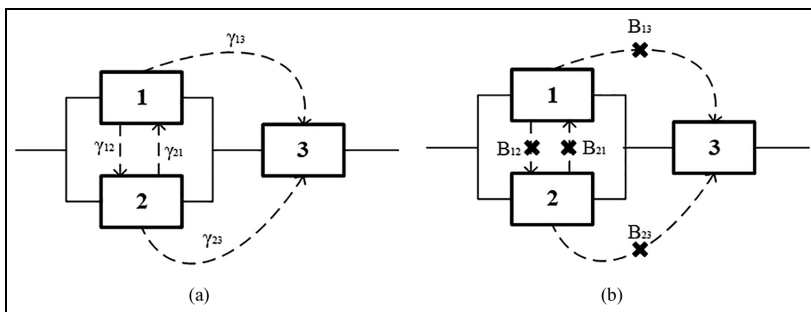


Figure 1. RBD with CAFs and corresponding barriers of example 1: (a) Dotted curves with arrows r_{ij} denote propagation paths of CAFs and (b) crosses B_{ij} the barriers installed on the path of failure propagation between components i and j .

5. Failure propagation is possible from one component to others under the condition that the system is still working.
6. Failure propagation time of CAFs from one component to the other is very short and negligible.
7. All the barriers are perfectly reliable and independent, meaning that they can always intervene in failure propagations once they are installed.

In addition, it should be noted that repairs and restorations after any failure is not considered in this article.

Specifications of CAF modeling

As shown in Figure 1(a) and (b), a RBD can be used to describe the structure of a system. Such a commonly used reliability analysis model is extended in this article, by introducing cascading paths as dotted curves with arrows. The following specifications are made in terms of CAFs based on the extended RBD:

1. A measure of cascading probability $\gamma_{ij}(t) \in [0, 1]$ ($\forall i, j \in \Omega, i \neq j$) is introduced to denote the easiness of failure propagation. It is defined as the failure probability of component j in case that component i has failed

$$\gamma_{ij}(t) = \Pr(\text{comp. } j \text{ fails by time } t | \text{comp. } i \text{ has failed by time } t) \tag{1}$$

2. The cascading probability $\gamma_{ij}(t)$ can be estimated based on test data or historic failure records by either parametric or nonparametric techniques. For the sake of simplification, $\gamma_{ij}(t)$ is assumed to be a constant representing cascading probability between components i and j in this article, denoted as γ_{ij} . The cascading probabilities between different components are illustrated in a matrix $\Gamma(\gamma_{ij})$

$$\Gamma(\gamma_{ij}) = \begin{bmatrix} 0 & \cdots & \gamma_{1n} \\ \vdots & \ddots & \vdots \\ \gamma_{n1} & \cdots & 0 \end{bmatrix} \tag{2}$$

3. The escaping probabilities that the components can escape from CAFs ($\bar{\gamma}_{ij} = 1 - \gamma_{ij}$) are illustrated in a matrix $\bar{\Gamma}(\bar{\gamma}_{ij})$.

RBD-based recursive aggregation approach

In order to evaluate the effects of CAFS, a RBD-based recursive aggregation approach is proposed in this section. Such an approach is developed based on the work of Liu et al.³⁴ with significant extension, since in that work only purely parallel systems are studied and their

system performances are measured relying on the number of survival components. In this article, the presented approach is able to evaluate the impacts of CAFs on more general structures, namely series-parallel ones, as well to assess the effectiveness of barriers. This approach is expected to be applicable for analyzing the systems with a number of components considered as cause of CAFs.

Reliability analysis of a system with CAFs

Consider a series-parallel system with n components. The reliability of such a system can be obtained by an approach using a RBD associated with minimal path sets (MPSs). Path sets are defined as a set of functioning components to ensure that the system is working.¹¹ As long as there is at least one logical path between functioning components, the system survives. A path set is said to be minimal if any component in a path set cannot be reduced without losing the function of the system. In this article, totality of MPSs of a system are denoted as $\mathbf{MPS} = \{\text{MPS}_1, \text{MPS}_2, \dots, \text{MPS}_p\}$. It can be found that MPSs of example 1 include $\text{MPS}_1 = \{1, 3\}$ and $\text{MPS}_2 = \{2, 3\}$, as shown in Figure 1(a).

As mentioned in section “Delimitations and assumptions in the CAF analysis,” a series-parallel system is subjected to independent/self failures and CAFs. Each independent/self failure may lead to CAFs that propagate between one component and other functioning components within the system. At the system level, let $F_S^c(t)$ represent the failure probability of system $\Omega(\Omega = [1, 2, \dots, n])$ considering CAFs. According to the total probability law, the failure probability can be calculated as

$$F_S^c(t) = \sum_{i \in \Omega} F_{S,i}^c(t) = \sum_{i \in \Omega} [P_r(\text{system fails} | F_{ii}) \cdot P_r(F_{ii})] \tag{3}$$

where $F_{S,i}^c(t)$ is the probability of system failure in case that the component i has failed at first and component $i \notin \mathbf{MPS}$. $P_r(F_{ii})$ is the probability of the event that component i fails due to a independent/self failure. The independent/self failure on the component i can propagate CAFs. Then, the probability of system failure $F_S^c(t)$ can be expressed as

$$F_S^c(t) = \sum_{i \in \Omega} \int_0^t F_{\Omega-i}(t_i, t) \prod_{j \neq i, j \in \Omega} R_j(t) dF_{ii}(t_i) \tag{4}$$

where t_i is the time to a independent/self failure of component i . When component i has failed, the system can be viewed as re-configured by removing the component i from the old system. In other words, the new system without component i can be regarded as a subsystem of the old one. The failure probability of subsystem $\{\Omega - \{i\}\}$ is denoted by $F_{\Omega-\{i\}}(t_i, t)$ in $[t_i, t]$. The failure propagation is conditioned that the failures can be propagated from component i and the system is

functioning at the time t_i . $R_j(t)$ is the reliability of component $j(\forall j \in \Omega - i)$ at time t .

Let $\Pr(n_c)$ denote the probability that the system are subject to n_c of CAFs. For example, $\Pr(n_c = 0)$ is the probability of the event of no cascading failure occurring ($\Pr(n_c = 0) = \prod_{j_1, j_2, \dots, j_{n_c} \neq i, j \in \Omega} \bar{y}_{ij_1} \bar{y}_{ij_2} \dots \bar{y}_{ij_{n_c}}$), where n_{ci} is the number of CAFs initiated from component i . If one failure propagates from component i to component j_1 , $\Pr(n_c = 1)$ represents the probability of the event with only one CAFs. $F_{\Omega - \{i, j_1\}}(t_i, t)$ is the failure probability of the subsystem $\{\Omega - \{i, j_1\}\}$. All the possible combinations of CAFs are considered. $F_{\Omega}(t_i, t)$ can be obtained by

$$\begin{aligned}
 F_{\Omega}(t_i, t) = & \Pr(n_c = 0)F_{\Omega - \{i\}}(t_i, t) \\
 & + \sum_{j_1 \in \Omega - \{i\}} \Pr(n_c = 1)F_{\Omega - \{i, j_1\}}(t_i, t) \\
 & + \sum_{j_1, j_2 \in \Omega - \{i\}} \Pr(n_c = 2)F_{\Omega - \{i, j_1, j_2\}}(t_i, t) + \dots \\
 & + \sum_{j_1, j_2, \dots, j_{n_c} \in \Omega - \{i\}} \Pr(n_c = n_{ci})F_{\Omega - \{i, j_1, \dots, j_{n_c}\}}(t_i, t)
 \end{aligned} \tag{5}$$

The subsystem $\Omega_m = (\forall \{\Omega - \{i\}, \Omega - \{i, j_1\}, \dots, \Omega - \{i, j_1, \dots, j_{n_{ci}}\}\})$. For example, considering the second independent/self failure occurring on the component $j(\forall j \in \Omega - \{i\})$ at time t_j , $F_{\Omega - \{i\}}(t_j, t)$ is the failure probability of subsystem $\{\Omega - \{i\}\}$ fails during $[t_j, t]$ with the condition that component j has failed and the system is working at time t_j . Since the occurrence of next failure is a Markov process, with a no-memory property, and t_i can be regarded as a new starting point for the new subsystems. The failure probability of the subsystem $F_{\Omega - \{i\}}(t_i, t)$ can therefore be expressed as

$$\begin{aligned}
 F_{\Omega - \{i\}}(t_i, t) = & \sum_{j \in \Omega - i} \\
 & \int_{t_j}^t F_{\Omega - \{i, j\}}(t_j, t) \prod_{k \neq i, j, k \in \Omega} R_k(t) dF_{ij}(t_j)
 \end{aligned} \tag{6}$$

For any subsystem Ω_m , $F_{\Omega_m}(t_m, t)$ can be deduced in a similar way as equations (4) and (5). Such recursive aggregations will stop:

1. When there is no MPS found in Ω_m . The corresponding failure probability of the subsystem is equal to 1;
2. When the subsystem Ω_m is one of MPSSs, such as $\text{MPS} = \{\text{MPS}_1, \text{MPS}_2, \dots, \text{MPS}_p\}$. The failure probability can be determined based on MPSSs.

To facilitate the integration of the failure probabilities, one can use convolution and Laplace transforms for equations (3)–(6).³ Laplace transforms for equation (4) can be expressed as

$$\mathcal{L}[F_{S, i^c}(t)] = \mathcal{L}[F_{\Omega - i}(t)] \frac{\lambda_i}{S + \lambda_1 + \dots + \lambda_n} \tag{7}$$

$$\mathcal{L}[F_{S^c}(t)] = \sum_{i \in \Omega} \mathcal{L}[F_{\Omega - i}(t)] \frac{\lambda_i}{S + \lambda_1 + \dots + \lambda_n} \tag{8}$$

Proof of equations (7) and (8) is given in Appendix 2. Similarly, Laplace transforms for equation (5) can be obtained

$$\begin{aligned}
 \mathcal{L}[F_{\Omega - i}(t)] = & \Pr(n_c = 0) \mathcal{L}[F_{\Omega - \{i\}}(t)] \\
 & + \sum_{j_1 \in \Omega - \{i\}} \Pr(n_c = 1) \mathcal{L}[F_{\Omega - \{i, j_1\}}(t)] \\
 & + \sum_{j_1, j_2 \in \Omega - \{i\}} \Pr(n_c = 2) \mathcal{L}[F_{\Omega - \{i, j_1, j_2\}}(t)] + \dots \\
 & + \sum_{j_1, j_2, \dots, j_{n_c} \in \Omega - \{i\}} \Pr(n_c = n_{ci}) \mathcal{L}[F_{\Omega - \{i, j_1, \dots, j_{n_{ci}}\}}(t)]
 \end{aligned} \tag{9}$$

By using inverting Laplace transforms, the failure probability of the system $F_{S^c}(t)$ can be obtained. Then, the system reliability should be expressed as

$$R_{S^c}(t) = 1 - \mathcal{L}^{-1}[F_{S^c}(t)] \tag{10}$$

In short, the system reliability can be obtained by applying the following steps:

- Step 1: Define the MPS of series-parallel systems based on RBD, and evaluate the failure probabilities of MPS as the first layer by using the Laplace transforms.
- Step 2: Incorporate one or more components into the MPSSs as new subsystems in the second layer, and evaluate the failure probabilities of the new subsystems.
- Step 3: Repeat step 2 to collect the failure probabilities of all possible subsystem in the upper layers until one reach to the system level with n components.
- Step 4: Obtain the failure probability $F_{S^c}(t)$, by taking the inverse Laplace transforms. The failure probability of the system $F_{S^c}(t)$ is an aggregation of all the possibilities.
- Step 5: Obtain the system reliability by time t .

Barrier analysis

The purpose of barrier analysis is to identify suitable and cost-effective solutions for protecting the system from CAFs. We consider two decision variables related with safety barriers: the location of barriers and the number of barriers within a system. B_{ij} denotes the barriers installed on the path of failure propagation between components i and j , as shown in Figure 1(b).

Important measures can be used for comparing the criticalities of barriers in different locations. As stated in equation (11), one of the measures is improvement in system reliability by using barrier i by time t denoted by $\text{Ip}(i|t)$

$$\text{Ip}(i|t) = h(1_i, R_{S^c}^c(t)) - h(0_i, R_{S^c}^c(t)) \tag{11}$$

where $h(1_i, R_{S^c}^c(t))$ is the λ_i probability that the system is functioning when barrier i is installed, while

$h(0_i, R_S^c(t))$ is the conditional probability that the system is functioning when barrier i is not installed. If the value $I_P(i,t)$ is large, it means that barrier i results in a comparatively large change in the system reliability at time t . This measure is applied for identifying the most important barrier and comparing the effects of barriers. However, the increase of absolute value is rather small,

$$\mathcal{L}[F_{2,3}(t)] = \frac{1}{s} - \frac{1}{s + \lambda_2 + \lambda_3}$$

$$\mathcal{L}[F_{1,3}(t)] = \frac{1}{s} - \frac{1}{s + \lambda_1 + \lambda_3}$$

Step 2: By using equations (6) and (9), $\mathcal{L}[F_{S-i}(t)](i = 1, 2, 3)$ can be obtained

$$\mathcal{L}[F_{S-1}(t)] = \left[\bar{\gamma}_{12}\bar{\gamma}_{13}\mathcal{L}[F_{2,3}(t)] + \frac{1}{s}(\gamma_{12}\bar{\gamma}_{13} + \gamma_{13}\bar{\gamma}_{12} + \gamma_{12}\gamma_{13}) \right] \frac{\lambda_1}{s + \lambda_1 + \lambda_2 + \lambda_3}$$

$$\mathcal{L}[F_{S-2}(t)] = \left[\bar{\delta}_{12}\bar{\gamma}_{23}\mathcal{L}[F_{1,2}(t)] + \frac{1}{s}(\gamma_{21}\bar{\gamma}_{23} + \gamma_{23}\bar{\gamma}_{21} + \gamma_{21}\gamma_{23}) \right] \frac{\lambda_2}{s + \lambda_1 + \lambda_2 + \lambda_3}$$

$$\mathcal{L}[F_{S-3}(t)] = \frac{1}{s} \cdot \frac{\lambda_3}{s + \lambda_1 + \lambda_2 + \lambda_3}$$

thus a modified Birnbaum measure is introduced as the ratio of the improvement in system reliability by using

Step 3: $F_S^c(t)$ is the sum of the failure probability of the system Ω ($\Omega = [1, 2, 3]$). Laplace transforms of the failure probability can be obtained by

$$\mathcal{L}[F_S^c(t)] = \mathcal{L}[F_{S-1}(t)] + \mathcal{L}[F_{S-2}(t)] + \mathcal{L}[F_{S-3}(t)] = \frac{1}{s} - \frac{\bar{\gamma}_{12}\bar{\gamma}_{13}}{s + \lambda_2 + \lambda_3} - \frac{\bar{\gamma}_{21}\bar{\gamma}_{23}}{s + \lambda_1 + \lambda_3} - \frac{(1 - \bar{\gamma}_{12}\bar{\gamma}_{13} - \bar{\gamma}_{21}\bar{\gamma}_{23})\lambda_1}{s + \lambda_1 + \lambda_2 + \lambda_3}$$

the barriers i by time t , denoted by $I_B(i,t)$ that is

$$I_B(i,t) = \frac{h(1_i, R_S^c(t)) - h(0_i, R_S^c(t))}{h(0_i, R_S^c(t))} \tag{12}$$

Two examples are presented to show the effects of cascading failures and safety barriers in the following sections.

An illustrative example

An illustrative example composing only three components is employed to elaborate on how system reliability is evaluated by the proposed method. RBD of this example and corresponding CAFs have been presented in Figure 1(a).

Impact analysis of CAFs

System reliability analysis with CAFs. According to equation (2), the matrix Γ with cascading possibilities and the matrix $\bar{\Gamma}$ with escaping probabilities are arranged as

$$\Gamma = \begin{bmatrix} 0 & \gamma_{12} & \gamma_{13} \\ \gamma_{21} & 0 & \gamma_{23} \\ 0 & 0 & 0 \end{bmatrix} \quad \bar{\Gamma} = \begin{bmatrix} 1 & \bar{\gamma}_{12} & \bar{\gamma}_{13} \\ \bar{\gamma}_{21} & 1 & \bar{\gamma}_{23} \\ 1 & 1 & 1 \end{bmatrix}$$

Step 1: We can obtain the failure probabilities of MPSs by using Laplace transforms $\mathcal{L}[F_{2,3}(t)]$ and $\mathcal{L}[F_{1,3}(t)]$ as

Step 4: By inverting Laplace transforms, the failure probability of the system $F_S^c(t)$ considering CAFs can be expressed as

$$F_S^c(t) = 1 - \bar{\gamma}_{12}\bar{\gamma}_{13}e^{-(\lambda_2 + \lambda_3)t} - \bar{\gamma}_{21}\bar{\gamma}_{23}e^{-(\lambda_1 + \lambda_3)t} - (1 - \bar{\gamma}_{12}\bar{\gamma}_{13} - \bar{\gamma}_{21}\bar{\gamma}_{23})e^{-(\lambda_1 + \lambda_2 + \lambda_3)t} \tag{13}$$

Step 5: The system reliability $R_S^c(t)$ considering CAFs can therefore be obtained as

$$R_S^c(t) = \bar{\gamma}_{12}\bar{\gamma}_{13}e^{-(\lambda_2 + \lambda_3)t} + \bar{\gamma}_{21}\bar{\gamma}_{23}e^{-(\lambda_1 + \lambda_3)t} + (1 - \bar{\gamma}_{12}\bar{\gamma}_{13} - \bar{\gamma}_{21}\bar{\gamma}_{23})e^{-(\lambda_1 + \lambda_2 + \lambda_3)t} \tag{14}$$

Verification of the numerical analysis. MC simulations for failure propagations are conducted in MATLAB to check the results of the proposed approach. Figure 2 is the flowchart of MC simulations. $T_i(\lambda_i)$ is denoted as an exponential random variable representing the time to failure of component i with a constant failure rate λ_i , η is a random variable generated from a uniform $[0, 1]$ and is delimited by a cascading probability, γ_{ij} is the failure that propagates from component i to j , and T_s is the simulated time to system failure.

To verify the numerical analysis results, it is assumed without losing generality that the values of the parameters are assigned as shown in Table 1. Here, 10^6 MC iterations run over a period of 2190 h (3 months). The results of the system reliability by using the analytical algorithm and MC simulations are presented in Figure 3. As seen, reliability calculation using equation (14) gives the exact same results as the MC simulations.

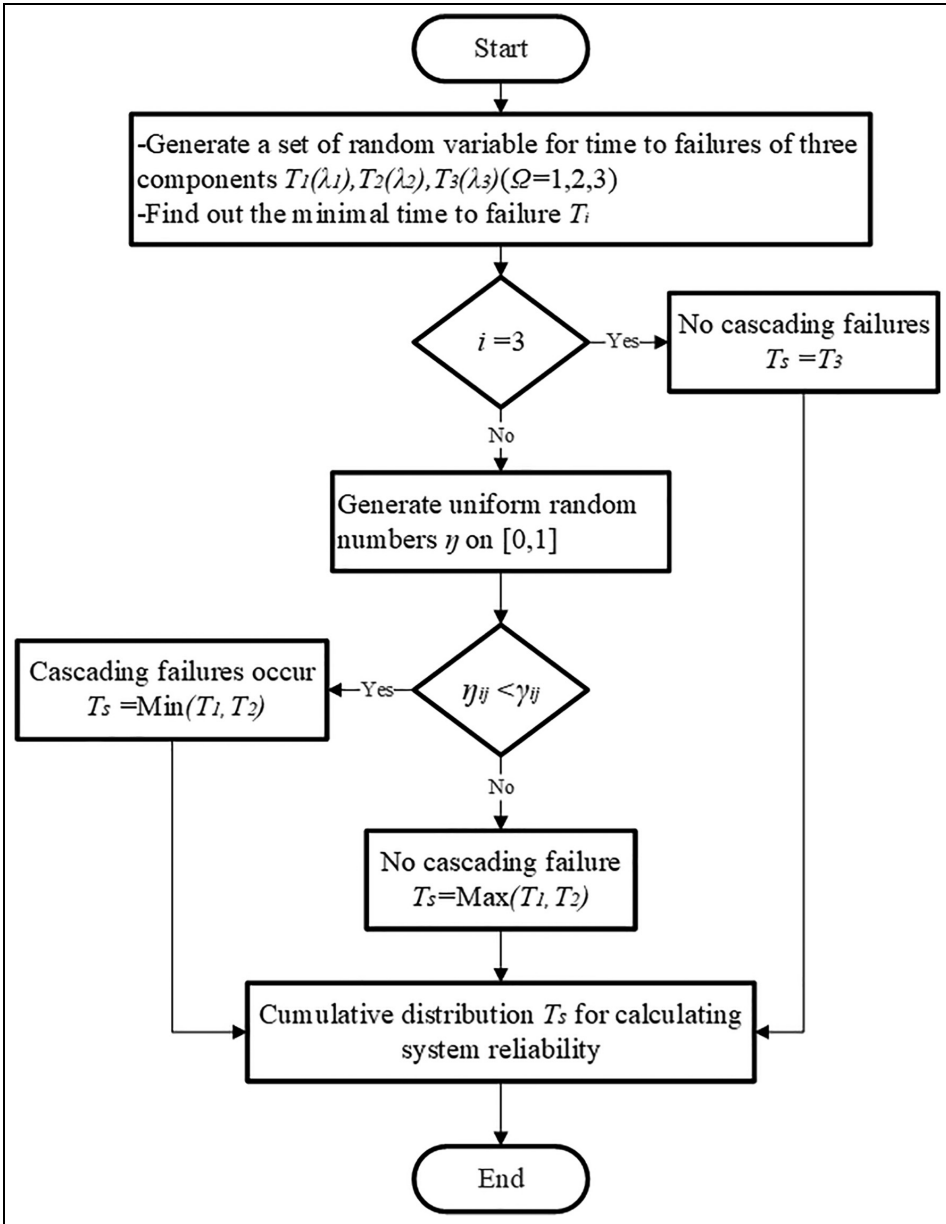


Figure 2. Flowchart of MC simulations for failure propagation.

Table 1. Inputs parameters for the analysis.

Parameter	Values	Parameter	Values
γ_{12}	0.2	λ_1	1.0×10^{-3} per hour
γ_{13}	0.1	λ_2	5.0×10^{-4} per hour
γ_{21}	0.2	λ_3	2.5×10^{-4} per hour
γ_{23}	0.1	—	—

It is demonstrated that the proposed approach is suitable for evaluating the reliability of series-parallel systems that subject to CAFs.

Sensitivity analysis. Sensitivity analysis is conducted here to examine how much does the system reliability changes when the cascading probabilities change. Here, all cascading probabilities in Table 1 are reduced by

Table 2. System reliability with multiple barriers at $t = 100$ h.

No.	Barriers	System reliability	$I_B(i t)(\%)$	Cost	No.	Barriers	System reliability	$I_B(i t)(\%)$	Cost
0	No	0.93	—	—	8	B_{12}, B_{23}	0.95	2.54	2a
1	B_{23}	0.94	0.37	a	9	B_{12}, B_{21}	0.96	2.64	2a
2	B_{13}	0.94	0.76	a	10	B_{12}, B_{13}	0.96	2.04	2a
3	B_{21}	0.94	0.84	a	11	B_{13}, B_{21}, B_{23}	0.95	3.00	3a
4	B_{12}	0.95	1.70	a	12	B_{12}, B_{21}, B_{23}	0.96	3.02	3a
5	B_{13}, B_{23}	0.94	1.12	2a	13	B_{12}, B_{13}, B_{23}	0.96	3.48	3a
6	B_{21}, B_{23}	0.95	1.30	2a	14	B_{12}, B_{13}, B_{21}	0.98	2.54	3a
7	B_{13}, B_{21}	0.95	1.58	2a	15	$B_{12}, B_{13}, B_{21}, B_{23}$	0.97	3.94	4a

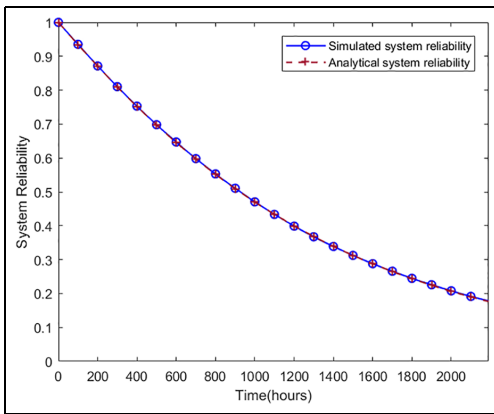


Figure 3. System reliability of example 1 by using MC simulation and analytical formula.

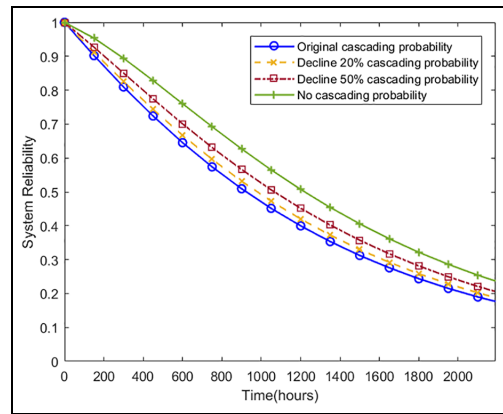


Figure 4. Sensitivity analysis of example 1 for cascading probability and failure rates.

20%, 50% and 100%, respectively. For example, γ_{12} is 0.2 in Table 1, and here it is set as 0.16, 0.1, and 0, respectively. Figure 4 shows the system reliability at a certain moment increases with the decreases of the cascading probabilities during 2190 h. The difference in the values for the system reliability with and without cascading probabilities can be explained by the effects of CAFs. For example, by 1000 h, reliability of the system without CAFs can be around 0.6, that is 50% higher than that of the system where CAFs always occur. Such findings imply that the introduction of any barriers is helpful to mitigate the effects of CAFs, but it is not increasing system reliability in a linear way. Therefore, it is necessary to analyze how many and where the safety barriers are to be installed in a more cost-effective manner ensuring system reliability.

Barrier analysis

In this subsection, we will analyze how the different layouts of safety barriers in such a small system can mitigate CAFs in different ways. The two scenarios are considered: only one single barrier is installed in the system at one time, and multiple barriers are available at the same time to intervene the failure propagations.

As shown in Figure 1(b), if only one barrier is employed, four options to install the barriers can be concerned: on the paths from components 1 to 2, from 2 to 1, from 1 to 3, and 2 to 3. Safety barriers have been assumed as perfect, meaning that when any of them is installed on a path, the cascading probability from the component at the starting side to that at the end side becomes 0. The system reliability can be calculated based on equations (4)–(10). Figure 5 presents the system reliability changing with time when a single barrier is installed at different places. Barrier B_{12} always leads to a higher reliability than the others in this case. With such a rough analysis, system designer can recognize the appropriate location if they only install one safety barrier in the system.

Considering multiple safety barriers to be installed in this system, it is necessary to identify which combination of the barriers is more effective. Similarly, the effects of different barrier combinations can be obtained (numbering from 0 to 15, and here we also consider $t = 100$ h as an example) as presented in Table 2 and Figure 6. It is noticed that some single barriers even have a greater impact on the system reliability than a combination of several ones. For example, barrier B_{12} (No. 4) is more effective than the combinations of two barriers B_{13} and B_{21} , B_{21} and B_{23} , and B_{13}

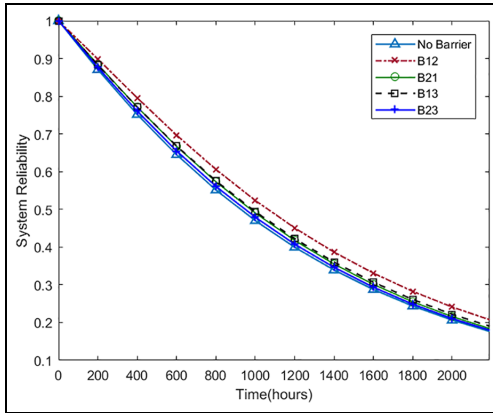


Figure 5. System reliability of example 1 with single barriers against CAFs.

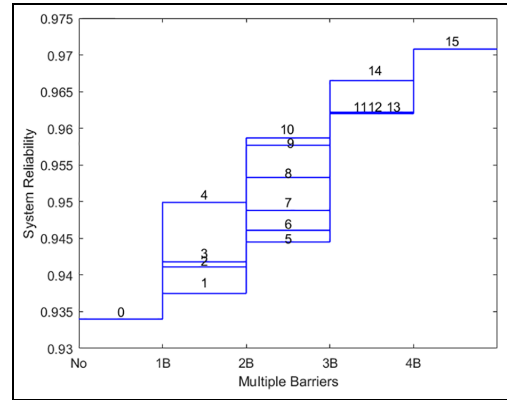


Figure 6. System reliability of example 1 with multiple barriers against CAFs.

and B_{23} (i.e. No. 7, No. 6, and No. 5). If the required resources for employing any of those barriers are assumed to be the same, the barrier B_{12} is more cost-effective than those combinations.

Since the increase of absolute value of system reliability is rather small in this case, the values of $I_B(i|t)$, in a straightforward way, can better reflect the mitigating effectiveness of employing a certain combinations of safety barriers. Once the cost information of safety barriers and system failures are available, $I_B(i|t)$ can be used to determine which barriers should be installed. For a simple example, if the cost of any safety barrier is a , and the loss/cost in a system failure is $100a$, it can be roughly summarized, that those barrier combinations with $(I_B(i|t)/n) > 1$ are more reasonable options, where n is the number of barriers, because the risk reduction is more significant than the cost increase. In this case, No. 4 is worth investing if only one barrier can considered due to limited budget. No. 14 is the best in consideration of barrier combinations.

designed to separate production fluids into their constituent components of oil, gas, and water. The scrubber is used to wash unwanted pollutants from the gas stream. The essential function of the compressors is to increase the pressure and temperature of the gas.

In this case, fires caused by independent failures (e.g. overheating) of components 1, 2, 3, 5, 6, and 7 can propagate to the other components in the same facility. Considering the locations of equipment, fires generated in a place may cause selective effects (i.e. the damage of parts of systems), as shown in Figure 7. It is assumed that cascading probabilities between the components are the same and the escaping probability is $\bar{\gamma}$. MPSs for this system are $MPS_1 = \{1, 2, 4, 5\}$, $MPS_2 = \{1, 2, 4, 6\}$, $MPS_3 = \{1, 2, 4, 7\}$, $MPS_4 = \{3, 4, 5\}$, $MPS_5 = \{3, 4, 6\}$, and $MPS_6 = \{3, 4, 7\}$.

Reliability analysis

Reliability of the system considering CAFs in Figure 7 can be obtained based on equation (10)

$$\begin{aligned}
 R_S^c(t) = & (\bar{\gamma}^7/2 + 2\bar{\gamma}^6/3 - 5\bar{\gamma}^5/3 - 11\bar{\gamma}^4/3 + 11\bar{\gamma}^3/6 + 7\bar{\gamma}^2/3 - \bar{\gamma})e^{-7\lambda t} + (3\bar{\gamma}^7 + 5\bar{\gamma}^6/2 \\
 & + \bar{\gamma}^5/2 - 15\bar{\gamma}^4/2 - 15\bar{\gamma}^3/2 + 5\bar{\gamma}^2 - 2\bar{\gamma} + 1)e^{-5\lambda t} - (2\bar{\gamma}^7 + 7\bar{\gamma}^6/6 + 17\bar{\gamma}^5/6 - 7\bar{\gamma}^4/6 \\
 & - 11\bar{\gamma}^3/3 + 5\bar{\gamma}^2/6 - 2\bar{\gamma})e^{-4\lambda t} + (\bar{\gamma}^7/2 + \bar{\gamma}^6/6 + 7\bar{\gamma}^5/6 + \bar{\gamma}^4/2 + \bar{\gamma}^3/3 + \bar{\gamma}^2/3)e^{-3\lambda t} \\
 & + (-2\bar{\gamma}^7 - 13\bar{\gamma}^6/6 + 17\bar{\gamma}^5/6 + 19\bar{\gamma}^4/2 + 5\bar{\gamma}^3/3 - 41\bar{\gamma}^2/6 + \bar{\gamma})e^{-6\lambda t}
 \end{aligned}
 \tag{15}$$

Case studies for preventing CAFs in oil and gas production

Consider applying the RBD-based recursive aggregation approach for a more complex system. A practical case of an oil and gas production system is taken into account, consisting of three separators (components 1, 2, and 3), one scrubber (component 4), and three compressors (components 5, 6, and 7). The separators are

MC simulations are conducted in a similar way as the one for example 1, using the flowchart in Figure 2. Figure 8 presents the analytical and simulated results of system reliability ($\lambda = 10^{-3}/h, \gamma = 0.2$). As seen, equation (15) gives the same results as the MC simulations, which can strengthen the confidence in the suggested approach.

Sensitivity analysis is used to understand the influences from changing design parameters (e.g. cascading probabilities). Figures 9 and 10 show the system

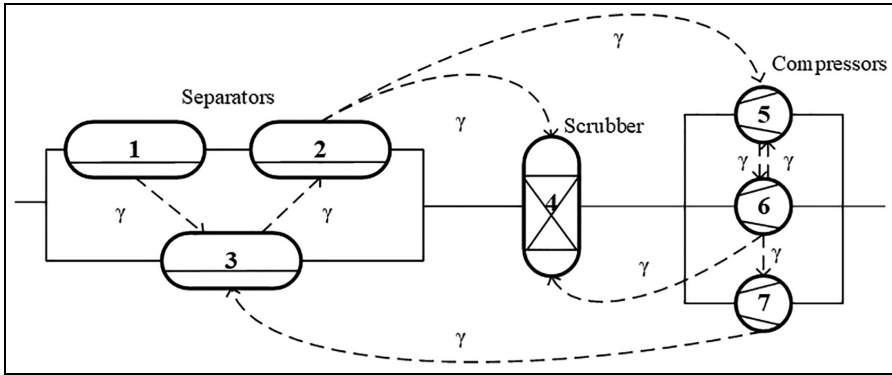


Figure 7. RBD of example 2 with CAFs.

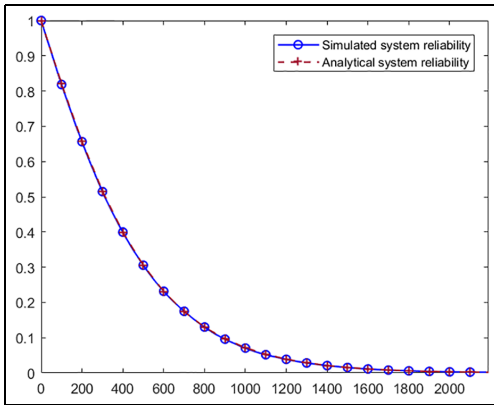


Figure 8. System reliability of example 2 by using MC simulations and analytical formula.

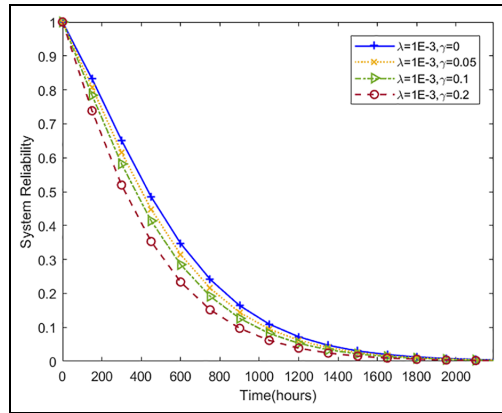


Figure 9. System reliability of example 2 with different cascading probabilities.

reliability profiles during 2190 h (3 months) with consideration of different cascading probabilities and failure rates. In Figure 9, the failure rates of independent failures on all the components are assigned as a fixed value of 1.0×10^{-3} per hour. With different value of cascading probabilities γ , we can observe the impact of CAFs on the system reliability. $\gamma = 0.2$ means that components are sensitive to the failure events (i.e. fires) and one failure can easily result in another failure. There is no CAFs when γ is equal to 0. Figure 10 presents the impacts of independent failures the system reliability. The failure rates of independent failures are assigned as the values varying from 0.5×10^{-3} to 2.0×10^{-3} per hour.

The distances between facilities can be far to reduce the cascading probability, or more suitable materials can be used to realize lower failure rates, because failure rates have more impacts than cascading probabilities on system reliability in this case. Thus, the system

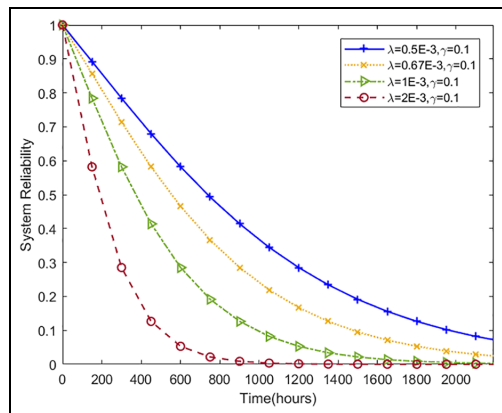


Figure 10. System reliability of example 2 with different failure rates.

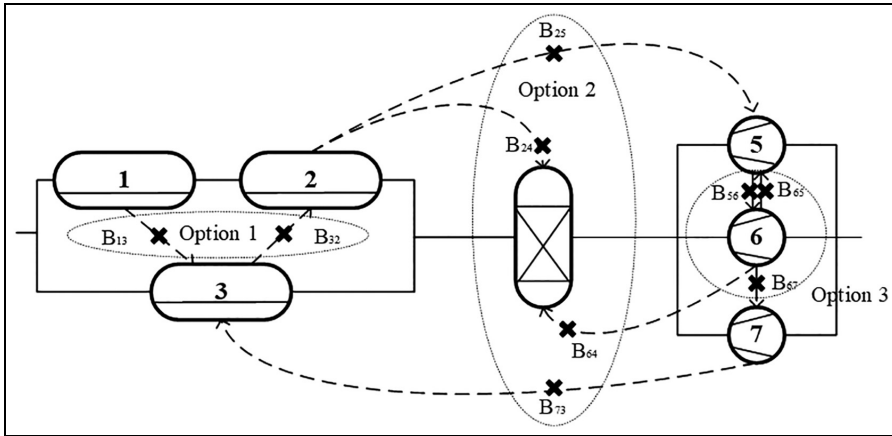


Figure 11. Series-parallel system of example 2 with barrier options against CAFs.

Table 3. System reliabilities of example 2 with single barrier against CAFs at $t = 100$ h.

B_{ij}	B_{13}	B_{32}	B_{24}	B_{25}	B_{56}	B_{65}	B_{64}	B_{67}	B_{73}
$R_S^C(t)$	0.83	0.83	0.84	0.83	0.82	0.82	0.84	0.82	0.82
$I_B(i t)$ (%)	1.73	1.66	1.78	1.68	0.13	0.38	1.79	0.39	0.25

designer or operators can compare different measures by using the proposed approach.

Barrier analysis

Firewalls can be introduced as safety barriers to prevent CAFs from the propagations, as illustrated in Figure 11. Without consideration of barriers, the cascading probabilities between the components are originally assigned to be 0.2.

Both single barrier and multiple barriers are considered in this case. By using equations (10) and (11), the system reliability and barrier importance can be obtained, as shown in Table 3. Figure 12 presents the system reliability at $t = 100$ h when only a single barrier is involved. The failure rates of independent failures for all the components are assumed as 1.0×10^{-3} per hour.

According to the importance of a single barrier, B_{13} , B_{24} , and B_{64} are more effective on preventing CAFs. Those failure propagations between components 1 to 3, components 2 to 4, and components 6 to 4 can lead to the system failure. The most significant reliability improvement can be achieved by localizing the barrier B_{64} ($I_B(i|t) = 1.79\%$ at $t = 100$ h). Subject to limited budget, such a barrier analysis can help designers and operators to find out the most critical barrier that lead to the greatest increase on system reliability.

In this case, three options (i.e. options 1, 2, and 3) with respect to different facilities are considered, as shown in Figure 11. Equations (10) and (11) can be

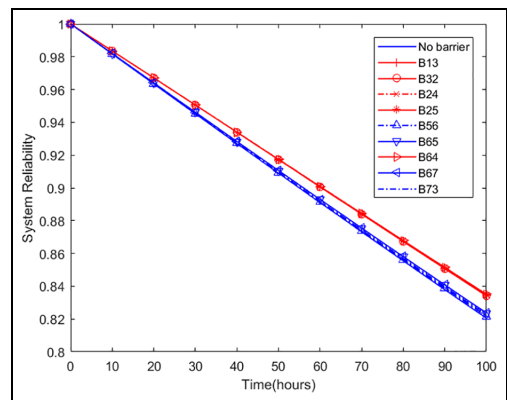


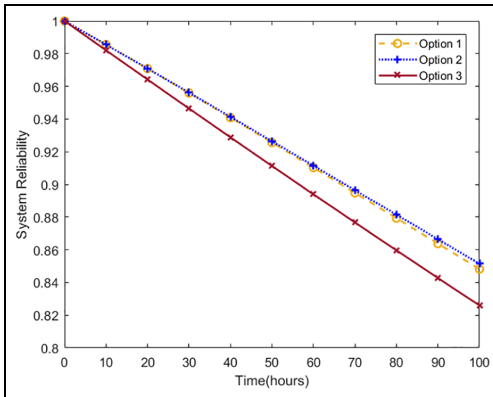
Figure 12. System reliability of example 2 with single barrier against CAFs.

used to measure the importance of multiple barriers. As seen in Table 4 and Figure 13, one can obtain comparable system reliability by using options 2 and 3 ($I_B(i|t) = 3.38\%$ and 3.77%). Option 3 has the lowest effects against CAFs since the barrier importance is only 0.67%. The reason is that option 3 of the barrier is designed to prevent failure propagations in the *1003* subsystem. This subsystem is more invulnerable than the other two subsystems.

By comparing the system reliabilities in Tables 3 and 4, the effects of the barrier B_{64} is found approximately

Table 4. System reliability with multiple barriers at $t = 100$ h.

Options	Barriers	Relevant components	System reliability $R_S^c(t)$	$I_B(i t)$ (%)	Cost
Option 1	B_{23}, B_{32}	1, 2, 3	0.8482	3.38	2a
Option 2	$B_{24}, B_{25}, B_{64}, B_{73}$	4, 5, 3	0.8514	3.77	4a
Option 3	B_{56}, B_{65}, B_{67}	5, 6, 7	0.8260	0.67	3a

**Figure 13.** System reliability of example 2 with multiple barriers against CAFs.

the same as the combined effects of barriers B_{23} and B_{32} . It is even higher than the effects of multiple barriers B_{56} , B_{65} , and B_{67} . This analysis can help the designers to compare the effectiveness of a single barrier and multiple barriers against CAFs in the system in case of limited budget.

Conclusion and future works

This article suggests the RBD-based recursive aggregation approach for assessing reliability of series-parallel systems that are subject to CAFs. Barrier analysis is then employed to mitigate CAFs more effectively. It is investigated in the examples to illustrate how the locations and the number of barriers should be considered in system reliability assurance. The approaches can help one to decide about allocation of the safety barriers to reduce and mitigate the consequence of CAFs in series-parallel technical systems.

The results of case studies in this article are encouraging both in term of qualitative and quantitative analysis. Indeed, the effectiveness of barriers is affected by many factors, including:

1. Cascading failure probabilities.
2. The available budget.
3. Difficulties and features of installations.
4. Frequencies of accidents generating CAFs.
5. Available number of protective barriers.

It is necessary to utilize the proposed barrier assessment in this article combining with other qualitative methods to support decisions in design and maintenance of safety barriers.

Independent/self failures are assumed to be distributed exponentially in this article, but many other distributions can be considered by using the convolutions in the approach. Although the consistency and the validity are shown on simple applications, the present approach may be ineffective to deal with the complexity of very large systems. For the common series-parallel systems with a moderate number of components incorporating CAFs, the approach is applicable to obtain the system reliability. However, the methodology still needs future developments to improve its numerical efficiency.

Future works can be expected from several perspectives. For example, approximation methods can be included to reduce the computational burden. Efforts can also be made to find more numerically performing solutions for more complex systems, for example, network systems, hierarchical systems, and dynamic systems. In addition, the assumption of constant cascading probability is rather restrictive. The statistical dependency between CAFs, for example, time-dependent or jointing cascading probability, can be considered in the analysis. It is also of interest to perform further barrier analysis, for example, multilevel barriers or imperfect barriers against CAFs.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Yiliu Liu  <https://orcid.org/0000-0002-0612-2231>

References

1. Murthy D and Nguyen D. Study of two-component system with failure interaction. *Nav Res Logist Q* 1985; 32(2): 239–247.
2. IEC 62551:2012. Analysis techniques for dependability–Petri net techniques.

3. Rausand M and Høyland A. *System reliability theory: models, statistical methods, and applications*. 2nd ed. Hoboken, NJ: John Wiley & Sons, 2004.
4. Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliab Eng Syst Safe* 2014; 121: 43–60.
5. Levitin G. A universal generating function approach for the analysis of multi-state systems with dependent elements. *Reliab Eng Syst Safe* 2004; 84(3): 285–292.
6. Rausand M. *Risk assessment: theory, methods, and applications*. Hoboken, NJ: John Wiley & Sons, 2013.
7. Xie L, Lundteigen M and Liu Y. Common cause failures and cascading failures in technical systems: similarities, differences and barriers. In: *Proceedings of the European safety and reliability conference*, Trondheim, 17–21 June 2018. Boca Raton, FL: CRC Press.
8. Edwards G and Watson I. *A study of common-mode failures*. Culcheth: UKAEA Risley Nuclear Power Development Establishment, 1979.
9. Harris B. Stochastic models for common failures. In: Basu AP (ed.) *Reliability and quality control*. New York: Elsevier, 1986, pp.185–200.
10. Fleming K. Reliability model for common mode failures in redundant safety systems. In: *Proceedings of the annual conference on modeling and simulation*, Pittsburgh, PA, 24 April 1975. Pittsburgh, PA: Instrument Society of America.
11. Rausand M. *Reliability of safety-critical systems: theory and applications*. Hoboken, NJ: John Wiley & Sons, 2014.
12. Vesely W. Estimating common cause failure probabilities in reliability and risk analysis: Marshall-Olkin specializations. *Nucl Syst Reliab Eng Risk Assess* 1977; 2: 314–341.
13. Khan FI and Abbasi S. Models for domino effect analysis in chemical process industries. *Process Saf Prog* 1998; 17(2): 107–123.
14. Khan FI and Abbasi S. An assessment of the likelihood of occurrence, and the damage potential of domino effect (chain of accidents) in a typical cluster of industries. *J Loss Prevent Proc* 2001; 14(4): 283–306.
15. Khan FI and Abbasi S. DOMIFECT (DOMIno EFFECT): user-friendly software for domino effect analysis. *Environ Modell Softw* 1998; 13(2): 163–177.
16. Khan FI and Abbasi S. Studies on the probabilities and likely impacts of chains of accident (domino effect) in a fertilizer industry. *Process Saf Prog* 2000; 19(1): 40–56.
17. Landucci G, Argenti F, Tugnoli A, et al. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. *Reliab Eng Syst Safe* 2015; 143: 30–43.
18. Cozzani V, Gubinelli G and Salzano E. Escalation thresholds in the assessment of domino accidental events. *J Hazard Mater* 2006; 129(1): 1–21.
19. Vilchez J, Montiel H, Casal J, et al. Analytical expressions for the calculation of damage percentage using the probit methodology. *J Loss Prevent Proc* 2001; 14(3): 193–197.
20. van Erp N, Linger R, Khakzad N, et al. Risk analysis framework for collateral impacts of cascading effects. Report, TU Delft, Delft, 2017. http://rain-project.eu/wp-content/uploads/2017/08/D5_2_Final_merged.pdf
21. Reniers G and Cozzani V. *Domino effects in the process industries: modelling, prevention and managing*. New York: Elsevier, 2013.
22. Cozzani V, Gubinelli G, Antonioni G, et al. The assessment of risk caused by domino effect in quantitative area risk analysis. *J Hazard Mater* 2005; 127(1–3): 14–30.
23. Khakzad N, Khan F, Amyotte P, et al. Domino effect analysis using Bayesian networks. *Risk Anal* 2013; 33(2): 292–306.
24. Khakzad N, Khan F, Amyotte P, et al. Risk management of domino effects considering dynamic consequence analysis. *Risk Anal* 2014; 34(6): 1128–1138.
25. Khakzad N and Reniers G. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. *Reliab Eng Syst Safe* 2015; 143: 63–73.
26. Khakzad N, Landucci G and Reniers G. Application of graph theory to cost-effective fire protection of chemical plants during domino effects. *Risk Anal* 2017; 37(9): 1652–1667.
27. Abdolhamidzadeh B, Abbasi T, Rashtchian D, et al. A new method for assessing domino effect in chemical process industry. *J Hazard Mater* 2010; 182(1–3): 416–426.
28. Abdolhamidzadeh B, Rashtchian D and Ashuri E. A new methodology for frequency estimation of second or higher level domino accidents in chemical and petrochemical plants using Monte Carlo simulation. *Iran J Chem Chem Eng* 2009; 28(4): 21–28.
29. Motter AE and Lai Y-C. Cascade-based attacks on complex networks. *Phys Rev* 2002; 66(6): 065102.
30. Albert R and Barabási A-L. Statistical mechanics of complex networks. *Rev Mod Phys* 2002; 74(1): 47–97.
31. Zio E and Sansavini G. Component criticality in failure cascade processes of network systems. *Risk Anal* 2011; 31(8): 1196–1210.
32. Crucitti P, Latora V and Marchiori M. Model for cascading failures in complex networks. *Phys Rev E* 2004; 69(4): 045104.
33. Murthy D and Nguyen D. Study of a multi-component system with failure interaction. *Eur J Oper Res* 1985; 21(3): 330–338.
34. Liu B, Wu J and Xie M. Cost analysis for multi-component system with failure interaction under renewing free-replacement warranty. *Eur J Oper Res* 2015; 243(3): 874–882.
35. Liu B, Xie M and Kuo W. Reliability modeling and preventive maintenance of load-sharing systems with degrading components. *IIE Trans* 2016; 48(8): 699–709.
36. Saad L, Chateaufneuf A and Raphael W. Stochastic dependency in life-cycle cost analysis of multi-component structures. *Struct Infrastruct E* 2019; 15(5): 679–695.
37. Liu B, Do P, Iung B, et al. Stochastic filtering approach for condition-based maintenance considering sensor degradation. *IEEE T Autom Sci Eng*. Epub ahead of print 19 June 2019. DOI: 10.1109/TASE.2019.2918734.
38. Levitin G. Incorporating common-cause failures into nonrepairable multistate series-parallel system analysis. *IEEE T Reliab* 2001; 50(4): 380–388.
39. Levitin G and Xing L. Reliability and performance of multi-state systems with propagated failures having selective effect. *Reliab Eng Syst Safe* 2010; 95(6): 655–661.
40. Xing L and Levitin G. Combinatorial analysis of systems with competing failures subject to failure isolation and propagation effects. *Reliab Eng Syst Safe* 2010; 95(11): 1210–1215.
41. Xing L, Levitin G, Wang C, et al. Reliability of systems subject to failures with dependent propagation effect. *IEEE T Syst Man Cy-S* 2013; 43(2): 277–290.

42. Fricks RM and Trivedi KS. Modeling failure dependencies in reliability analysis using stochastic Petri nets. In: *Proceedings of European simulation multiconference (ESM 97)*, Istanbul, Turkey, 1–4 June 1997, pp.355–368.

43. Tsilipanos K, Neokosmidis I and Varoutas D. A system of systems framework for the reliability assessment of telecommunications networks. *IEEE Syst J* 2012; 7(1): 114–124.

44. Delvosalle C, Fievez C, Pipart A, et al. ARAMIS project: a comprehensive methodology for the identification of reference accident scenarios in process industries. *J Hazard Mater* 2006; 130(3): 200–219.

45. De Dianous V and Fievez C. ARAMIS project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. *J Hazard Mater* 2006; 130(3): 220–233.

46. Wang J. Mitigation strategies on scale-free networks against cascading failures. *Physica A* 2013; 392(9): 2257–2264.

47. Motter AE. Cascade control and defense in complex networks. *Phys Rev Lett* 2004; 93(9): 098701.

48. Ash J and Newth D. Optimizing complex networks for resilience against cascading failure. *Physica A* 2007; 380: 673–683.

49. Peters K, Buzna L and Helbing D. Modelling of cascading effects and efficient response to disaster spreading in complex networks. *Int J Crit Infrastruct* 2008; 4(1–2): 46–62.

50. Janssens J, Talarico L, Reniers G, et al. A decision model to allocate protective safety barriers and mitigate domino effects. *Reliab Eng Syst Safe* 2015; 143: 44–52.

51. Chen C, Reniers G and Khakzad N. Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: a dynamic graph approach. *Reliab Eng Syst Safe* 2019; 191: 106470.

52. SRDR418. *Dependent failures procedures guide*. Cheshire: United Kingdom Atomic Energy Authority, Safety and Reliability Directorate, 1989.

53. Abdelmoez W, Nassar D, Shereshevsky M, et al. Error propagation in software architectures. In: *Proceedings of the 10th international symposium on software metrics*, Chicago, IL, 14 September 2004. Washington, DC: IEEE.

54. Hauge S, Hoem A, Hokstad P, et al. Common cause failures in safety instrumented systems. Report, SINTEF, Trondheim, 20 May 2015.

55. Sklet S. Safety barriers: definition, classification, and performance. *J Loss Prevent Proc* 2006; 19(5): 494–506.

56. Schupp B, Hale A and Pasman H. Optimal integration of safety in complex system design using the safety modelling language. In: *European safety and reliability conference (ESREL)*, Berlin, 14–18 June 2004. Berlin: Springer.

Appendix I

Notation

$F_{fi}(t)$	probability that component i fails due to an independent failure by time t
$F_S^c(t)$	system unreliability by time t considering cascading failures
$F_{S,i}^c(t)$	system unreliability by time t considering cascading failures given that component i has failed at first
$F_{\Omega_m}(t_m, t)$	failure probability of any subsystem Ω_m

$I_P(i t)$	improvement potential in system reliability by using barrier i by time t
$I_B(i t)$	modified Birnbaum measure of barrier i by time t
n_c	number of cascading failures
n_{ci}	number of cascading failures that originate from component i
$T_i(\lambda_i)$	random exponential variable representing the time to failure of component i with a failure rate λ_i
$R_S^c(t)$	system reliability by time t considering cascading failures
γ_{ij}	cascading probability corresponding to the failure probability of component j that is conditioned on the failure of component i
$\bar{\gamma}_{ij}$	escaping probability corresponding to the survival probability of component j that is conditioned on the failure of component i
η	random variable generated from a uniform $[0, 1]$ in simulations
λ_i	independent failure rate of component i
Γ	matrix of failure propagation probabilities between components
$\bar{\Gamma}$	matrix of the escaping probabilities between components
Ω	system consisting of n components
Ω_m	subsystem consisting of $m(m < n)$ components

Appendix 2

Proof of equations (7) and (8)

Let us define Laplace transform $f^*(s)$ of the function $f(t)$ as

$$f^*(s) = \mathcal{L}[f(t)] = \int_0^\infty e^{-st} f(t) dt \tag{16}$$

Unreliability of the system $U_{S,i}^c(t)$ conditioned that component i has failed at first can be expressed as

$$\begin{aligned}
 U_{S,i}^c(t) &= \int_0^t F_{\Omega-i}(t_i, t) \prod_{j \neq i, j \in \Omega} R_j(t) dF_{fi}(t_i) \\
 &= \int_0^t F_{\Omega-i}(t_i, t) \lambda_i e^{-\sum_{\Omega} \lambda_j t_i} d(t_i)
 \end{aligned} \tag{17}$$

Due to the memoryless property of exponential distribution, equation (17) can be modified as

$$U_{S,i}^c(t) = \int_0^t F_{\Omega-i}(t-t_i) \lambda_i e^{-\sum_{\Omega} \lambda_j t_i} d(t_i) \tag{18}$$

Let $\mathcal{L}[f_1(t)]$ and $\mathcal{L}[f_2(t)]$ denote Laplace transforms of two functions $f_1(t)$ and $f_2(t)$, and satisfy the property of convolution

$$f_1(t)*f_2(t) = \int_0^t f_1(x)f_2(t-x)dx \tag{19}$$

$$\mathcal{L}[f_1(t)*f_2(t)] = \mathcal{L}[f_1(t)]\mathcal{L}[f_2(t)] \tag{20}$$

Therefore, Laplace transform of equation (18) can be expressed as

$$\mathcal{L}[U_{S,i^c}(t)] = \mathcal{L}[F_{\Omega-i}(t)] \frac{\lambda_i}{S + \lambda_1 + \dots + \lambda_n} \tag{21}$$

$$\mathcal{L}[U_{S^c}(t)] = \sum_{i \in \Omega} \mathcal{L}[F_{\Omega-i}(t)] \frac{\lambda_i}{S + \lambda_1 + \dots + \lambda_n} \tag{22}$$

This page is intentionally left blank



Article V

Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Performance assessment of K-out-of-N safety instrumented systems subject to cascading failures. *ISA transitions* (2021). Volume 118. s. 35-43.

This page is intentionally left blank



Contents lists available at ScienceDirect

ISA Transactions

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

Research article

Performance assessment of K-out-of-N safety instrumented systems subject to cascading failures

Lin Xie^a, Mary Ann Lundteigen^b, Yiliu Liu^{a,*}^a Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, 7491, Trondheim, Norway^b Department of Engineering Cybernetics, Norwegian University of Science and Technology, 7491, Trondheim, Norway

ARTICLE INFO

Article history:

Received 21 November 2018

Received in revised form 10 February 2021

Accepted 10 February 2021

Available online 15 February 2021

Keywords:

Safety instrumented systems

Cascading failures

K-out-of-N configuration

Performance assessment

Average probability of failure on demand

ABSTRACT

Safety instrumented systems often employ redundancy to enhance the ability to detect and respond to hazardous events. The use of redundancy increases the fault tolerance to single failure but remains vulnerable in case of dependent failures, including common cause failures and cascading failures. Reliability analysis of safety instrumented systems therefore involves the impact of dependent failures. The used approaches have primarily focused on common cause failures. In this paper, it is argued the need to consider the effects of cascading failures that are caused by functional dependencies, hazardous events, and shared resources. A recursive aggregation-based approach is proposed for performance analyzing of K-out-of-N safety instrumented systems with consideration of cascading failures. General approximation formulas are developed for estimating the average probability of failures on demand of different configurations of safety instrumented systems. These formulas are compared with those for common cause failures. Then a case of fire water pump is studied to illustrate the effects of cascading failures on safety instrumented systems.

© 2021 The Authors. Published by Elsevier Ltd on behalf of ISA. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Safety instrumented systems (SISs) are employed to prevent hazardous events and mitigate damages in diverse industries, including but not limited to process and nuclear power plants, and oil and gas facilities. A SIS is characterized as a system that relies on electrical/electronic/programmable electronic (E/E/PE) technologies to detect abnormal situations [1]. A SIS performs one or more safety instrumented functions (SIFs) to protect the equipment under control (EUC) [2]. It often consists of one or more components (such as sensors, gas detectors), logic solvers (such as programmable logic controller) and final elements (such as circuit breakers). Considering a process shutdown system as an example of SISs, it performs its safety function as following: In case of process upsets, the sensors of the SIS s detect possible abnormal situations. The sensors will send the alarm information to the logic solver(s), which can activate the final elements, shutdown valves, to stop production [3].

According to the standards IEC 61508 [1] and IEC 61511 [2], performance requirement on a SIS is often assigned to each SIF and reliability assessment is carried out to prove compliance to the requirement [1,2]. It is stated that the SIFs performed by a SIS must fulfill specified safety integrity levels (SILs). Four different

SILs are defined in accordance with the average probability of failure on demands ($PF_{D,avg}$), ranging the safety integrity from SIL 1 (the lowest level) to SIL4 (the highest level). $PF_{D,avg}$ is the performance measure for SISs operating in the low-demand mode [1]. It can also be interpreted as a mean proportion of time that the item is not able to perform its specified SIF in a certain period or a long term [4]. $PF_{D,avg}$ may be calculated on the basis of several methods: simplified formulas based on fault tree analysis (FTA) [4], IEC 61508 formulas [1], PDS method [5], and Markov methods [6].

To reduce $PF_{D,avg}$, it is often effective to introduce redundancy, such as K-out-of-N ($KooN$) configurations, into a SIS subsystem. $KooN$ means that the subsystem with N parallel components is available when at least K components are functioning. A typical SIS in the oil & gas industry, high-integrity pressure protection system (HIPPS), can comprise a 2oo3 configuration of pressure transmitters, a 1oo1 configuration of logic solver, and a 1oo2 configuration of shutdown valves. The HIPPS does not terminate its SIF until there are two or more failures on transmitters, one failure on the logic solver, or two failures on the valves. Such kind of configurations normally can increase the reliability and availability of systems. This redundancy often brings dependent failures, which occur on multiple components with functional dependencies and shared resources [7]. IEC 61508 [1], ISO/TR 12489 [8] and PDS ("Reliability of SIS" in Norwegian) handbook [5] have indicated that the effects of dependent failures on the performance of SISs should be considered. Biswal et al. have

* Corresponding author.

E-mail address: yiliu.liu@ntnu.no (Y. Liu).

proposed approaches based on FTA for redundant structure in production systems like hydrogen cooling systems [9]. However, it is difficult to straightforwardly use by such traditional methods like FTA, IEC 61508 formulas and Markov to deal with dependent issues with SISs [10–12].

IEC 61508 and relevant literature focus primarily on common cause failures (CCFs) as dependent failures. CCFs are characterized by the failures of two or more components fail due to the same reasons [1]. They can be modeled by the standard and the multiple beta-factor model incorporated with FTA, PDS method and Markov model in PFD_{avg} calculation [5,12]. Cascading failures (CAFs) are another type of dependent failures, reflecting the multiple failures that one component's failure results in chain reactions [12]. The differences between cascading and CCFs in interdependences and propagation mechanisms have been discussed in the previous work [13]. CCFs are the failures that are first in line and directly linked to the failure causes, while the propagation of CAFs follows a series of interactions. Therefore, the models for assessing performance of SISs with CCFs are not applicable for the SISs with CAFs.

SISs are vulnerable to CAFs that are originated from the reliance on shared loads, shared testing and maintenance resources, hazardous events, and dependent functions [13,14]. For example, several components are configured in parallel in a flow transmission system sharing maintenance resources. The failure of one component may occupy the maintenance resource, decrease the possibilities of maintenances on other components, and then trigger more failures [14]. Another example is a fire water supply system where the pumps are operating in a *KooN* configuration. When one of the pumps fails, the corresponding pipeline is closed, and other pumps must carry the whole loads. The probabilities of failures-to-start of the other pumps thereby increase. Many researchers analyze the impacts of CAFs on general systems based on different theory and models including but not limited to complex network [15–18], risk analysis [19–22], probabilistic analysis [23,24] and maintenance optimizations [25,26].

Nevertheless, performance assessment of SISs that are subject to CAFs is seldom explored. SISs are such a kind of systems whose SIFs are only be activated upon abnormal situations. Since SISs are not running all the time in the low demand operational mode, many failures cannot be detected immediately after their occurrences. These so-called hidden failures can be both independent- and dependent-failures. Periodical proof tests, such as once per year, are conducted in many process plants to reveal hidden failures of SISs, but with noticeable delays. Performance assessment of SISs thus needs specific measures, such as PFD_{avg} for low demand mode of SISs. The value of PFD_{avg} is not only related with the internal properties of a SIS, but also related with the frequency and effectiveness of proof tests (see [1,2] and [4]). These particularities distinguish SISs from production or general systems and impede the adaption of the existing approaches for CAF analysis to SISs.

Therefore, the objective of this paper is to introduce the approaches for incorporating CAFs into performance assessment of SISs: (1) A generalized approach based on recursive aggregation for reliability analysis of SISs subsystems voted *KooN*. (2) Approximation formulas for performance assessment of most common configuration SISs. The approximation formulas may be considered for the standards with respect to SISs, such as IEC 61508 and ISO TR 12489, as a complement to the existing formulas for performance assessment of SISs.

The rest of the paper is organized as follows: Section 2 discusses the considerations in SIS performance assessment and the basic analysis approaches for CAFs. Section 3 presents an approach based on recursive aggregations for reliability analysis of SISs that subject to CAFs, and Monto Carlo Simulation is

adopted to verify the numerical results. Section 4 introduces approximation formulas for evaluating the performance of SISs with general configurations, and Section 5 illustrates the approach and the effects of CAFs with a case study. Finally, a discussion is presented, and further works are discussed in Section 6.

2. Considerations in assessing SISs with CAFs

It is important to clarify the characteristics of CAFs and SISs before quantitative analysis, in consideration that many arguments still exist.

2.1. Failures and performance measures of SISs

IEC 61508 splits the failures of SISs into two groups [1]: dangerous failures and safe failures. Owing to many automatic diagnosis functions in SISs, some dangerous failures can be found immediately when they occur, as dangerous detected (DD) failures, but some other failures are hidden after occurrence for some time, as dangerous undetected (DU) failures. DU failures are more of interests in many studies including this paper, because DU failures are the main contributors to the unavailability of SISs and only can be revealed by proof tests or when a demand/shock occurs [4]. A proof test is a periodic test performed to detect DU failures in SISs so that, if necessary, a repair can restore the system to an 'as-good-as-new' condition or as close as practical to this condition. In case of DU failures, the SISs cannot activate when a demand comes, and a disaster may therefore occur.

Performance of a SIS is often measured by PFD_{avg} if the SIS is in low demand mode, namely the demand rate is less than once per year according to IEC 61508 [2]. PFD_{avg} of subsystems (sensors, logical solvers, and final elements) is dependent on DU failure rates of components, system configurations, and frequency and effectiveness of tests and maintenances. The overall PFD_{avg} of a SIS is a sum of the values of PFD_{avg} of its three subsystems. The rest parts of this paper will be limited to the SIS subsystems in low-demand modes, concerning DU failures and PFD_{avg} in the quantification of SILs. For the assessment of SISs in other demand modes and the applicability of PFD_{avg} , readers can find more information in [6,27].

2.2. CAFs analysis

CAFs appear in the current literatures with different names, including induced failures, domino failures, and propagating failures [19,25,28]. Rausand and Høyland [12] define CAFs as the multiple failures that the failure of one component result in a chain reaction. Murthy and Nguyen regard CAFs as the failures that affect the remaining components in a system [25]. Hauge et al. [9] view CAFs as the escalating failures that one or more components fail caused by failures of other components. Although there is no standard definition for CAFs, researchers have some common agreements that CAFs start from one component and spread to more in the system. On the contrary, there are some failures whose occurrence probabilities are irrelevant with other components [4], like, an age-related failure. In this paper, such failures are called as independent failures or self-failures, and their occurrences are irrelevant with other components.

For subsystems in a SIS, especially for sensor- and final element subsystems, it is common that identical components are installed in a voting structure. These components can suffer from the same hazardous events and are monitored with the same mechanism. Thus, the dependency among these components, as the root cause of CAFs, is difficult to be avoided.

In this study on the performance assessment of SISs, the following assumptions are existing:

- (1) All the components in a subsystem of SISs are identical and unreparable.
- (2) Only two states account for all the components: either functioning or failed.
- (3) An independent/self-failure of a component is characterized by a distribution function $F(t)$, and the time to failures is assumed as an exponential distribution, namely the component has a constant failure rate λ . Other distributions, such as Weibull distribution for many mechanical systems can also be considered.

Considering the particulars of CAFs, additional assumptions are needed in analysis:

- (1) Any component can lose its SIF due to a self-failure or the cascading impact of the failures of other components.
- (2) Propagation duration of CAFs is rather short and can be ignored.

We use cascading intensity $\gamma_{ij}(t) \in (0, 1]$ ($i \neq j$) to reflect the easiness of failure propagation from component i to component j . In mathematics, the cascading intensity is expressed as the conditional failure probability of component j when component i fails by time t :

$$\gamma_{ij}(t) = \Pr(\text{comp. } j \text{ fails by } t \mid \text{comp. } i \text{ has failed by } t) \quad (1)$$

The value of cascading intensity $\gamma_{ij}(t)$ can be estimated by either parametric or nonparametric techniques based on historic data. It is not difficult to identify cascading failures that origin from a failure in another component from review of maintenance notifications in case of adequate and detailed failure causes descriptions. The probability $\gamma_{ij}(t)$ is arranged as a matrix γ that represents failure propagation between the components. The probabilities escaping from CAFs are $\delta_{ij}(t) = 1 - \gamma_{ij}(t)$. With the assumption of exponential distributions, $\gamma_{ij}(t)$ and $\delta_{ij}(t)$ can be simplified as two constants γ_{ij} and δ_{ij} , or even γ and δ for identical components in the rest parts of this paper.

3. SIS reliability analysis with CAFs

The performance assessment often starts from reliability analysis based on probabilistic theory and models [12]. This section suggests a system reliability analysis approach of *KooN* configurations subject to CAFs. Then, Monte Carlo simulation is used to check whether the analytical results are appropriate or not.

3.1. The recursive aggression-based approach

The reliability of the systems in parallel and in series that are affected by CAFs has been discussed in [26]. For many traditional reliability methods, such as fault tree, they are not effective in dealing with failures with dependencies. In this section, we extend the research to SISs, and to more general configurations, namely *KooN* voting structures. A recursive aggregation-based approach proposed can be applicable for analyzing systems with several components and many CAFs propagation paths. Recursive aggregation means that evaluation is repeated for each combination of the components in the systems.

Let $F_{\Omega}(t_a, t)$ express a probability that the system Ω ($\Omega = [1, 2 \dots n]$) fails by time t , conditioned on that all the component in the system Ω is functioning by time t_a . Let $G_{\Omega}(t_i, t)$ denote the probability that the system Ω fails in $[t_i, t]$ given that component i fails at time t_i . The failure probability of the system Ω is obtained:

$$F_{\Omega}(t_a, t) = \sum_{i \in \Omega} \int_{t_a}^t G_{\Omega}(t_i, t) \prod_{j \neq i, j \in \Omega} R_{j_m}(t) / \prod_{j \in \Omega} R_j(t_a) dF_i(t_i) \quad (2)$$

where $R_{j_m}(t)$ denotes the reliability of component j_m ($\forall j_m \in \Omega - i, m \in [1, 2, \dots, n - k - 1]$) at time t . $F_i(t_i)$ denotes the failure probability because of independent /self-failures. $G_{\Omega}(t_i, t)$ is given by:

$$\begin{aligned} G_{\Omega}(t_i, t) = & \Pr(n_c = 0)F_{\Omega - \{i\}}(t_i, t) \\ & + \sum_{j_1 \in \Omega - \{i\}} \Pr(n_c = 1)F_{\Omega - \{i, j_1\}}(t_i, t) \\ & + \sum_{j_1, j_2 \in \Omega - \{i\}} \Pr(n_c = 2)F_{\Omega - \{i, j_1, j_2\}}(t_i, t) \dots \\ & + \sum_{j_1, j_2, \dots, j_{n-k-1} \in \Omega - \{i\}} \Pr(n_c = n - k - 1) \\ & \times F_{\Omega - \{i, j_1, j_2, \dots, j_{n-k-1}\}}(t_i, t) + \Pr(n_c \geq n - k) \end{aligned} \quad (3)$$

where n_c denotes the number of CAFs. $\Pr(n_c | m \in [0, 1, 2, \dots, n - k - 1])$ denotes the probability that the system is subject to CAFs with number of n_c . All the components in the SIS subsystem are identical and $\Pr(n_c)$ can be expressed as:

$$\Pr(n_c) = \binom{n_c}{n-1} \delta^{n-n_c-1} \gamma^{n_c} \quad (4)$$

In consideration of the exponential distribution assumption, the starting point of the study, t_a , can be regarded as zero when the system like $\Omega - \{i\}$, $\Omega - \{i, j_m\}$ is regarded as a new system Ω . $F_s(t)$ denotes failure probability of system Ω , and $F_s(t) = F_{\Omega}(t) = F_{\Omega}(0, t)$.

The failure rates for all the components are λ . Hence, the system failure probability $F_s(t)$ can be obtained by using Eqs. (3) and (4) when $t_a = 0$:

$$\begin{aligned} F_s(t) = F_{\Omega}(t) = & n \left[\delta^{n-1} F_{\Omega-1}(t) + \binom{1}{n-1} \delta^{n-2} \gamma F_{\Omega-2}(t) \right. \\ & + \binom{2}{n-1} \delta^{n-3} \gamma^2 F_{\Omega-2}(t) + \dots \\ & + \binom{n-k-1}{n-1} \delta^k \gamma^{n-k-1} F_{\Omega-(n-k-1)}(t) \\ & + \left(\binom{n-k}{n-1} \delta^{k-1} \gamma^{n-k} \right. \\ & + \binom{n-k-1}{n-1} \delta^{k-2} \gamma^{n-k+1} \dots \\ & \left. + \binom{n-1}{n-1} \gamma^{n-1} \right] \end{aligned} \quad (5)$$

The failure probability $F_{\Omega_m}(t_m, t)$ for any subsystem Ω_m is obtained in a similar way by using Eqs. (4) and (5). This aggregation stops when there are more than $N-K-1$ failures in Ω_m . Then, the failure probability of this subsystem is $F_{\Omega-(n-k-1)}(t) = 1 - e^{-k\lambda t}$.

The convolution and Laplace transformation is used to facilitate integration of system failure probabilities in Eq. (2) [12]. We obtained:

$$\mathcal{L}[F_s(t)] = \mathcal{L}[G_{\Omega}(t)] \lambda / (S + n\lambda) \quad (6)$$

.....

$$\mathcal{L}[F_{\Omega-(n-k-1)}(t)] = \frac{1}{S} - \frac{1}{S + k\lambda} \quad (7)$$

Then, the system failure probability $F_s(t)$ and system reliability $R(t)$ can be obtained by inverting Laplace transforms.

3.2. Verification with Monte Carlo simulations

To examine whether the analytical algorithms are appropriate, Monte Carlo (MC) simulations are conducted in MATLAB in this

Table 1
Inputs parameters for the models.

Parameter	Values
γ	0.1, 0.2 and 0.5
λ	2.0×10^{-6} per hour
t	2.5×10^4 hours

section. Two typical configurations of SIS subsystems, 2oo3 and 1oo3 voting structures, have been chosen as examples for formula verification. For a 2oo3 configuration, its reliability can be obtained by Eqs. (3)–(7) as:

$$R(t) = 3\delta^2 e^{-2\lambda t} + (1 - 3\delta^2) e^{-3\lambda t} \quad (8)$$

Similarly, the reliability of a 1oo3 configuration can be obtained as:

$$R(t) = 3\delta(1 - \delta\gamma) e^{-\lambda t} + 3\delta^2(2\gamma - 1) e^{-2\lambda t} + (1 - 3\delta(1 - \delta\gamma) - 3\delta^2(2\gamma - 1)) e^{-3\lambda t} \quad (9)$$

Fig. 1 shows the flowchart of MC simulation for CAFs propagation. $T_i(\lambda)$ denotes random exponential variables. They are the time to failure of component i with λ failure rate. Let P_{ij} denote a random variable that is generated from a uniform distribution in $[0, 1]$. It is limited by γ_{ij} that represents the propagated probability from component i to component j . $T_s(t)$ denotes the simulated time to system failures.

To verify the proposed algorithms, without losing generality, it is assumed that γ_{ij} has fixed values of 0.1, 0.2 and 0.5 respectively for all cascades between components. The time to independent/self-failures $F_i(t)$ is exponentially distributed with a constant failure rate of 2.1×10^{-6} per hour. We run Monte Carlo simulations over a period of 2.5×10^4 hours with 10^5 iterations. Inputs of the parameters are summarized in Table 1.

The results of system reliability for 2oo3 and 1oo3 configurations using analytical approach and MC simulation are presented in Figs. 2 and 3.

As seen, the results using analytical formulas give the almost same results as the MC simulations of 2oo3 and 1oo3 configurations. That gives the confidence on the proposed approach for further reliability analysis of $KooN$ SISs subject to CAFs.

4. Analysis for PFD_{avg} and approximation formulas

In this section, the reliability analysis results can be transformed to PFD_{avg}. Moreover, to simplify the calculations and analyses in practices, approximation formulas for PFD_{avg} of a SIS subsystem with consideration of CAFs are summarized. Then, we have compared of these approximation formulas for CAFs with those for CCFs.

4.1. PFD_{avg} With CAFs

PFD_{avg} is the average probability that the component is not able to react and perform its safety function in response to the demand. Such a measure relates to the time dependent unavailability (PFD(t)) in a proof test interval, denoted by τ . PFD(t) can be expressed as in [4]:

$$\begin{aligned} \text{PFD}(t) &= \text{Pr}(a \text{ DU failure has occurred at or before time } t) \\ &= \text{Pr}(T \leq t) = F(t) \end{aligned} \quad (10)$$

The long-run average PFD_{avg} is equal to the average value of PFD(t) in the first proof test interval (0, τ):

$$\text{PFD}_{\text{avg}} = \frac{1}{\tau} \int_0^\tau \text{PFD}(t) dt = \frac{1}{\tau} \int_0^\tau F(t) dt = 1 - \frac{1}{\tau} \int_0^\tau R(t) dt \quad (11)$$

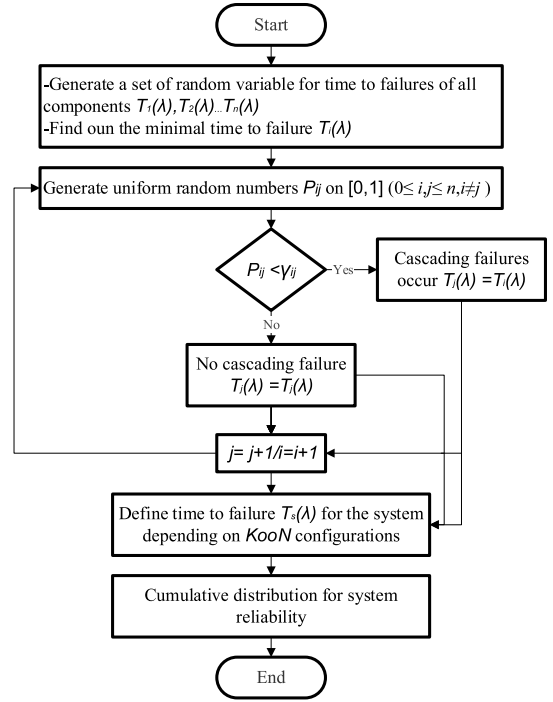


Fig. 1. Flowchart of MC simulation of CAFs propagation.

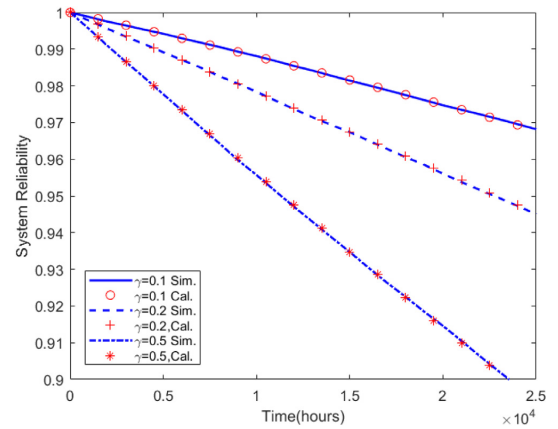


Fig. 2. Simulated and analytical system reliability for 2oo3 configuration.

where τ denotes the length of proof test interval.

Reconsider the two systems, namely 2oo3 and 1oo3 configurations, with all components having a constant DU failure rate λ and cascaded failure probability γ ($\delta = 1 - \gamma$) between any two components. Based on system reliability obtained in Section 3, PFD_{avg} of the 2oo3 configuration can be expressed as:

$$\text{PFD}_{\text{avg}}^{(2oo3)} = 1 - \frac{1}{\tau} \int_0^\tau R(t) dt$$

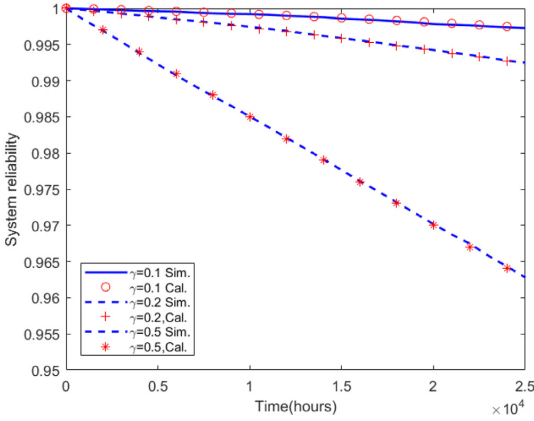


Fig. 3. Simulated and analytical system reliability for 1oo3 configuration.

Table 2 Approximation formulas for PFD_{avg} with CAFs.

K/N	N = 1	N = 2	N = 3	N = 4
K = 1	$\lambda\tau/2$	$2\gamma \cdot \lambda\tau/2$	$3\gamma^2 \cdot \lambda\tau/2$	$4\gamma^3 \cdot \lambda\tau/2$
K = 2	-	$\lambda\tau$	$3\gamma(2 - \gamma) \cdot \lambda\tau/2$	$4\gamma^2(3 - 2\gamma) \cdot \lambda\tau/2$
K = 3	-	-	$3\lambda\tau/2$	$4\gamma(3 - 3\gamma + \gamma^2) \cdot \lambda\tau/2$
K = 4	-	-	-	$2\lambda\tau$

$$= 1 - \int_0^\tau (3\delta^2 e^{-2\lambda t} + (1 - 3\delta^2)e^{-3\lambda t}) dt$$

$$= 1 - \frac{3\delta^2}{2\lambda\tau} (1 - e^{-2\lambda\tau}) - \frac{(1 - 3\delta^2)}{3\lambda\tau} (1 - e^{-3\lambda\tau}) \quad (12)$$

Since SIS components are always highly reliable, λ is a rather small number. Given that $\lambda\tau$ is small (<0.1), we can replace $e^{-2\lambda t}$ and $e^{-3\lambda t}$ by using Taylor series deployment:

$$PFD_{avg}^{(2oo3)} = 1 - 3\delta^2 \left(1 - \frac{2\lambda\tau}{2} + \frac{(2\lambda\tau)^2}{3!} \dots \right) - (1 - 3\delta^2) \left(1 - \frac{3\lambda\tau}{2} + \frac{(3\lambda\tau)^2}{3!} \dots \right)$$

$$\approx 3(1 - \delta^2) \frac{\lambda\tau}{2} \quad (13)$$

While for the 1oo3 configuration, the PFD_{avg} can be obtained as:

$$PFD_{avg}^{(1oo3)} \approx 3\gamma^2 \frac{\lambda\tau}{2} \quad (14)$$

4.2. Generalized formulas for PFD_{avg} with CAFs

With the same approach, PFD_{avg} for other KooN systems can be obtained. PFD_{avg} of some simple KooN ($n \leq 4$) systems are listed in Table 2.

When cascaded failure probability γ is small (for example when $\gamma \leq 0.2$), $\gamma^2, \gamma^3, \gamma^4 \dots$ are negligible. Therefore, simplified formulas for PFD_{avg} is presented in Table 3.

By observing the values in Table 3, a general approximation formula for PFD_{avg} of any KooN configurations is summarized as:

$$PFD_{avg}^{(KooN)} = \binom{N-1}{K-1} N\gamma^{N-K} \frac{\lambda\tau}{2} \quad (15)$$

The general formula is more meaningful for practitioners of SISs, because it can provide enough information only with some simple input numbers.

Table 3 Approximation formulas for PFD_{avg} with CAFs after simplification.

K/N	N = 1	N = 2	N = 3	N = 4
K = 1	$\lambda\tau/2$	$2\gamma \cdot \lambda\tau/2$	$3\gamma^2 \cdot \lambda\tau/2$	$4\gamma^3 \cdot \lambda\tau/2$
K = 2	-	$\lambda\tau$	$6\gamma \cdot \lambda\tau/2$	$12\gamma^2 \cdot \lambda\tau/2$
K = 3	-	-	$3\lambda\tau/2$	$12\gamma \cdot \lambda\tau/2$
K = 4	-	-	-	$2\lambda\tau$

Table 4 Factors σ_{KooN} for different configurations.

K/N	N = 2	N = 3	N = 4	N = 5
K = 1	2γ	$3\gamma^2$	$4\gamma^3$	$5\gamma^4$
K = 2	-	6γ	$12\gamma^2$	$20\gamma^3$
K = 3	-	-	12γ	$30\gamma^2$
K = 4	-	-	-	20γ

Table 5 $\sigma_{KooN}(\gamma = 0.05)$ for CAFs in different configurations.

σ_{KooN}	N = 2	N = 3	N = 4	N = 5
K = 1	1.0×10^{-1}	7.5×10^{-3}	5.0×10^{-4}	3.1×10^{-5}
K = 2	-	3.0×10^{-1}	3.0×10^{-2}	2.5×10^{-3}
K = 3	-	-	6.0×10^{-1}	7.5×10^{-2}
K = 4	-	-	-	10.0×10^{-1}

The validity of such a general formula needs to be examined. A more complicate system of 3oo5 configuration is concerned. The system reliability of the 3oo5 configuration subject to CAFs can be expressed as:

$$R(t) = (10\delta^3\gamma + 10\delta^7)e^{-3\lambda t} + (5\delta^4 - 20\delta^7)e^{-4\lambda t} + [1 - (10\delta^3\gamma + 10\delta^7) - (5\delta^4 - 20\delta^7)]e^{-5\lambda t} \quad (16)$$

PFD_{avg} of 3oo5 configuration is found to be:

$$PFD_{avg}^{(3oo5)} = 1 - \frac{1}{\tau} \int_0^\tau R(t) dt = 5\gamma^2 (6 - 8\gamma + 3\gamma^2) \frac{\lambda\tau}{2}$$

$$\approx 30\gamma^2 \frac{\lambda\tau}{2}$$

$$= \binom{5-1}{3-1} 5\gamma^{5-3} \frac{\lambda\tau}{2} \quad (17)$$

The result matches the general formula Eq. (15) that is proposed in this subsection.

4.3. Comparisons of formulas for CCFs and CAFs

In the PDS handbook [5], PFD_{avg} of SISs subject to CCFs have also been summarized to be approximation formulas relevant with configurations. Here we compare the formulas for PFD_{avg} considering CCFs and CAFs. A factor σ_{KooN} is introduced to distinguish the effects of CAFs on the value of PFD_{avg} among various configurations. Based on Eq. (15), the factors σ_{KooN} for CAFs in different configurations are summarized in Table 4.

PFD_{avg} of the KooN configurations subject to CAFs is therefore calculated as:

$$PFD_{avg(CAF)}^{KooN} = \sigma_{KooN} \frac{\lambda\tau}{2} \quad (18)$$

The factor C_{KooN} is used to describe the effects of CCFs [5]. The general formula for PFD_{avg} is expressed as [5]:

$$PFD_{avg(CCF)}^{KooN} = C_{KooN} \beta \frac{\lambda\tau}{2} \quad (19)$$

To compare the effects of two factors, γ and β are assigned as 0.05 as an example. The factors σ_{KooN} and $C_{KooN}\beta$ for different configurations are illustrated in Tables 5 and 6.

Table 6
 $C_{KooN}\beta(\beta = 0.05)$ for CCFs in different configurations.

$C_{MooN}\beta$	$N = 2$	$N = 3$	$N = 4$	$N = 5$
$K = 1$	5×10^{-2}	2.5×10^{-2}	1.5×10^{-2}	1.0×10^{-2}
$K = 2$	-	1.0×10^{-1}	5.5×10^{-2}	4.0×10^{-2}
$K = 3$	-	-	1.4×10^{-1}	8.0×10^{-2}
$K = 4$	-	-	-	1.8×10^{-1}

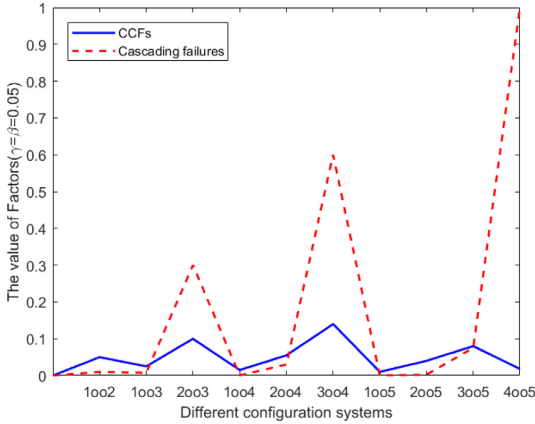


Fig. 4. Comparison of the factors for CCFs and CAFs.

Apparently, the value of factor σ_{KooN} for CAFs is higher than that of $C_{KooN}\beta$ for CCFs, when K is close to N , for example $N-K$ is equal to 1, as shown in Fig. 4. This deviation can be explained that the value of $C_{KooN}\beta$ for CCFs is constant, whereas σ_{KooN} for CAFs relies on γ^{N-K} . Fig. 4 indicates that the curve of CAFs fluctuates much more than that of CCFs, in other words the effects of CAFs towards PF_{Davg} are more likely to rely on configurations. Such a phenomenon with case studies is explored in the next section.

5. Case studies

The purpose of case studies is to investigate the changing trend of SIS performance related to CAFs and then to examine the relevant operational strategies. We consider a fire water supply system, with the focus on the subsystem of final elements, namely firewater pumps.

5.1. System description

The fire water supply system consists of three parts: sensors (for example fire and gas (F&G) detectors, signal from ESD

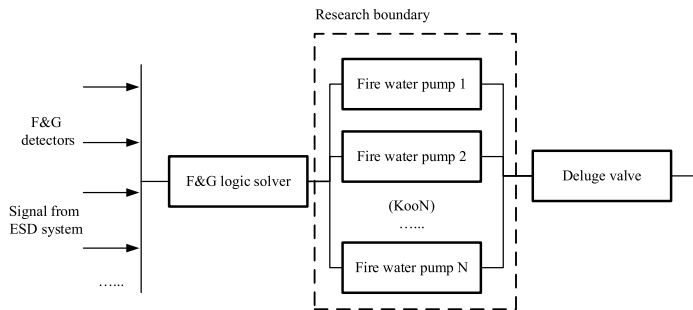


Fig. 5. Research boundary in fire water supply system.

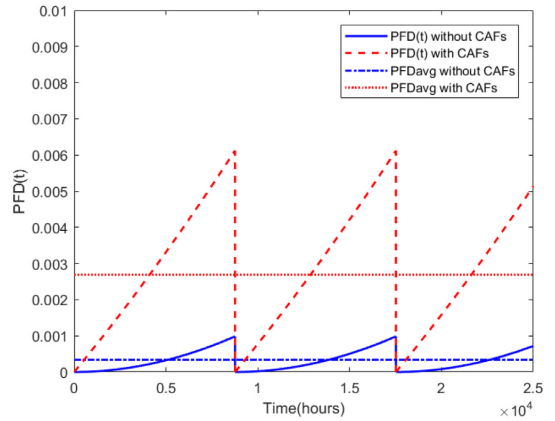


Fig. 6. PFD(t) without and with CAFs for 2003 system.

system), logic solver (for example F&G logic solver) and final elements (for example fire water pumps, deluge valves). Our study here is limited to firewater pumps that are structured in a $KooN$ configuration and are subject to CAFs, as shown in Fig. 5. In this case study, some situations like the system lose power and the logic solver fails, are beyond the delimitation.

The fire pump subsystem is a load-sharing system, where the pumps share common loads, such as water pressure. If one pump fails, the other pumps must carry the whole loads, and thus their failure rates can increase. Such failures are referred to as CAFs in the SIS.

5.2. PFD(t) and PFDavg with CAFs

Two configurations of such a SIS subsystem: 2003 and 1003 are considered in this subsection. The time to self-failures $F_i(t)$ for all the pumps is assumed to be distributed exponentially with constant failure rates of 2.1×10^{-6} per hour. The cascaded failure probability γ of each pump is set as a fixed value of 0.05. The relevant PFD(t) over time within three proof test intervals is calculated by Eqs. (8) and (9).

Figs. 6 and 7 illustrate PFD(t) with and without CAFs for 2003 and 1003 configurations, respectively. It is found that the effects of CAFs on 2003 configuration are more obvious than those on 1003 configuration. For the 2003 configuration, PFDavg increase dramatically from 3.4×10^{-4} to 2.7×10^{-3} , while PFDavg of the 1003 configuration rises from 1.6×10^{-6} to 6.9×10^{-5} . The absolute difference of PFDavg for 2003 configuration that are caused

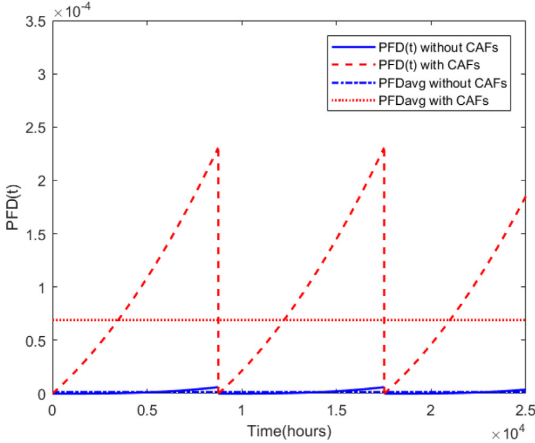


Fig. 7. PFD(t) without and with CAFs for 1003 system.

by CAFs is obviously bigger than that for 1003 configuration. It implies that the 2003 configuration is more sensitive to CAFs compared to the 1003 one. That is because only one cascade result in the failures within 2003 configuration. The implication to the SIS designer is to increase the number of N-K in the voting structure if the budget is allowed.

5.3. Effects of cascaded failure probability γ

To examine the effect of the cascading failure probability γ , the changes of PFD_{avg} and SILs are observed in different configurations when γ varying from 0 to 0.2. PFD_{avg} is calculated by the proposed formulas Eq. (15) for some selected typical configurations, such as 1002, 1003, 1004, 2003, 3004 and 2004 configurations. Fig. 8 illustrates how γ affects PFD_{avg} in different system configurations. It is obvious that the PFD_{avg} increases along with γ and the values of PFD_{avg} for 3004 and 2003 configurations are more sensitive to CAFs. A conclusion can be reached that CAFs have more significant influence on the PFD_{avg} when the value of N-K decrease. Particularly, if N-K is equal to one, the configurations are the most vulnerable to CAFs. On the other hand, when the configuration is limited as N-K=1, the effectiveness of reducing γ in controlling PFD_{avg} is higher.

It is essential to ensure that SISs can achieve required SIL requirement in operational phase. $\text{Log}_{10}(PFD_{avg})$ is used to illustrate corresponding SILs for these configurations in Fig. 9. The variation of SILs with different γ depends on configurations, namely the value of N-K. In this case, PFD_{avg} of the 1004 configuration is always within the range of SIL4. The values of PFD_{avg} for 2004 and 1003 configurations drop from the range of SIL4 to that of SIL3. The values of PFD_{avg} for 3004, 2003 and 1002 configurations change from SIL3 to SIL2.

The findings are helpful in determining SIL of SISs. When considering CAFs in SISs, their integrities are not only relying on the reliability of parallel components, but on the identified dependency of components and the system configurations. It shows that the impacts of CAFs on PFD_{avg} and SILs are unignorable regardless SIS configurations, especially when γ is not small. The results encourage the industry to put more efforts into analyzing and avoiding CAFs.

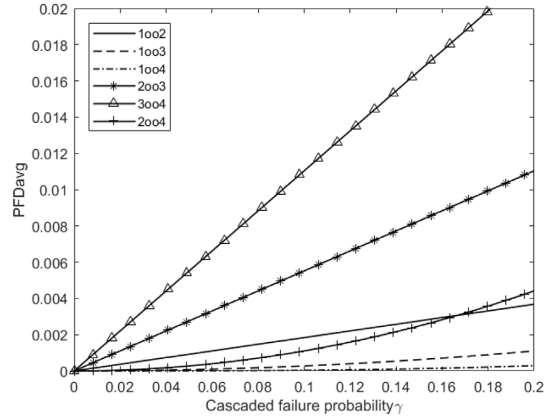


Fig. 8. PFD_{avg} of different configurations subject to CAFs.

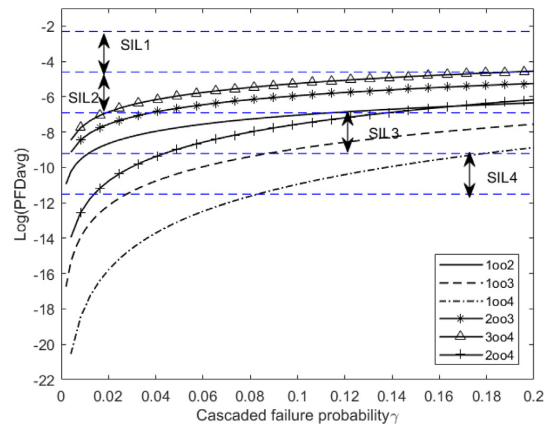


Fig. 9. $\text{Log}_{10}(PFD_{avg})$ of different configurations subject to CAFs.

5.4. The effects of CCFs and CAFs

To illustrate the need to consider the efforts of CAFs, we compare the effects of CCFs and CAFs on PFD_{avg} with different parameters, beta value β for CCFs and cascading intensity γ for CAFs. The configurations 2003 and 1003 are reconsidered in this subsection. According to Table 4, σ_{K00N} for 2003 and 1003 configurations are $3\gamma^2$ and 6. C_{K00N} for 2003 and 1003 configurations are 0.5 and 2. PFD_{avg} can be calculated by Eqs. (18) and (19), and the results are shown in Figs. 10 and 11. It is demonstrated that CAFs have comparable effects on PFD_{avg} and SIL as CCFs in this case.

The effects of CCFs and cascading failure on PFD_{avg} become more significant when the parameters increase. PFD_{avg} of the 2003 configuration considering CAFs is always higher than that of the same configuration considering CCFs. In a 1003 configuration, however, the effects of CCFs on PFD_{avg} are more significant than those from CAFs when the value of parameter is less than 0.17 approximately. Both two figures show that performance assessment of redundant SISs should be conservative since CAFs have comparable effects on PFD_{avg} and SIL as CCFs. It is noted that different configurations of SISs perform differently in terms of their vulnerabilities to CAFs and CCFs, even though the parameters of these two types of failures are set as equal.

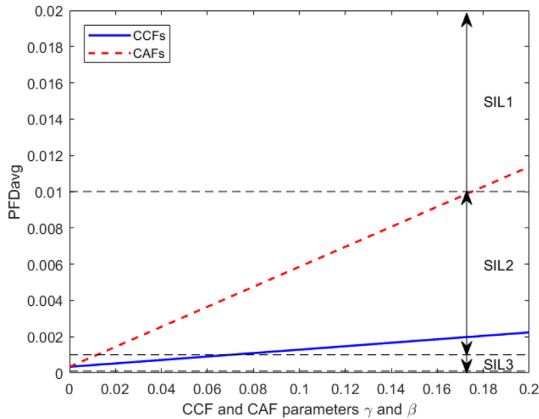


Fig. 10. The effects of CCFs and CAFs in 2oo3 systems.

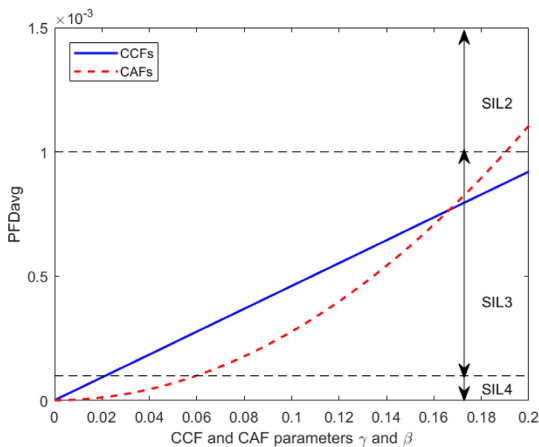


Fig. 11. The effects of CCFs and CAFs in 1oo3 systems.

The results of the case studies may increase the awareness to how CAFs can impact on the SIS performance and encourage that contribution of CAFs are considered in analyzes carried out design and in the operational phase. It is necessary to investigate the root causes and possible influence factors of CAFs. Possible solutions to decrease cascading intensities may include reducing functional dependence or sharing loads, enhancing absorptive ability and resistant capacity. In the operation phase, when determining proof test interval of SISs, the potential effects of CAFs should also be considered to ensure that the SISs can met SIL requirement.

6. Conclusions and future works

In this paper, a recursive aggregation-based approach has been developed for incorporating CAFs into reliability and availability analysis of SISs. General approximation formulas for PFD_{avg} of $KooN$ voted SISs have been proposed considering CAFs. The effects of cascading failures in the performance of SISs have been presented in comparison with those by CCFs. Numerical examples have shown that the contribution of CAFs towards PFD_{avg} relies on not only the cascaded failure probability, but also the system configurations. Such analysis can help designers and operators

better evaluate effects of dependent failures and estimate system performance of SISs. The proposed approach has been illustrated in the case study of SISs, but it must be highlighted that the analytical formulas can be more generally applied to other industrial $KooN$ voted systems.

Independent/self-failures are assumed to be exponential distribution because the exponential distribution is the most used life distribution in applied reliability analysis. However, many other distributions, such as Weibull distribution for many mechanical systems, can also be considered by using the convolutions in the approach.

In this paper, we assume constant cascading probability, which is rather restrictive. It is worthy to consider statistical dependency, such as time-dependent cascading probability between CAFs. Further, the future work can involve performance assessment for the SISs in high/continuous mode, where average frequency of failure (PFH) are used as a measure. New approximation formulas for these SISs are needed.

Another topic to be explored is how to allocate SILs to reduce required amount of risk with consideration of dependent failures, like CCFs and CAFs. Traditionally, the allocation process often excludes dependent failures that may exist within and between SISs. It is thus of interest to perform further studies on the SIL allocation considering dependent failures.

Declaration of competing interest

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

References

- [1] IEC61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: International Electrotechnical Commission; 2010.
- [2] IEC61511. Functional safety-safety instrumented systems for the process industry sector. Geneva: International Electrotechnical Commission; 2016.
- [3] Xie L, Håbrekke S, Liu Y, Lundteigen MA. Operational data-driven prediction for failure rates of equipment in safety instrumented systems: A case study from the oil and gas industry. *J Loss Prevent Process Ind* 2019;60:96–105.
- [4] Raus M. Reliability of safety-critical systems: Theory and applications. Hoboken, New Jersey, USA: John Wiley & Sons; 2014.
- [5] Hauge S, Kråkenes T, Hokstad P, Håbrekke S, Jin H. Reliability prediction method for safety instrumented systems-PDS method handbook. Trondheim, Norway: SINTEF; 2013.
- [6] Liu Y, Raus M. Reliability assessment of safety instrumented systems subject to different demand modes. *J Loss Prevent Process Ind* 2011;24(1):49–56.
- [7] Summers AE, Raney G. Common cause and common sense, designing failure out of your safety instrumented systems (SIS). *ISA Trans* 1999;38(3):291–9.
- [8] ISO/TR12489. Petroleum, petrochemical and natural gas industries—Reliability modelling and calculation of safety systems. 2013.
- [9] Biswal GR, Maheshwari RP, Dewal M. System reliability and fault tree analysis of SeSHRS-based augmentation of hydrogen: Dedicated for combined cycle power plants. *IEEE Syst J* 2012;6(4):647–56.
- [10] Levitin G, Xing L. Reliability and performance of multi-state systems with propagated failures having selective effect. *Reliab Eng Syst Saf* 2010;95(6):655–61.
- [11] Xing L, Levitin G, Wang C, Dai Y. Reliability of systems subject to failures with dependent propagation effect. *IEEE Trans Syst Man Cybern Syst* 2013;43(2):277–90.
- [12] Rausand M, Høyland A. System reliability theory: Models, statistical methods, and applications. 2nd ed. Hoboken, New Jersey, USA: John Wiley & Sons; 2004.
- [13] Xie L, Lundteigen MA, Liu YL. Common cause failures and cascading failures in technical systems: similarities, differences and barriers. In: European safety and reliability conference (ESREL). Trondheim: NTNU; 2018.
- [14] Levitin G. A universal generating function approach for the analysis of multi-state systems with dependent elements. *Reliab Eng Syst Saf* 2004;84(3):285–92.

- [15] Motter AE, Lai Y-C. Cascade-based attacks on complex networks. *Phys Rev* 2002;66(6):065102.
- [16] Albert R, Barabási A-L. Statistical mechanics of complex networks. *Rev Modern Phys* 2002;74(1):47–97.
- [17] Zio E, Sansavini G. Component criticality in failure cascade processes of network systems. *Risk Anal* 2011;31(8):1196–210.
- [18] Crucitti P, Latora V, Marchiori M. Model for cascading failures in complex networks. *Phys Rev E* 2004;69(4):045104.
- [19] Cozzani V, Gubinelli G, Antonioni G, Spadoni G, Zanelli S. The assessment of risk caused by domino effect in quantitative area risk analysis. *J Hazard Mater* 2005;127(1–3):14–30.
- [20] Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliab Eng Syst Saf* 2001;71(3):249–60.
- [21] Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. *Nature* 2010;464(7291):1025–8.
- [22] Iyer SM, Nakayama MK, Gerbessiotis AV. Markovian dependability model with cascading failures. *IEEE Trans Comput* 2009;58(9):1238–49.
- [23] Xie L, Lundteigen MA, Liu Y. Reliability and barrier assessment of series-parallel systems subject to cascading failures. *Proc. Inst. Mech. Eng. O* 2020;234(3):455–69.
- [24] Zhao G, Xing L. Reliability analysis of IoT systems with competitions from cascading probabilistic function dependence. *Reliab Eng Syst Saf* 2020;198:106812.
- [25] Murthy D, Nguyen D. Study of two-component system with failure interaction. *Nav Res Logist* 1985;32(2):239–47.
- [26] Liu B, Wu J, Xie M. Cost analysis for multi-component system with failure interaction under renewing free-replacement warranty. *European J Oper Res* 2015;243(3):874–82.
- [27] Jin H, Lundteigen MA, Raus M. New PFH-formulas for k-out-of-n: F-systems. *Reliab Eng Syst Saf* 2013;111:112–8.
- [28] Abdolhamidzadeh B, Abbasi T, Rashtchian D, Abbasi SA. A new method for assessing domino effect in chemical process industry. *J Hard Mater* 2010;182(1–3):416–26.

This page is intentionally left blank

Article VI

Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Performance Assessment of Safety-instrumented Systems Subject to Cascading Failures in High-demand Mode. *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, September 22-26, 2019, Hannover, Germany.

This page is intentionally left blank

Performance Assessment of Safety-instrumented Systems Subject to Cascading Failures in High-demand Mode

Lin Xie, Mary Ann Lundteigen & Yiliu Liu

*Department of mechanical and industrial engineering, Norwegian university of science and technology, Norway.
E-mail: lin.xie@ntnu.no*

Elias Kassa

Department of civil and environmental engineering, Norwegian university of science and technology, Norway.

Shengyang Zhu

Department of train and track research institute, State key laboratory of traction power, Southwest jiaotong university, China.

Safety-instrumented systems are designed to act upon hazardous events and reinforce safety. IEC 61508 specifies two possible reliability measures of safety-instrumented systems: the average probability of failure on demand for low-demand mode systems, and average frequency of dangerous failures for high/continuous-demand mode systems. Redundancy is applied to ensure the reliability of safety-instrumented systems so that they are commonly constructed as K -out-of- N systems. The potential effects of dependency must therefore be included in the reliability analysis. So far, both standards and literature focus primarily on common cause failures as the source of dependencies. With the technology trends (e.g. cyber-physical and programmable electronic technologies), cascading failures caused by functional dependencies and shared resources may be issues in the implementation of safety-instrumented systems. Few attempts have been made to investigate the effects of cascading failures in the reliability of safety-instrumented systems. This paper aims to propose approximation formulas for average frequency of dangerous failures for high/continuous-demand mode systems that are subject to cascading failures. This research is an extension of previous research where the focus was directed to low-demand mode systems.

Keywords: Safety-instrumented systems, cascading failures, high-demand mode, PFH.

1. Introduction

Safety-instrumented systems (SISs) are designed to act upon hazardous events and reinforce safety in many applications, such as process industry, public transportation, and critical infrastructure (Rausand 2014). A SIS performs one or more safety-instrumented functions (SIFs) to protect the equipment under control (EUC) against a specific hazardous event, namely a demand (IEC61508 2010). A SIS generally comprises three main subsystems in a series structure: sensor(s) (e.g. level transmitters, gas detectors, and obstacle detector), logic solver(s) (e.g. programmable logic controller, and industrial computer) and final element(s) (e.g. shutdown valves, and circuit breakers). Sensors identify the possible hazardous situations, logic solvers decide what to do, and final elements take actions to respond to negations.

According to IEC 61508 (2010), the operational modes of SISs include low-demand and high/continuous-demand mode. Once per year the frequency of demands is suggested to be the borderline of two modes (IEC61508 2010).

Many authors have studied the difference between low-demand and high/continuous-demand systems (Liu 2014, Innal et al. 2010, Liu and Rausand 2011). The average probability of failure on demand (PFD_{avg}) is proposed as the reliability measure for SISs operating in the low-demand mode, while the average frequency of a dangerous failure per hour (PFH) is used when operating in the high/continuous-demand mode. The calculated PFD or PFH is one out of several inputs that decide the safety integrity level (SIL) achieved for a safety instrumented function (SIF) carried out by a SIS. IEC 61508 defines four different SILs, where SIL 1 is the lowest level and SIL 4 is the highest (IEC61508 2010).

PFD_{avg} and PFH may be calculated on the basis of several methods: simplified formulas (Rausand 2014), IEC 61508 formulas (IEC61508 2010), PDS method (Hauge et al. 2013), fault tree analysis (Jin et al. 2013), Markov methods (Liu and Rausand 2011) and petri nets (Rausand 2014). Among those methods, simplified formulas are the most widely accepted to assess the performance of SISs due to their simplicity.

Proceedings of the 29th European Safety and Reliability Conference.

Edited by Michael Beer and Enrico Zio

Copyright ©2019 by ESREL2019 Organizers. *Published by* Research Publishing, Singapore

ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2019-paper

It is often necessary to introduce redundancy to achieve the required value of PFD or PFH for the SIF. Redundancy may be introduced to one or more subsystems, i.e. to the sensor system, logic solver system, or actuated devices system. The use of redundancy implies that it is necessary to incorporate the effects of dependent as well as independent failures (Torres-Echeverria et al. 2009). So far, IEC 61508, its related standards, and literature in general focus primarily on common cause failures (CCF) as dependent failures. CCFs are characterized by the failures of two or more components due to a shared cause. CCFs are often modeled by the standard beta-factor model and the multiple beta-factor model (Rausand and Høyland 2004, Hauge et al. 2013). With the development of technology (e.g. cyber-physical and programmable electronic technologies), cascading failures may be another type of failures resulting from dependency in technical systems. Cascading failures are the multiple failures in a chain reaction that are initiated by the failure of one component in the system (Rausand and Høyland 2004). Such kind of failures can propagate from one component to others owing to functional dependencies, shared loads and resources, and hazardous events. The differences between cascading and CCFs have been discussed in the previous work (Xie et al. 2018).

Cascading failures occur frequently within the SISs in the high/continuous-demand mode. For example, one channel's failure in a flow transmission system may result in an increase of loads on others, which trigger cascading failures on the others (Levitin 2004). Cascading failures influence significantly system performance of critical infrastructure systems, such as signal systems and transport network in railway industry (Zimmerman and Restrepo 2009, Wang et al. 2018). The effects of cascading failures have been studied intensively in literature (Xing et al. 2014, Xing et al. 2018, Liu et al. 2015, Liu et al. 2016, Levitin 2004). Topological approaches are also motivated by the complex network theory to analyze and mitigate the cascading impacts on system connectedness and robustness (Motter and Lai 2002, Albert and Barabási 2002, Zio and Sansavini 2011, Crucitti et al. 2004, Golnari and Zhang 2015).

A careful literature study has revealed that there have been few attempts to model the effects of cascading failures on the SIS reliability. The objective of this paper is therefore to propose an approach for incorporating the effects of cascading failures in analytical formulas for PFH. The focus of this paper is given to

high/continuous demand mode system because this research is an extension of previous research where the focus was directed to low-demand mode systems. The new formulas are applied as a case study in a railway signaling system.

The remaining parts of the paper is structured as follows: section 2 explains definitions of PFH and cascading failures. Sections 3 presents approximation formulas for PFH with consideration of cascading failures. In section 4, case studies in railway industry are employed to illustrate the effects of cascading failures. Section 5 contains conclusions and discussions.

2. Definitions and Assumptions

This section presents several basic concepts and assumptions in relation to PFH and cascading failures.

2.1. PFH

PFH is a reliability measure that incorporates the effects of dangerous failures. A dangerous failure is a failure that brings the components into a state where it is not able to perform its safety functions (IEC61508 2010). Some dangerous failures may be detected by online diagnostics, and are then referred to as dangerous detected (DD) failures. Dangerous failures that may only be revealed by regular tests or during the execution of the SIF. These failures are therefore referred to as dangerous undetected (DU) failures. We assume that the EUC is brought to a safe state upon a DD failure, or corrected in due time before the next demand. DD failures are therefore disregarded in the calculation of PFH.

The PFH may be regarded as an average failure rate, calculated in a period of length τ . During this period, it is assumed that the components' failure rates are constant. This means that necessary maintenance and inspections are carried out as needed. At the end of the period τ , a more thorough test and renewal may be carried out, but not always. In the high-demand mode, most failures are revealed upon demands, and they are therefore corrected immediately.

The PFH for a single component for given time period of length τ can be define as (Rausand 2014):

$$PFH = \frac{\text{Mean No. of DU failures in } (0, \tau)}{\tau} = \frac{F(\tau)}{\tau} \quad (1)$$

It is assumed that measures such as regular inspections and maintenance are taken to ensure that the components' failure rate remain constant during the period.

For a subsystem voted k-out-of-n (*koon* system), we may introduce the term dangerous failures

(DGF). In the presence of a DGF, the subsystem loses its ability to perform the safety function. The PFH for a DGF in a period $(0, \tau)$:

$$\begin{aligned} PFH_G^{(koon)} &= \frac{\text{Mean No. of DGFs in } (0, \tau)}{\tau} \\ &= \frac{Pr(N(\tau) \geq n-k+1)}{\tau} \end{aligned} \quad (2)$$

Here, $N(\tau)$ denotes the number of dangerous failures of *koon* system, and a DGF occurs when the number of dangerous failures is more than $n - k + 1$.

2.2. Cascading Failures

Cascading failures are multiple failures that are initiated by other components' failures (Rausand and Høyland 2004). In the literature, we have identified alternative terms with similar meaning, such as induced failures, domino failures, propagating errors and interaction failures in literatures (Abdelmoez et al. 2004, Cozzani et al. 2005, Murthy and Nguyen 1985).

For the development of formulas for PFH with the effects of cascading failures included, we have made the following assumptions:

- All components in a subsystem of SISs are identical and are organized as *koon* configurations.
- Only two states are taken into account for all the components: either functioning, or completely failed;
- All components may suffer from independent failures (i.e. DU failures) and cascading failures;
- Independent failures are characterized by distribution function $F(t)$, and are assumed as an exponential distribution with a constant failure rate λ_{DU} . This constant failure rates is assumed to be 1.5×10^{-6} per hour in this paper;
- Delays in the propagations of cascading failures are rather short and can be ignored;
- A cascading probability, namely $\gamma_{ij}(t) \in (0, 1]$ ($i \neq j$), is introduced to reflect the easiness of failure propagation from component i to component j in case that the former one has failed. The cascading probability is expressed as:

$$\gamma_{ij}(t) = Pr\left(\frac{\text{comp. } j \text{ fails by } t}{\text{comp. } i \text{ has failed}}\right) \quad (3)$$

- This cascading probability $\gamma_{ij}(t)$ can be estimated based on test data or historic failure data by either parametric or

nonparametric techniques. To simplify the analysis, $\gamma_{ij}(t)$ is assigned as a constant γ for all the components in this paper.

- For a system with n components, cascading probabilities can be arranged as a matrix $\boldsymbol{\gamma}$ that represents failure propagation between the components.

3. Approximation Formulas of PFH

Consider a *koon* system that are subject to cascading failures. The system fails as soon as at least $n - k + 1$ components fail. The failure of a component can be an independent failure occurring on itself and a dependent failure cascaded from the others. According to Eq. (2), the average PFH for *koon* system can be defined as:

$$PFH_G^{(koon)} = \frac{Pr(N_I(\tau) + N_C(\tau) \geq n-k+1)}{\tau} \quad (4)$$

$N_I(\tau)$ denotes the number of independent failures and $N_C(\tau)$ denotes the number of cascading failures.

Take a 1oo2 system that is subject to independent failures and cascading failures as an example. The 1oo2 system fails with two independent failures or one independent failure as well as one cascading failure. The PFH for this system can be calculated by:

$$\begin{aligned} PFH_G^{(1oo2)} &= \frac{Pr(N_I(\tau)=2) + Pr(N_I(\tau)=1 \& N_C(\tau)=1)}{\tau} \\ &= \frac{\binom{1-e^{-\lambda_{DU}\tau}}{2} + \binom{2}{1}(1-e^{-\lambda_{DU}\tau})e^{-\lambda_{DU}\tau}\gamma}{\tau} \end{aligned} \quad (5)$$

Where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

By using the approximation $1 - e^{-\lambda_{DU}\tau} \approx \lambda_{DU}\tau$ and $e^{-\lambda_{DU}\tau} \approx 1$, Eq. (6) can be approximated by:

$$PFH_G^{(1oo2)} \approx \lambda_{DU}^2 \tau + 2 \lambda_{DU} \gamma \quad (6)$$

Note that only one DGF is concerned in period of interest, since SISs are highly reliable. Similarly, for a 2oo3 system, the PFH can be expressed as:

$$\begin{aligned} PFH_G^{(2oo3)} &= \frac{Pr(N_I(\tau)=2) + Pr(N_I(\tau)=1 \& N_C(\tau)=1)}{\tau} \\ &= \frac{\binom{3}{2}(1-e^{-\lambda_{DU}\tau})^2 + \binom{3}{1}\binom{2}{1}(1-e^{-\lambda_{DU}\tau})(e^{-\lambda_{DU}\tau})^2 \gamma}{\tau} \\ &\approx 3\lambda_{DU}^2 \tau + 6 \lambda_{DU} \gamma \end{aligned} \quad (7)$$

With consideration of independent failures and cascading failure, Table 1 presents approximation formulas for the different structures of SISs.

Table 1. PFH of various structures with independent failures and cascading failures

System	PFH
1oo2	$\lambda_{DU}^2\tau + 2\lambda_{DU}\gamma$
1oo3	$\lambda_{DU}^3\tau^2 + 6\lambda_{DU}^2\tau\gamma + 3\lambda_{DU}\gamma^2$
2oo3	$3\lambda_{DU}^2\tau + 6\lambda_{DU}\gamma$
1oo4	$\lambda_{DU}^4\tau^3 + 12\lambda_{DU}^3\tau^2\gamma + 12\lambda_{DU}^2\tau\gamma^2 + 4\lambda_{DU}\gamma^3$
2oo4	$4\lambda_{DU}^3\tau^2 + 24\lambda_{DU}^2\tau\gamma + 12\lambda_{DU}\gamma^2$
3oo4	$6\lambda_{DU}^2\tau + 12\lambda_{DU}\gamma$

The approximation formulas of PFH for *koon* systems can be generalized as:

$$\begin{aligned}
 & PFH_G^{(koon)} \\
 &= \binom{n}{n-k+1} \lambda_{DU}^{n-k+1} \tau^{n-k} \\
 &+ \binom{n}{n-k} \binom{n-k}{1} \binom{k}{1} \lambda_{DU}^{n-k} \tau^{n-k-1} \gamma \\
 &+ \binom{n}{n-k-1} \binom{n-k-1}{1} \binom{k+1}{2} \lambda_{DU}^{n-k-1} \\
 &\tau^{n-k-2} \gamma^2 + \dots + \binom{n}{1} \binom{n-1}{n-k} \lambda_{DU} \gamma^{n-k} \quad (8)
 \end{aligned}$$

We assume that $\lambda_{DU}\tau$ and γ are significantly small (e.g. $\lambda_{DU}\tau \leq 0.1$) to obtain adequacy of the formula (Rausand 2014). It is therefore not valid for very long period τ .

4. Case Study

To illustrate the effects of cascading failures, a case study is used in this section. Consider a European vital computer (EVC) system in European Train Control System (ETCS). EVC, as the core part of ETCS onboard sub-system, is a computer-based system that supervises the movement of the train and can apply the emergency brake if necessary. It can be regarded as an embedded real-time SIS that handles telegrams from balises and measures the train speed and position. Such a SIS is widely employed in high-speed railways in Europe.

The dual-duplex system and triple modular redundancy system are two typical redundancy strategies for EVC. The reliability block diagrams (RBDs) show the logical functions of EVCs, as illustrated in Fig.1 (a) and Fig.1 (b). We use 1oo2 (Fig.1 (a)) to simplify the dual-duplex system and 2oo3 (Fig.1 (b)) for the triple modular redundancy system. To ensure that the same outputs (i.e. calculations) are performed in parallel by two or three components, a macro-synchronization procedure is performed beforehand. This is achieved through specific point-to-point serial links between the components. In those cases, all components share the same power/bus system and working

environment, which may cause the cascading failures. In case that one component of EVC fails, the failure probability of other single component will rise. That can be reflected by cascading probability γ .

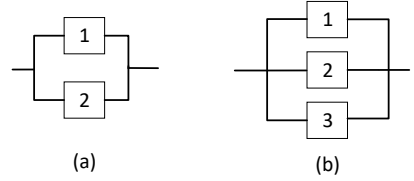


Fig. 1 RBD of EVCs

To simplify the analysis, γ is assumed to be a fixed value for all cascades between components, varying from 0 to 1. The independent DU failures are distributed exponentially with constant failure rates λ_{DU} of 1.5×10^{-6} per hour. In this case study, it is assumed that the period τ is corresponding to a periodic test interval, to ensure that any DU failure in redundant channels are identified. The regular test interval τ is assigned to be one month. The values of failure rates and test interval are taken from typical datasheets (Flammini et al. 2006).

By using Eq. (8) proposed in section 3, the PFH for 1oo2 and 2oo3 of EVC with different cascading probability γ ($0 \leq \gamma \leq 1$) are shown in Fig. 2. It is obvious that the PFH increases along with the increase of γ . The values of PFH of 2oo3 system is more sensitive to cascading failures.

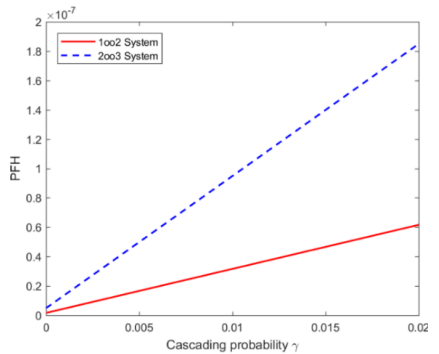


Fig. 2 PFH of 1oo2 and 2oo3 EVCs with DU failures and cascading failures

$\text{Log}_{10}(\text{PFH})$ is used to illustrate the effects of cascading failures on the two structures, as shown in Fig. 3. The variation of SILs with different γ corresponds to the structures of

EVC. In this case, for both 1oo2 and 2oo3 EVC, the values of PFH drop from SIL4 to SIL2. Even though the value of cascaded failure probability γ is small (e.g. $\gamma < 0.05$) when we maintain other parameters, the systems cannot fulfil the requirement of SIL4. Such findings emphasize the importance of the contribution from the cascading failures on SISs. It also implies that the capacity of SISs to prevent cascading failures escalating into system failures, can be achieved by reducing the value of cascading failure probabilities γ .

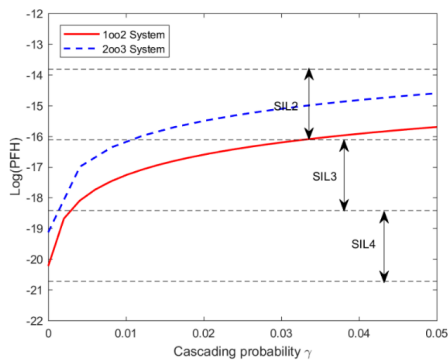


Fig. 3 SILs of 1oo2 and 2oo3 EVCs with DU failures and cascading failures

5. Conclusions And Further Work

In this paper, approximation formulas have been derived for PFH of SISs in high/continues mode that are subject to cascading failures. The proposed formulas can be applied to other industrial systems that are susceptible to cascading failures.

Numerical examples illustrating the effects of cascading failures are presented. The paper demonstrates that the contribution of cascading failures towards PFH relies on the cascading failure probability. The cascading failure possibly could lead to unacceptable SIL for the SISs even though the value of cascading probability is rather small. In cases where the effects of cascading failures is substantial, it dominates reliability measures. This analysis helps decision making process for maintenance and inspection strategies.

The future work will involve further barrier analysis in SISs with consideration of cascading failures. The effects of different barriers in terms of cascading failure probabilities will be assessed.

Acknowledgement

This work was supported partly by the Rail Infrastructure Systems Engineering Network (RISEN) project (GA691135, <http://www.risen2rail.eu>). The professors from train and track research institute in Southwest Jiaotong University of China and Norwegian University of Science and Technology are acknowledged.

References

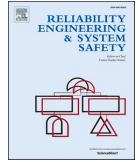
- Abdelmoez, W., D. Nassar, M. Shereshevsky, N. Gradetsky, R. Gunnalan, H. H. Ammar, B. Yu, and A. Mili. (2004). Error propagation in software architectures. *Software Metrics*, 2004. Proceedings. 10th International Symposium on.
- Albert, R., and A.-L. Barabási. (2002). Statistical mechanics of complex networks. *Reviews of modern physics* 74 (1), 47-97.
- Cozzani, V., G. Gubinelli, G. Antonioni, G. Spadoni, and S. Zanelli. (2005). The assessment of risk caused by domino effect in quantitative area risk analysis. *Journal of hazardous Materials* 127 (1-3), 14-30.
- Crucitti, P., V. Latora, and M. Marchiori. (2004). Model for cascading failures in complex networks. *Physical Review E* 69 (4), 045104.
- Flammini, F., S. Marrone, N. Mazzocca, and V. Vittorini. (2006). Modelling system reliability aspects of ERTMS/ETCS by fault trees and Bayesian networks. Proc. European Safety and Reliability Conference, ESREL.
- Golnari, G., and Z.-L. Zhang. (2015). The effect of different couplings on mitigating failure cascades in interdependent networks. 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPs).
- Hauge, S., T. Kråkenes, P. Hokstad, S. Håbrekke, and H. Jin. (2013). *Reliability prediction method for safety instrumented systems-pds method handbook*. Vol. 6031, SINTEF report. Trondheim, Norway: SINTEF.
- IEC61508. (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. Review of Reviewed Item. *Journal Volume (Issue)*.
- Innal, F., Y. Dutuit, A. Rauzy, and J. Signoret. (2010). New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk Reliability* 224 (2), 75-86.
- Jin, H., M. A. Lundteigen, and M. Rausand. (2013). New PFH-formulas for k-out-of-n: F-systems.

- Reliability Engineering System Safety* 111, 112-118.
- Levitin, G. (2004). A universal generating function approach for the analysis of multi-state systems with dependent elements. *Reliability Engineering & System Safety* 84 (3), 285-292.
- Liu, B., J. Wu, and M. Xie. (2015). Cost analysis for multi-component system with failure interaction under renewing free-replacement warranty. *European Journal of Operational Research* 243 (3), 874-882.
- Liu, B., M. Xie, and W. Kuo. (2016). Reliability modeling and preventive maintenance of load-sharing systems with degrading components. *IIE transactions: industrial engineering research & development* 48 (8), 699-709.
- Liu, Y. (2014). Discrimination of low-and high-demand modes of safety-instrumented systems based on probability of failure on demand adaptability. *Journal of Risk Reliability* 228, 409-418.
- Liu, Y., and M. Rausand. (2011). Reliability assessment of safety instrumented systems subject to different demand modes. *Journal of Loss Prevention in the Process Industries* 24 (1), 49-56.
- Motter, A. E., and Y.-C. Lai. (2002). Cascade-based attacks on complex networks. *Physical Review* 66 (6), 065102.
- Murthy, D., and D. Nguyen. (1985). Study of two-component system with failure interaction. *Naval Research Logistics (NRL)* 32 (2), 239-247.
- Rausand, M. (2014). *Reliability of safety-critical systems: theory and applications*. Hoboken, New Jersey, USA: John Wiley & Sons.
- Rausand, M., and A. Høyland. (2004). *System reliability theory: models, statistical methods, and applications*. 2nd ed. Vol. 396. Hoboken, New Jersey, USA: John Wiley & Sons.
- Torres-Echeverria, A., S. Martorell, and H. Thompson. (2009). Design optimization of a safety-instrumented system based on RAMS+ C addressing IEC 61508 requirements and diverse redundancy. *Reliability Engineering System Safety* 94 (2), 162-179.
- Wang, W., S. Yang, F. Hu, H. E. Stanley, S. He, M. J. P. A. S. M. Shi, and i. Applications. (2018). An approach for cascading effects within critical infrastructure systems. 510, 164-177.
- Xie, L., M. A. Lundteigen, and Y. L. Liu. (2018). Common cause failures and cascading failures in technical systems: similarities, differences and barriers European Safety and Reliability Conference (ESREL), Trondheim.
- Xing, L., B. A. Morrisette, and J. B. Dugan. (2014). Combinatorial reliability analysis of imperfect coverage systems subject to functional dependence. *IEEE Transactions on Reliability* 63 (1), 367-382.
- Xing, L., G. Zhao, Y. Wang, and L. Mandava. (2018). Competing Failure Analysis in IoT Systems with Cascading Functional Dependence. 2018 Annual Reliability and Maintainability Symposium (RAMS).
- Zimmerman, R., and C. E. Restrepo. (2009). Analyzing cascading effects within infrastructure sectors for consequence reduction. 2009 IEEE Conference on Technologies for Homeland Security.
- Zio, E., and G. Sansavini. (2011). Component criticality in failure cascade processes of network systems. *Risk Analysis* 31 (8), 1196-1210.

Article VII

Xie, Lin; Lundteigen, Mary Ann; Liu, Yiliu. Performance analysis of safety instrumented systems against cascading failure during prolonged demand. *Reliability engineering and safety system* (2021); Volume 216. s. 107975.

This page is intentionally left blank



Performance analysis of safety instrumented systems against cascading failures during prolonged demands

Lin Xie, Mary Ann Lundteigen, Yiliu Liu^{*}

Norwegian University of Science and Technology, Trondheim, Norway

ARTICLE INFO

Keywords:

Cascading failure
Safety instrumented system
Demand
Reliability block diagram
System reliability

ABSTRACT

Cascading failures may occur in many technical systems where the failure of one component triggers successive events. Safety barriers like safety instrumented systems are installed in many industries to prevent failures and failure propagations. However, little attention has been paid to the impacts of safety instrumented systems employed to prevent cascading failures in the literature. This paper proposes a novel method for analyzing how the performance of safety instrumented systems influences the protection against and mitigation of cascading failures. It considers SIS reliability and SIS durability in the mitigation of cascading failures. The method uses recursive aggregations based on the reliability block diagram and is verified with Monte Carlo simulations. The application is illustrated with a practical case study, where the proposed method is found beneficial to identify the criticality of safety instrumented systems in consideration of their locations and performance.

1. Introduction

Cascading failures (CAFs) are multiple failures in which the failure of one component leads to high stress and a consequently high failure probability in other components [1]. CAFs are a concern for many technical systems, such as railway signaling systems, power distribution networks, process systems, industrial communication networks, and internet systems [2,3]. Functional dependencies and interactions exist commonly among components, and thus a single failure can negatively influence other parts in the same system. As a result, CAFs may cause catastrophes in technical systems without proper preventions and mitigations [4,5].

The awareness of CAFs is not new. In the past decade, much research has aimed at developing models to evaluate the effects of CAFs and associated preventive measures. These models can be categorized as topological, probabilistic, state-transition, and simulations. In the context of topological models, some efforts have been devoted to assessing mitigation measures of CAFs based on complex network theory [6–9] and graph theory [10–12]. Probabilistic models have been applied to quantify the ability of preventions against CAFs in risk propagations [13–16]. State-transition models, such as Markov processes, Petri nets, and Bayesian networks, have effectively analyzed CAFs [17–21]. Besides, simulations like the Monto Carlo simulation (MCS) have been used

in analyzing the systems associated with CAFs in many application areas, including power and gas networks, traffic-power, and infrastructure systems [22–24].

To prevent CAFs, Safety instrumented systems (SISs) can install as a type of safety barrier. SISs are widely employed to reduce accidents in the process industries and other sectors [25]. An SIS applies electrical/electronic/programmable electronic (E/E/PE) technologies to detect and act upon hazardous situations arising in the assets [26]. The assets can be humans, equipment, or process sections. They are called equipment under control (EUC) in the generic standard IEC 61508 [26]. An SIS generally consists of three main subsystems: sensors (e.g., level transmitters, gas detectors, and push buttons), logic solvers (e.g., programmable logic controllers and industrial computers), and final elements (e.g., shutdown valves and circuit breakers). As illustrated in Fig. 1, the sensors detect possible abnormal situations (e.g., CAFs), and the logic solvers activate, then the final elements act according to the sensor inputs. The event upon which an SIS is activated is considered a demand [1]. A typical example of SISs to prevent CAFs is an automatic fire extinguishing system (AFES)¹. An AFES activates when a fire or gas leakage at a tank is detected. If the SIS fails to extinguish or control the fire at a specific time, the fire can propagate and affect several facilities [27].

SIS performance is of great significance to ensure the safety of EUC systems [28]. Several indicators can reflect SIS performance, such as

^{*} Corresponding author.

¹ There has been debate over the categorization of fire extinguishing systems as SISs, but they are included in SISs in this paper since Petroleum Safety Authority (PSA) in Norway and Guideline 070 consider such systems as SISs.

Nomenclature			
CAF	cascading failure	RBD	reliability block diagram
SIS	safety instrumented system	EUC	equipment under control
AFES	automatic fire extinguishing system	SIL	safety integrity level
PFDF	probability of failure on demand	PFDF _{avg}	average PFDF in a test interval
FOD	failure on demand	FDD	failure during demand
MCS	Monte Carlo simulation	RAW	risk achievement worth
EUC _i	EUC component <i>i</i>	<i>t</i>	observing time
<i>t_i</i>	EUC _i fails at time <i>t_i</i>	SIS _{ij}	SIS between EUC _i and EUC _j
<i>T_{DD}</i>	demand duration	<i>μ</i>	time at an FDD occurrence
<i>f_{SIS_i}(t)</i>	probability density function of time to failures in SIS _i	<i>f_i(t)</i>	probability density function of time to failures in EUC _i
<i>R_i(t)</i>	conditional reliability of EUC _i by time <i>t</i>	$\tilde{R}_{\Omega_{n-F}}(t)$	conditional reliability of subsystem Ω_{n-F} by time <i>t</i>
<i>θ_ν(t)</i>	probability that CAF event <i>ν</i> occurs by time <i>t</i>	<i>η, η₁</i>	random variable generated from a uniform [0, 1] in simulations
<i>δ_{h,g}(t)</i>	probability that EUC _h fails and <i>g</i> SIS event occurs by time <i>t</i>	<i>Q_ν(t)</i>	conditional probability for <i>ν</i> CAF event by time <i>t</i>
<i>λ_{SIS}</i>	scale parameter of Weibull distribution for SIS	<i>α_{SIS}</i>	shape parameter of Weibull distribution for SIS
<i>T(λ_{SIS})</i>	simulated time to failure within SIS with <i>λ_{SIS}</i>	<i>T_i(λ_i)</i>	simulated time to failure within EUC _i with <i>λ_i</i>
<i>γ_i</i>	probability that failures are cascaded from EUC _i	<i>T_{SIS}</i>	operating time of SIS from activation to the failed state

specificity, functionality, reliability, response time, capacity, durability, robustness, audit-ability, and independence [25,29,30]. Among them, reliability is the most crucial for SISs since it expresses the ability of an SIS to protect EUC systems at a specific time [1].

The SIS reliability is related to the ability to respond on-demand as expected. For example, when a fire occurs, an AFES is expected to start to splash water. If an SIS works on-demand, it is reliable. However, many SIS failures cannot be detected immediately after their occurrences. Instead, those failures can be revealed upon actual demands or periodical proof tests with noticeable delays. Such failures are called failures on demand (FODs). In applications, a specific measure, the probability of failure on demand (PFDF), is widely applied for FODs of SISs [26]. If the proof test intervals are fixed, the average PFDF within one interval as PFDF_{avg} is a commonly used reliability measure [22]. PFDF_{avg} can be obtained by simplified formulas [1], IEC 61508 formulas [26], the PDS method [31], and Markov models [19,32].

In recent years, PFDF_{avg} and SIS reliability have been intensively studied. For example, Cai et al. [28] have proposed a method for evaluating SISs with heterogeneous components based on Bayesian networks. Liu and Rausand have considered different demand modes for the SIS reliability analysis [19,33]. Alizadeh and Sriramula [34] have developed an unreliability model for redundant SISs using Markov chains. Meng et al. [35] have modeled the SIS reliability measures in AltaRica 3.0. Xie et al. [36] have considered the reliability of redundant SISs where dependent failures may occur. An analytical approach for simplification of complex Markov model has been proposed in SIS reliability analysis [37]. In addition, Ding et al. [38] have derived a diverse redundancy method based on system degradation using a reliability block diagram to evaluate the SIS reliability. Yu et al. [39] have

proposed a fuzzy reliability assessment for SIS taking account of common cause failures.

However, little attention has been paid to the impacts of SISs employed to protect against CAFs. In addition, the currently defined SIS reliability is insufficient to evaluate the overall SIS performance in preventing and mitigating CAFs. That is because the demands on SISs for preventing or mitigating CAFs may not be instantaneous [3]. As a result, even though an SIS can respond to demands, it may fail afterward. For example, fires can last few seconds or several days, and AFESs must operate for a specified period to suppress fires. Such a period is defined as a prolonged demand duration. During this period, SISs are often exposed to high stress and thereby have more chances to fail.

Therefore, it is of interest to examine whether an SIS is reliable while responding and how an SIS performs after activation. The former is related to SIS reliability, whereas the latter is related to SIS durability. Durability represents how long an SIS can perform its safety instrumented functions and withstand stress. The failures related to durability are called failures *during* demand (FDDs) in this study. In other words, SISs that are employed against CAFs may suffer from intensive degradations and failure before demands are complete.

Considering both FODs and FDDs, it is thus challenging to use straightforward traditional methods to evaluate the SISs against CAFs. For example, fault tree analysis is often used for the specific analysis of the accident, and it is difficult to cope with dependent issues such as CAFs [40]. In addition, Markov models have a problem in dealing with a large-scale system where CAFs occur [37,41]. Furthermore, the formulas listed in IEC 61508 do not consider CAFs [42]. Therefore, a new method to assess the performance of SISs against CAFs is required.

This paper proposes a method for analyzing how SIS performance

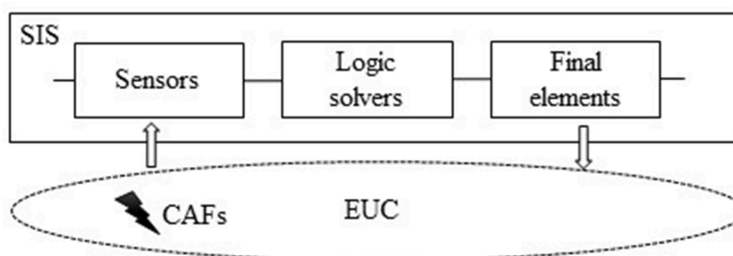


Fig. 1. A general configuration of an EUC system and an SIS.

influences the protection against and mitigation of CAFs. This paper's novelty and main contributions are two folds: 1) developing a new method to model SISs against CAFs and evaluate their effectiveness; 2) revealing the influences of reliability and durability of SISs on the mitigation of CAFs.

The benefits of the proposed method include the following: 1) providing precise and holistic performance analysis considering SIS reliability and durability; 2) considering time-dependent failures on SISs while responding and after activation, and there is no limitation on failure distributions; 3) offering guidelines for the SIS design and deployment to improve the reliability of EUC systems.

The rest of the paper is organized as follows. Section 2 illustrates the models of CAFs and SISs. Section 3 suggests the method for evaluating the impacts of SISs associated with their failures. In Section 4, an illustrative example is provided and is verified by Monte Carlo simulations. A practical case study in the oil and gas industry is presented in Section 5. Finally, in Section 6, we conclude and discuss future works.

2. Modeling SISs against cascading failures

2.1. Modeling cascading failures

CAFs are identified in the literature by many names, such as induced failures, domino failures, propagated failures, and interaction failures [43-45]. This paper deals with CAFs between EUC components. The case that CAFs within SISs have been studied in work [36]. CAFs are assumed to originate from a fault in an EUC component, triggering successive failures of other parts of EUC systems. For example, when an external leakage of flammable gases from a valve is detected, a failure in a control system can cause a valve misclosure and sudden pressure increases.

In previous research [36,46-48], cascading probability $\gamma_i \in [0, 1]$ has been introduced as a measure of propagation easiness. This measure is also employed in this paper. Given that EUC_i fails, the probability that the failure cascades to other components is γ_i . The failure propagation is shown as a dotted curved arrow in Fig. 2 (a). Cascading probability influences the extent of CAFs damages. It can be estimated based on test data or historic failure records [48]. The probability that there are no CAFs is denoted by $\bar{\gamma}_i$ ($\bar{\gamma}_i = 1 - \gamma_i$).

2.2. Modeling SISs against CAFs

Fig. 2(b) illustrates that SIS_{ij} is installed to prevent failure propagation from EUC_i. This paper focuses on the situations that demands on SISs are prolonged (e.g., 2 hours or more). An SIS may fail due to failures in any of its three main subsystems (i.e., the sensors, logic solvers, and final elements). The failures can be classified into two groups:

- FOD refers to an event when an SIS cannot act on demands (e.g., the inability to activate an AFES). An FOD is always a dangerous undetected failure, as defined in IEC 61508 [26]. It is hidden until upon demand or in a proof test. An SIS is often considered as-good-as-new after a proof test [1]. If the proof test interval is not changed, PFD_{avg} is the same in the whole life. PFD_{avg} is also used to determine if an SIS

satisfies a specified safety integrity level (SIL) [26]. IEC 61508 defines four SILs: SIL 1 (the lowest level) through SIL 4 (the highest level) [26].

- FDD refers to an event when an SIS fails during a prolonged demand (e.g., an AFES stops operating even though the fire has not been suppressed). Since an FDD is revealed immediately, it is similar to those dangerous detected failures defined in IEC 61508 [26]. The difference is that FDD is also undetectable by continuous monitoring. It is natural to assume an FDD can be found upon a demand or test. Time to FDD reflects the capability of SISs to resist stress during demands. It is reasonable to use known distributions with probability density functions $f_{SIS_{ij}}(t)$ for FDD, such as a Weibull distribution.

Fig. 3 depicts the sequence of failure events associated with Fig. 2(b). An initiating event is a hazardous event like overheating or a short circuit in the EUC system. EUC_i may fail due to hazardous events, which causes a fire. The fire can propagate to the other components with cascading probability γ_i . An FOD may occur when the demand on SIS_{ij} presents. SIS_{ij} may also fail due to FDD even if it is activated. The failures in SIS_{ij}, including FOD and FDD, determine the outcomes of EUC_j.

This paper focuses on the performance of SISs starting from hazardous events, meaning that the moment $t = 0$ in this context is the occurrence of a hazardous event. In other words, the EUC system is as-good-as-new until $t = 0$. The EUC system is still functioning in a degraded mode under hazardous events. Let t_i denote time that EUC_i fails, and a fire propagates from EUC_i. Then, a demand on SIS_{ij} occurs. The condition of the SIS is unknown when it needs to be activated, and it may be working or failed due to a hidden failure. An FOD may thus be observed at time t_i . Let μ represent time when an FDD occurs. T_{DD} denotes a demand duration of SIS_{ij}. Fig. 4 describes failure time in EUC_i and SIS_{ij}.

Let $P_{ij}(t)$ denote the probability that SIS_{ij} fails by time t , considering FOD and FDD. The probability $P_{ij}(t)$ can be obtained as:

$$\begin{aligned}
 P_{ij}(t) &= P_r(\text{SIS}_{ij} \text{ fails by time } t) \\
 &= PFD(t_i) + [1 - PFD(t_i)]P(T_{SIS} \leq (t - t_i)) \\
 &= PFD(t_i) + [1 - PFD(t_i)] \frac{\int_0^t f_i(t_i) \int_{t_i}^t f_{SIS_{ij}}(\mu - t_i) d\mu dt_i}{\int_0^t f_i(t) dt} \quad (1)
 \end{aligned}$$

where T_{SIS} denotes the operating time of SIS_{ij} from activation to the failed state. T_{SIS} is assumed to be less than T_{DD} , because the demand is prolonged.

Accordingly, let $\bar{P}_{ij}(t)$ denote the probability that the SIS_{ij} functions by time t . The probability $\bar{P}_{ij}(t)$ can be obtained as:

$$\begin{aligned}
 \bar{P}_{ij}(t) &= P_r(\text{SIS}_{ij} \text{ is functioning by time } t) \\
 &= [1 - PFD(t_i)]P(T_{SIS} \geq (t - t_i)) \\
 &= [1 - PFD(t_i)] \frac{\int_0^t f_i(t_i) \left[1 - \int_{t_i}^t f_{SIS_{ij}}(\mu - t_i) d\mu\right] dt_i}{\int_0^t f_i(t) dt} \quad (2)
 \end{aligned}$$



Fig. 2. An EUC system with CAF and SIS.

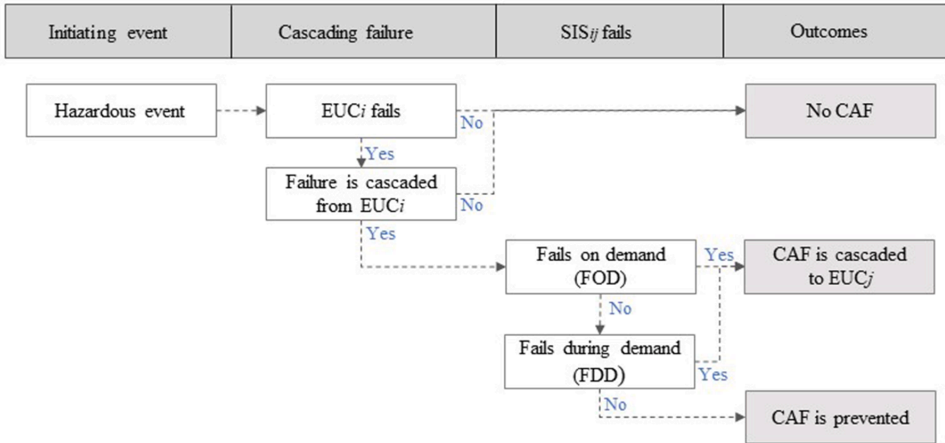


Fig. 3. The sequences of failure events.

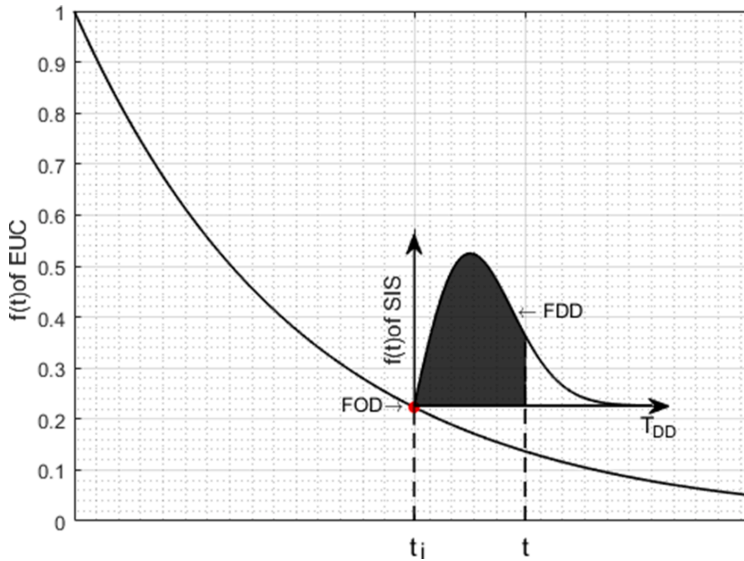


Fig. 4. An illustration of time to failure in EUC_i and SIS_j.

3. Performance analysis considering CAFs and SISs

A recursive aggregation method based on reliability block diagrams (RBDs) is proposed in this section. The method builds on the previous studies of multi-state systems with failure propagation time [47]. The method in this paper is applied to EUC systems in which SISs are employed to intervene in CAF propagation. We take EUC system reliability into account in the analysis of SIS performance in the context of CAFs. The term of system reliability in the following sections refers to the reliability of EUC systems. EUC systems are constructed as typical series-parallel structures.

3.1. Reliability analysis with conditional failures

System reliability can usually be calculated with reliability functions derived from RBDs as long as there are two states of components (functioning and failed) [49]. However, when the system is subject to CAFs, the components are not independent. Consequently, the general rules for structure functions cannot be applied. Reliabilities with conditions are therefore introduced to complement the RBD method. Here, three scenarios may arise considering the states of EUC_i and CAFs: 1) EUC_i functions; 2) EUC_i fails, and the failure is not cascaded; 3) EUC_i fails, and the failure is cascaded, as shown in Fig. 5.

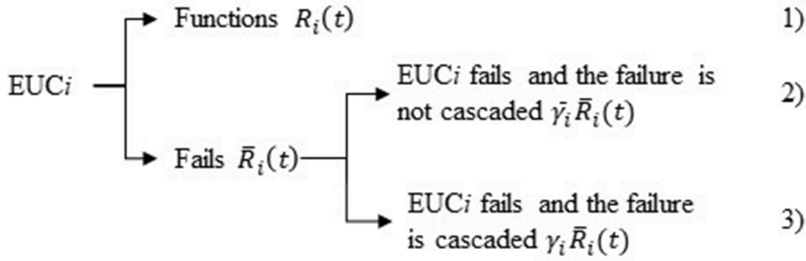


Fig. 5. Three scenarios considering EUC_i and CAFs.

The conditional reliability of EUC_i, denoted by $\tilde{R}_i(t)$, is defined as the probability that EUC_i is functioning at time t given no CAF from EUC_i. No CAF phenomena include the two scenarios: 1) EUC_i functions; 2) EUC_i fails, and the failure is not cascaded. Hence, the probability of no CAF, denoted by $P_r(\text{No CAFs})$, is equal to $R_i(t) + \tilde{\gamma}_i \tilde{R}_i(t)$ or $1 - \gamma_i \tilde{R}_i(t)$. Accordingly, the probability that a CAF occurs $P_r(\text{CAF occurs})$ is equal to $\gamma_i \tilde{R}_i(t)$. The conditional reliability $\tilde{R}_i(t)$ can be described as:

$$\tilde{R}_i(t) = \frac{P_r(\text{EUC functions})}{P_r(\text{No CAFs})} = \frac{R_i(t)}{R_i(t) + \tilde{\gamma}_i \tilde{R}_i(t)} = \frac{R_i(t)}{1 - \gamma_i \tilde{R}_i(t)} \quad (3)$$

If the failure in EUC_i will never be cascaded out, the conditional reliability $\tilde{R}_i(t)$ is defined to be equal to the reliability $R_i(t)$.

Consider a system Ω_n with n components EUC_{*i*} ($i = 1, 2, \dots, n$) organized in a series structure. One can obtain the conditional system reliabilities by time t as:

$$\tilde{R}_{\Omega_{\text{series}}}(t) = \prod_{i=1}^n \tilde{R}_i(t) \quad (4)$$

Similarly, the conditional reliability of a parallel system with n components EUC_{*i*} can be obtained as:

$$\tilde{R}_{\Omega_{\text{parallel}}}(t) = 1 - \prod_{i=1}^n (1 - \tilde{R}_i(t)) \quad (5)$$

The conditional system reliability for an arbitrary series-parallel system can be obtained based on Eq.s (4) and (5). The method is similar to the traditional RBD method [49], replacing component reliabilities by corresponding conditional reliabilities.

3.2. Reliability of an EUC system

This section presents the method for analyzing the reliability of an EUC system. The following assumptions are made:

- The two states are considered for EUC_{*i*}: functioning or failed.
- The time to failure in EUC_{*i*} follows a known distribution with probability density functions, denoted by $f_i(t)$.
- There are no repairs and inspections during demand durations.

First, consider a system Ω_n with n components structured as a series-parallel system, and only one CAF may occur from EUC_{*i*} to EUC_{*j*}. If the CAF occurs and an SIS is functioning with the probability of $\bar{P}_{ij}(t)$, EUC_{*j*} is protected from the CAF by the safety function of the SIS. It implies that only EUC_{*i*} is in a failed state at time t for this system. On the contrary, when the CAF occurs and an SIS fails with the probability of $P_{ij}(t)$, EUC_{*j*} is impacted by the CAF. Both EUC_{*i*} and EUC_{*j*} are in failed states at time t . $\bar{P}_{ij}(t)$ corresponds to the conditional reliability $\tilde{R}_{\Omega_{n-(ij)}}(t)$ in case that the SIS is functioning. Similarly, $P_{ij}(t)$ corresponds to the conditional reliability $\tilde{R}_{\Omega_{n-(ij)}}(t)$ in case that the SIS is in a failed state. Hence, the reliability of the system Ω_n by time t is listed as follows:

$$\begin{aligned} R_S(t) &= P_r(\text{No CAFs}) \tilde{R}_{\Omega_n}(t) \\ &\quad + P_r(\text{CAF occurs}) \left[P_{ij}(t) \tilde{R}_{\Omega_{n-(ij)}}(t) + \bar{P}_{ij}(t) \tilde{R}_{\Omega_{n-(i)}}(t) \right] \\ &= \left[1 - \gamma_i \tilde{R}_i(t) \right] \tilde{R}_{\Omega_n}(t) + \gamma_i \tilde{R}_i(t) \left[P_{ij}(t) \tilde{R}_{\Omega_{n-(ij)}}(t) + \bar{P}_{ij}(t) \tilde{R}_{\Omega_{n-(i)}}(t) \right] \end{aligned} \quad (6)$$

where $\Omega_{n-(ij)}$ and $\Omega_{n-(i)}$ are the subsystems with functioning components. $\tilde{R}_{\Omega_{n-(i)}}$ and $\tilde{R}_{\Omega_{n-(ij)}}$ denote the corresponding conditional reliabilities of $\Omega_{n-(ij)}$ and $\Omega_{n-(i)}$. The failed components can be removed when calculating system reliability, meaning that their reliabilities are replaced by zero. One can obtain $\tilde{R}_{\Omega_{n-(i)}}$ and $\tilde{R}_{\Omega_{n-(ij)}}$ based on Eq.s (4) and (5).

Second, consider a system Ω_n with multiple CAFs. Subsystem Ω_m ($\Omega_m \in \Omega_n$) has m EUC components with CAFs, denoted by CAF₁, CAF₂, CAF₃, ..., and CAF_{*m*}. Cascading probabilities are $\gamma_1, \gamma_2, \gamma_3, \dots$, and γ_m . All possible combinations of CAF occurrence are considered. The event θ_1 describes no CAF in subsystem Ω_m ($\theta_1 = \bar{\text{CAF}}_1 \cap \bar{\text{CAF}}_2 \cap \dots \cap \bar{\text{CAF}}_m$). The event θ_2 is a situation when CAFs generate from the first component ($\theta_2 = \text{CAF}_1 \cap \bar{\text{CAF}}_2 \cap \dots \cap \bar{\text{CAF}}_m$). The event when all CAFs occur in m components is denoted by θ_{2^m} ($\theta_{2^m} = \text{CAF}_1 \cap \text{CAF}_2 \cap \dots \cap \text{CAF}_m$). The probability $\theta_\nu(t)$ ($\nu \in \forall(1, 2, \dots, 2^m)$) describes that the CAF event θ_ν occurs by time t , and it is given as follows:

$$\theta_\nu(t) = \prod_{i=1}^m \left[\gamma_i \tilde{R}_i(t) \right]^{\text{mod} \left(\left\lfloor \frac{\nu-1}{2^{i-1}} \right\rfloor, 2 \right)} \left[1 - \gamma_i \tilde{R}_i(t) \right]^{\left(1 - \text{mod} \left(\left\lfloor \frac{\nu-1}{2^{i-1}} \right\rfloor, 2 \right) \right)} \quad (7)$$

Assume the CAF event θ_ν is connected to a specific subsystem Ω_ν ($\Omega_\nu \in \Omega_m$) where CAFs are triggered from the components. Assume EUC_{*h*} ($\text{EUC}_h \in \forall \Omega_\nu$) is linked to l SISs denoted by SIS_{*h1*}, SIS_{*h2*}, SIS_{*h3*}, ..., and SIS_{*hl*}. All possible combinations of the SISs' states (i.e., functioning or failed) are considered SIS events. The event δ_1 involves no SIS failure ($\delta_1 = \text{SIS}_{h1} \cap \text{SIS}_{h2} \cap \dots \cap \text{SIS}_{hl}$). The event δ_2 involves one failure in SIS_{*h1*} ($\delta_2 = \bar{\text{SIS}}_{h1} \cap \text{SIS}_{h2} \cap \dots \cap \text{SIS}_{hl}$). The event when all SISs fail is denoted by δ_{2^l} ($\delta_{2^l} = \bar{\text{SIS}}_{h1} \cap \bar{\text{SIS}}_{h2} \cap \dots \cap \bar{\text{SIS}}_{hl}$). The probability $\delta_{hg}(t)$ ($g \in \forall(1, 2, \dots, 2^l)$) describes that EUC_{*h*} fails and the SIS event δ_g occurs by time t , and it is given as follows:

$$\delta_{h,g}(t) = \frac{\int_0^t f_h(t_h) \prod_{j=1}^l [P_{h,j}(t)]^{\text{mod} \left(\left\lfloor \frac{g-1}{2^{j-1}} \right\rfloor, 2 \right)} \left[\bar{P}_{h,j}(t) \right]^{\left(1 - \text{mod} \left(\left\lfloor \frac{g-1}{2^{j-1}} \right\rfloor, 2 \right) \right)} dt_h}{\int_0^t f_h(t) dt} \quad (8)$$

where

$$P_{h,j}(t) = \text{PFDF}_{\text{avg},h,j} + (1 - \text{PFDF}_{\text{avg},h,j}) \int_{t_h}^t f_{\text{SIS}_{h_j}}(\mu - t_h) d\mu$$

$$\bar{P}_{h,j}(t) = (1 - PFD_{avg,hj}) \left[1 - \int_{t_h}^t f_{SIS_{hj}}(\mu - t_h) d\mu \right]$$

$P_{h,j}(t)$ is the probability that SIS_{hj} has failed by time t , while $\bar{P}_{h,j}(t)$ is the probability that SIS_{hj} is functioning at time t . EUC_h fails at time t_h . $PFD_{avg,hj}$ denotes the steady-state probability for FOD in SIS_{hj} . SISs are critical safety barriers so that they are often designed to be highly reliable under normal conditions [50]. PFD(t) is relatively small and varies slightly. It is unnecessary to determine the probability as a function of time, and an average value is sufficient for FOD [1]. Furthermore, IEC 61508 distinguishes four SILs relating to PFD_{avg} , rather than PFD(t) [26]. Therefore, in Eq. (8), we use PFD_{avg} to represent PFD(t) approximately.

Combining all SIS events, conditional probability for the CAF event θ_v by time t is obtained as:

$$Q_v(t) = \prod_{h \in \sqrt{\Omega_v}} \sum_{g=1}^{2^l} \delta_{h,g}(t) \tilde{R}_{\Omega_{n-F}}(t) \quad (9)$$

where Ω_{n-F} denotes a subsystem with the functioning EUC components, and $\tilde{R}_{\Omega_{n-F}}(t)$ denotes the conditional reliability by time t for the subsystem Ω_{n-F} . Eventually, system reliability can be obtained as:

$$R_S(t) = \sum_{v=1}^{2^m} \theta_v(t) Q_v(t) \quad (10)$$

In short, system reliability can be obtained by applying the following steps:

- 1 Define a subsystem comprising m EUC components that may trigger CAFs and calculate their conditional reliabilities.
- 2 Generate all combinations of CAFs and compute probabilities of CAF events.
- 3 For each CAF event, generate all SIS states' combinations and compute probabilities of SIS events.
- 4 Based on RBDs, compute conditional reliabilities for all SIS events.
- 5 Obtain system reliability by combining conditional reliabilities for all CAF events.

The following section introduces an example. Then, a practical case is used to present the method's effectiveness.

4. Example and verifications

4.1. An illustrative example

Consider a system Ω_n with three EUC components (the RBD of this system is shown in Fig. 6). Subsystem Ω_m represents a subsystem with m EUC components that may trigger multiple CAFs. The subsystem Ω_m includes the components EUC_1 and EUC_2 . The cascading possibilities are γ_1 and γ_2 . SIS_{12} , SIS_{13} , SIS_{21} and SIS_{23} are installed to prevent and mitigate CAFs propagation. The probability of FODs is $PFD_{avg,12}$, $PFD_{avg,13}$, $PFD_{avg,21}$, and $PFD_{avg,23}$.

The reliability of the EUC system is calculated using the following five steps:

Step 1: According to Eq. (3), the conditional reliabilities of EUC_1 , EUC_2 , and EUC_3 considering CAFs are obtained as:

$$\tilde{R}_1(t) = \frac{R_1(t)}{1 - \gamma_1 \bar{R}_1(t)}$$

$$\tilde{R}_2(t) = \frac{R_2(t)}{1 - \gamma_2 \bar{R}_2(t)}$$

$$\tilde{R}_3(t) = R_3(t)$$

Step 2: By using Eq. (7), the probabilities of the CAF events are obtained as:

$$\theta_1(t) = [1 - \gamma_1 \bar{R}_1(t)] \cdot [1 - \gamma_2 \bar{R}_2(t)]$$

$$\theta_2(t) = [\gamma_1 \bar{R}_1(t)] \cdot [1 - \gamma_2 \bar{R}_2(t)]$$

$$\theta_3(t) = [1 - \gamma_1 \bar{R}_1(t)] \cdot [\gamma_2 \bar{R}_2(t)]$$

$$\theta_4(t) = [\gamma_1 \bar{R}_1(t)] \cdot [\gamma_2 \bar{R}_2(t)]$$

Step 3: By using Eq. (8), the probabilities of the SIS events are obtained as:

$$\delta_{1,1}(t) = 1$$

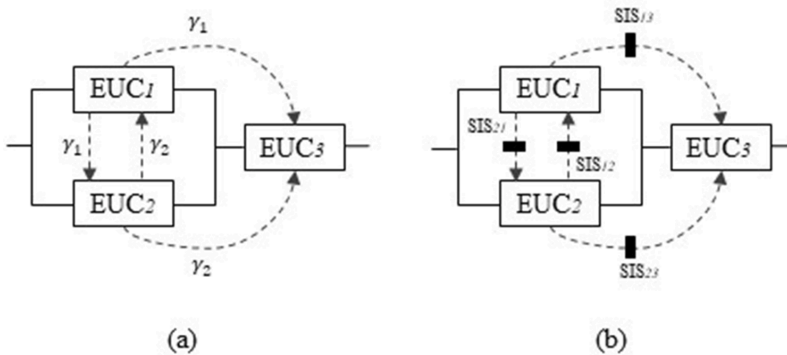


Fig. 6. RBD of an EUC system with CAFs and SIS.

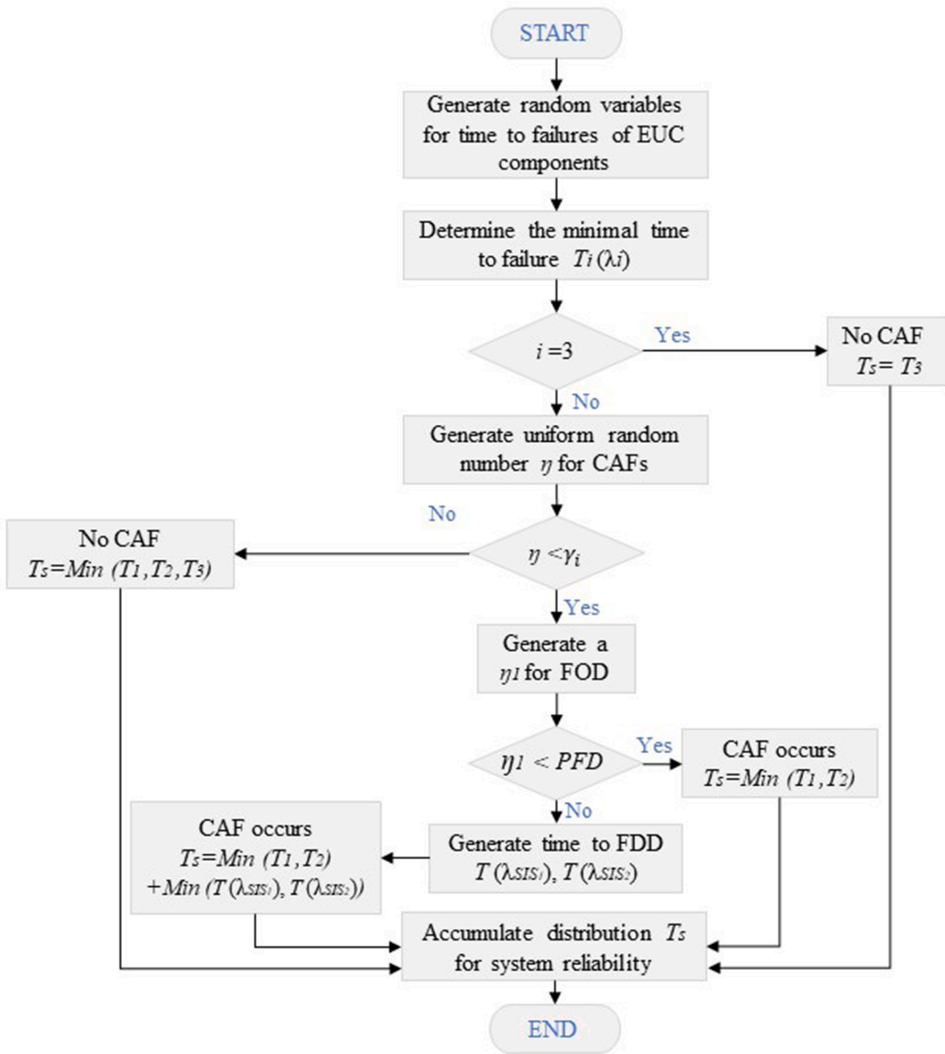


Fig. 7. The MCS flowchart for failure propagations.

$$\delta_{2,1}(t) = \frac{\int_0^t f_1(t_1) \left[(1 - PFD_{avg,12}) \left(1 - \int_{t_1}^{\mu} f_{SIS_{12}}(\mu - t_1) d\mu \right) \right] \left[(1 - PFD_{avg,13}) \left(1 - \int_{t_1}^{\mu} f_{SIS_{13}}(\mu - t_1) d\mu \right) \right] dt_1}{\int_0^t f_1(t) dt}$$

$$\delta_{2,2}(t) = \frac{\int_0^t f_1(t_1) \left[PFD_{avg,12} + (1 - PFD_{avg,12}) \int_{t_1}^{\mu} f_{SIS_{12}}(\mu - t_1) d\mu \right] \left[(1 - PFD_{avg,13}) \left(1 - \int_{t_1}^{\mu} f_{SIS_{13}}(\mu - t_1) d\mu \right) \right] dt_1}{\int_0^t f_1(t) dt}$$

$$\delta_{2,3}(t) = \frac{\int_0^t f_1(t_1) \left[(1 - PFD_{avg,12}) \left(1 - \int_{t_1}^{\mu} f_{SIS_{12}}(\mu - t_1) d\mu \right) \right] \left[PFD_{avg,13} + (1 - PFD_{avg,13}) \int_{t_1}^{\mu} f_{SIS_{13}}(\mu - t_1) d\mu \right] dt_1}{\int_0^t f_1(t) dt}$$

$$\delta_{2,4}(t) = \frac{\int_0^t f_1(t_1) \left[PFD_{avg,12} + (1 - PFD_{avg,12}) \int_{t_1}^{\mu} f_{SIS_{12}}(\mu - t_1) d\mu \right] \left[PFD_{avg,13} + (1 - PFD_{avg,13}) \int_{t_1}^{\mu} f_{SIS_{13}}(\mu - t_1) d\mu \right] dt_1}{\int_0^t f_1(t) dt}$$

$$\delta_{3,1}(t) = \frac{\int_0^t f_2(t_2) \left[(1 - PFD_{avg,21}) \left(1 - \int_{t_2}^{\mu} f_{SIS_{21}}(\mu - t_2) d\mu \right) \right] \left[(1 - PFD_{avg,23}) \left(1 - \int_{t_2}^{\mu} f_{SIS_{23}}(\mu - t_2) d\mu \right) \right] dt_2}{\int_0^t f_2(t) dt}$$

$$\delta_{3,2}(t) = \frac{\int_0^t f_2(t_2) \left[PFD_{avg,21} + (1 - PFD_{avg,21}) \int_{t_2}^{\mu} f_{SIS_{21}}(\mu - t_2) d\mu \right] \left[(1 - PFD_{avg,23}) \left(1 - \int_{t_2}^{\mu} f_{SIS_{23}}(\mu - t_2) d\mu \right) \right] dt_2}{\int_0^t f_2(t) dt}$$

$$\delta_{3,3}(t) = \frac{\int_0^t f_2(t_2) \left[(1 - PFD_{avg,21}) \left(1 - \int_{t_2}^{\mu} f_{SIS_{21}}(\mu - t_2) d\mu \right) \right] \left[PFD_{avg,23} + (1 - PFD_{avg,23}) \int_{t_2}^{\mu} f_{SIS_{23}}(\mu - t_2) d\mu \right] dt_2}{\int_0^t f_2(t) dt}$$

$$\delta_{3,4}(t) = \frac{\int_0^t f_2(t_2) \left[PFD_{avg,21} + (1 - PFD_{avg,21}) \int_{t_2}^{\mu} f_{SIS_{21}}(\mu - t_2) d\mu \right] \left[PFD_{avg,23} + (1 - PFD_{avg,23}) \int_{t_2}^{\mu} f_{SIS_{23}}(\mu - t_2) d\mu \right] dt_2}{\int_0^t f_2(t) dt}$$

Step 4: According to Eqs. (4) and (5), the conditional reliabilities of the subsystems considering CAFs can be obtained as:

$$\tilde{R}_{\Omega_n}(t) = [\tilde{R}_1(t) + \tilde{R}_2(t) - \tilde{R}_1(t)\tilde{R}_2(t)]\tilde{R}_3(t)$$

$$\tilde{R}_{\Omega_{n-1}}(t) = \tilde{R}_2(t)\tilde{R}_3(t)$$

$$\tilde{R}_{\Omega_{n-2}}(t) = \tilde{R}_1(t)\tilde{R}_3(t)$$

$$\tilde{R}_{\Omega_{n-(1,2)}}(t) = \tilde{R}_{\Omega_{n-(1,3)}}(t) = \tilde{R}_{\Omega_{n-(2,3)}}(t) = \tilde{R}_{\Omega_{n-(1,2,3)}}(t) = 0$$

Step 5: The system reliability $R_S(t)$ can be calculated using Eq. (10):

$$R_S(t) = \theta_1(t)\delta_{1,1}(t)\tilde{R}_{\Omega_n}(t) + \theta_2(t)\left[\delta_{2,1}(t)\tilde{R}_{\Omega_{n-1}}(t) + \delta_{2,2}(t)\tilde{R}_{\Omega_{n-(1,2)}}(t) + \delta_{2,3}(t)\tilde{R}_{\Omega_{n-(1,3)}}(t) + \delta_{2,4}(t)\tilde{R}_{\Omega_{n-(1,2,3)}}(t)\right] + \theta_3(t)\left[\delta_{3,1}(t)\tilde{R}_{\Omega_{n-2}}(t) + \delta_{3,2}(t)\tilde{R}_{\Omega_{n-(2,1)}}(t) + \delta_{3,3}(t)\tilde{R}_{\Omega_{n-(2,3)}}(t) + \delta_{3,4}(t)\tilde{R}_{\Omega_{n-(1,2,3)}}(t)\right]$$

By removing the subsystems whose reliabilities with conditions are equals to zero, the system reliability can be obtained as:

$$R_S(t) = \theta_1(t)\tilde{R}_{\Omega_n}(t) + \theta_2(t)\delta_{2,1}(t)\tilde{R}_{\Omega_{n-1}}(t) + \theta_3(t)\delta_{3,1}(t)\tilde{R}_{\Omega_{n-2}}(t) \tag{11}$$

Notice that the calculations regarding $\theta_4(t)$ are excluded since the system is down when EUC₁ and EUC₂ fail simultaneously.

4.2. Verifications of the proposed formulas

Monte Carlo simulations (MCSs) were conducted to check the validity of the proposed method and Eq. (11) in the previous sections. Fig. 7 is a flowchart of MCSs constructed in MATLAB. The flowchart illustrates the simulation process of the example in section 4.1. The principals should be the same for different examples, but details may be modified according to the algorithm and configurations. The proposed method can be applied to any arbitrary type of failure distribution. In this case, the time to failures in EUC components is assumed to follow an exponential distribution, while time to FDD in SISs is assumed to follow a Weibull distribution. An exponential random variable, denoted by $T_i(\lambda_i)$, expresses the time to failure in EUC_i. A variable η is a random variable generated from a uniform [0, 1]. If η is smaller than cascading probability γ_i , CAFs occur in the simulations. Similarly, η_1 is another random variable generated from a uniform [0, 1]. An FOD occurs when η_1 is smaller than FOD probability (i.e., $PF_{D_{avg}}$ of SISs). Time $T(\lambda_{SIS})$ denotes the simulated time to FDD of SISs, which is reflected by time $(\mu - t_i)$ in Fig. 4. Time T_s denotes simulated time to system failure.

Table 1
The parameters of the illustrative example.

	SIS			EUC	
	Failures	Parameter	Value	Parameter	Value
Case 1	No SIS	-	-	λ_i	0.2/hour
	No SIS	-	-	α_i	1
Case 2	FOD	$PF_{D_{avg,ij}}$	0.1	-	-
	FDD	λ_{ij}	0.08/hour	λ_i	0.2/hour
		α_{ij}	1	α_i	1
Case 3	FOD	$PF_{D_{avg,ij}}$	0.2	-	-
	FDD	λ_{ij}	0.16/hour	λ_i	0.1/hour
		α_{ij}	2	α_i	1

The EUC components and SISs are assumed to be identical. Without losing generality, γ_1 and γ_2 are assigned to 0.2 and 0.3, respectively. The other parameters are presented in Table 1. Fig. 8 shows the system reliability profiles in 2 hours. Here, we run the simulations with 10^6 MC iterations. System reliability calculation using the proposed method in this paper gives the same results as the simulations for all three cases. Thus, it is demonstrated that the method in this paper is suitable for evaluating system reliability considering CAFs and SISs.

5. Case study

This section conducts a practical case study in the oil and gas industry to illustrate deploying SISs based on the proposed method. A EUC system consists of three separators (EUC₁, EUC₂, and EUC₃), one scrubber (EUC₄), and three compressors (EUC₅, EUC₆, and EUC₇), as

shown in Fig. 9. The separators separate production fluids into oil, gas, and water, and the scrubber is used to wash unwanted pollutants from the gas stream. Finally, the compressors are applied to increase gas pressure and temperature.

In this case, hazardous events like overheating or short circuits can result in failures of the EUC system. We assume that the failures in EUC₂ and EUC₆ can initiate fires. The fires can propagate to the components located in the same facility, as shown in Fig. 9. They cannot cause fires in the rest of the components because of separation systems like firewalls. Time to failure in an EUC component is assumed to follow a Weibull distribution with a scale parameter λ_{EUC} and a shape parameter α_{EUC} . Cascading probabilities are denoted by γ_2 and γ_6 . The parameters used in this case study are presented in Table 2. In general, such parameters can be obtained from historical statistics, vendor data, and equipment certifications. The failure probability of EUC components and SISs is much higher than in regular operations. That is because they are supposed to be exposed to high stress in hazardous events in this case.

AFESs are installed to suppress and extinguish fires. Each AFES is for the analysis generalized as SIS_{ij}. As shown in Fig. 9, SIS₂₄ and SIS₂₅ can prevent failure propagation from EUC₂, while SIS₆₄ and SIS₆₇ can prevent failure propagation from EUC₆. For all SIS_{ij}, $PF_{D_{avg}}$ is assigned to be 10^{-3} for FODs to achieve the required SIL 3 requirements, i.e., the maximum allowed value of a SIL 3 function. Time to FDD is assumed to follow a Weibull distribution with scale parameter λ_{SIS} and shape parameter α_{SIS} . The parameters of SISs are summarized in Table 3.

5.1. System reliability calculation

The reliability of the EUC system can be calculated using Eq. (10). The EUC system is evaluated by considering the following states of the SISs: (1) perfect SISs, (2) SISs with FOD, and (3) SISs with FOD and FDD. Here, γ_2 and γ_6 are set at 0.5. The calculation results are shown in Fig. 10. Since we focus on the situations when demands on SISs are prolonged (e.g., 2 hours or more), it is reasonable to observe the reliability in the first two hours as an example. As seen, the reliability profiles of the EUC systems with (1) perfect SISs and (2) SISs with FOD are almost the same. That means the effects of FOD are relatively low. The reliability gap between the EUC systems with (1) perfect SISs and (3) SISs with FOD and FDD is noticeable. The effects of FDD can explain such a gap. The reason is that we focus on what happens after a hazardous event, and the probability of FOD is extremely low. The

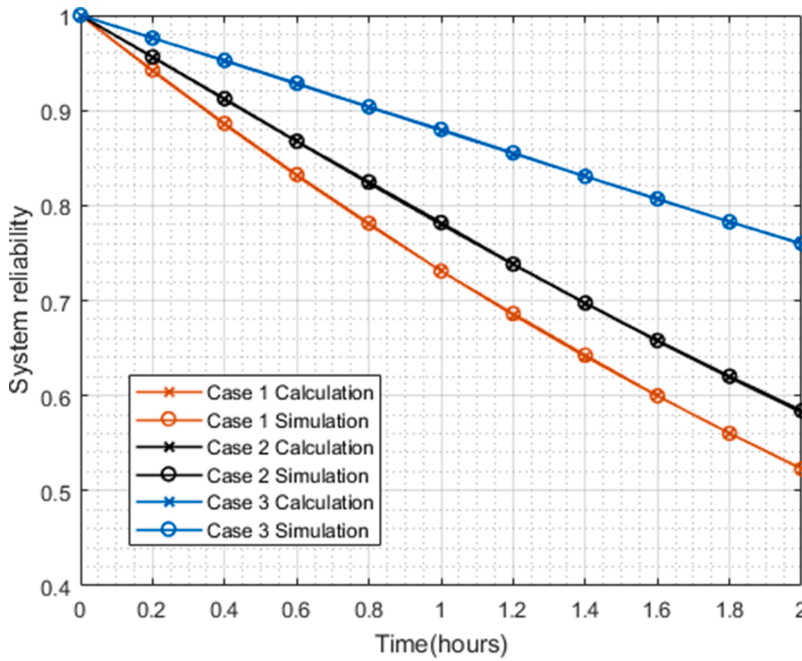


Fig. 8. System reliability for three cases using calculation and simulations.

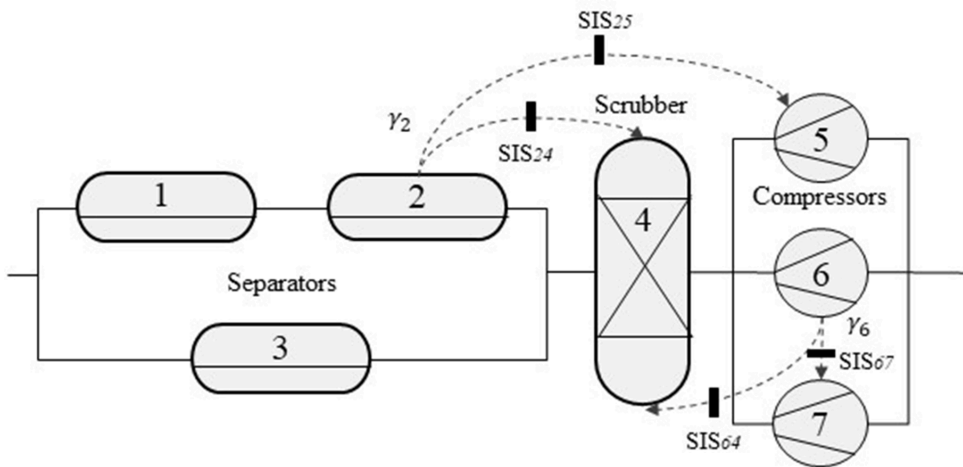


Fig. 9. RBD with CAFs and SISs of the case study.

reliability gaps can be changed when λ_{SIS} and PFD_{avg} are set differently. It implies that it is reasonable to pay more attention to the effects of FDD when considering the high stress from CAFs.

5.2. Sensitivity analysis

Given that SISs are installed, the reliability of the EUC system is impacted by the strength of CAFs (i.e., cascading probability γ) and the capacity of SISs (i.e., PFD_{avg} in terms of FOD and scale parameters λ_{SIS}

for FDD). This section will carry out sensitivity analyses to understand the influences of these parameters.

5.2.1 Effects of origins of CAFs

To evaluate the impacts of CAFs, we observe the situations when cascading probabilities γ_2 and γ_6 are changed, keeping the other parameters as constants. For example, cascading probability γ_2 is increased, meaning that the failure is more likely to affect the others due to geographical location (e.g., closing to the center of an industrial area).

Table 2
The parameters of EUC components in the case study.

EUC _i	Components	λ_{EUC} (/hour)	α_{EUC}
1	Separator 1	0.21	1.4
2	Separator 2	0.12	1.3
3	Separator 3	0.24	1.2
4	Scrubber	0.17	1.5
5	Compressor 1	0.32	2.1
6	Compressor 2	0.32	2.1
7	Compressor 3	0.32	2.1

Table 3
The parameters of SISs in the case study.

SIS _{ij}	λ_{SIS} (/hour)	FOD	α_{SIS}	FDD (PFD _{avg})
SIS ₂₄	0.42	2.0	10^{-3}	
SIS ₂₅	0.33	2.0	10^{-3}	
SIS ₆₄	0.41	2.0	10^{-3}	
SIS ₆₇	0.18	2.0	10^{-3}	

γ_2 and γ_6 are assigned from 0 to 0.5. The other parameters are presented in Table 2 and Table 3. The result at time $t = 2$ hours is provided in Figure 11. The 3D plot indicates that the system reliability is more sensitive to γ_6 than γ_2 , which means that CAFs generated from EUC₆ are more critical to system reliability in this case. In other words, if EUC₆ is physically closer to other parts of the production system, the system is more vulnerable in case of fires.

5.2.2 Mitigating effects of SISs

The mitigating effects of SISs are considered in this section. Now, the cascading probabilities γ_2 and γ_6 are kept constant and set equal to 0.5, while the values of PFD_{avg} for FOD and scale parameters for FDD are

changed. We assume that the same values are applied for all SISs since the SISs are identical and perform similar safety functions. The system reliabilities with increasing $\text{Log}_{10}(\text{PFD}_{\text{avg}})$ at the different observing times (e.g., $t = 0.5, 1, 1.5, 2$ hours) are presented in Fig. 12. For clarity, the ranges of SILs are SIL 1 to SIL 4. As seen, when changing $\text{Log}_{10}(\text{PFD}_{\text{avg}})$, the trend of the system reliability in the four subplots are approximately similar. The system reliabilities remain almost unchanged when SISs are at SIL 2 or higher. If the SIL of the SISs drops to SIL1, the system reliabilities decrease dramatically. In other words, SISs mitigate CAFs almost as well at SIL 2 as at SIL 4. This analysis provides information on improving system reliabilities with increasing SILs regarding safety integrity. In practice, it is beneficial to determine proof test intervals of SISs to satisfy the SIL safety requirements and the EUC reliability requirements.

Fig. 13 illustrates how the system reliability is impacted when the scale parameters λ_{SIS} varies. For example, by $t = 2$ hours, the system reliabilities with $\lambda_{SIS}, 1.5\lambda_{SIS}, 2\lambda_{SIS}, 2.5\lambda_{SIS}, 3\lambda_{SIS}$ of SISs are 0.74, 0.70, 0.66, 0.64 and 0.63, respectively. The system reliabilities do not decrease linearly with higher values of the scale parameters. Thus, it is necessary to analyze how specific SISs mitigate CAFs and deploy suitable SISs, and it will be discussed in the following sections.

5.3. Criticality analysis of SISs

Based on the method in Section 3, criticality analysis is carried out to identify optimal solutions of SISs in protecting against CAFs. We consider three variables related to optimal solutions: location, number, and cost of SISs. Specifically, risk achievement worth (RAW), denoted by $I^{RAW}(SIS|t)$, is employed as the critical analysis. It is defined as the ratio of the system unreliability if an SIS is not present (or in the failed state) with the system unreliability if an SIS is functioning at time t [49]:

$$I^{RAW}(SIS|t) = \frac{1 - h(0_{SIS}, R_S(t))}{1 - h(1_{SIS}, R_S(t))} \tag{12}$$

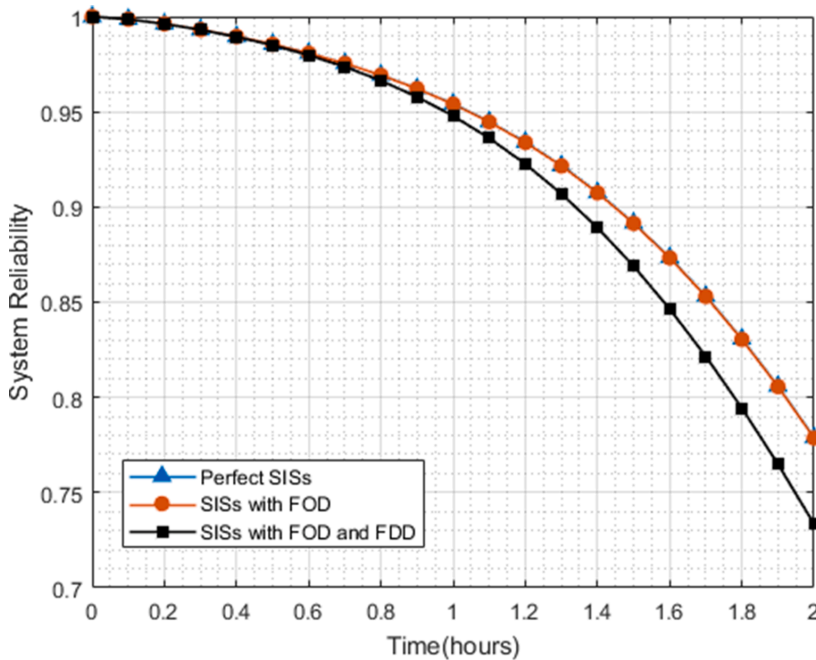


Fig. 10. System reliability profiles for different states of SISs.

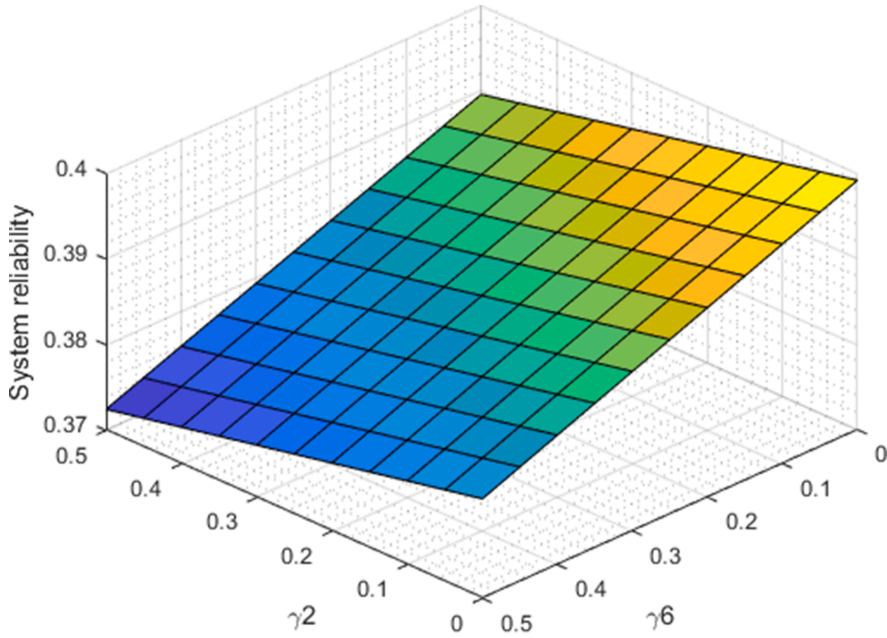


Fig. 11. System reliability considering γ_2 and γ_6 at $t = 2$ hours.

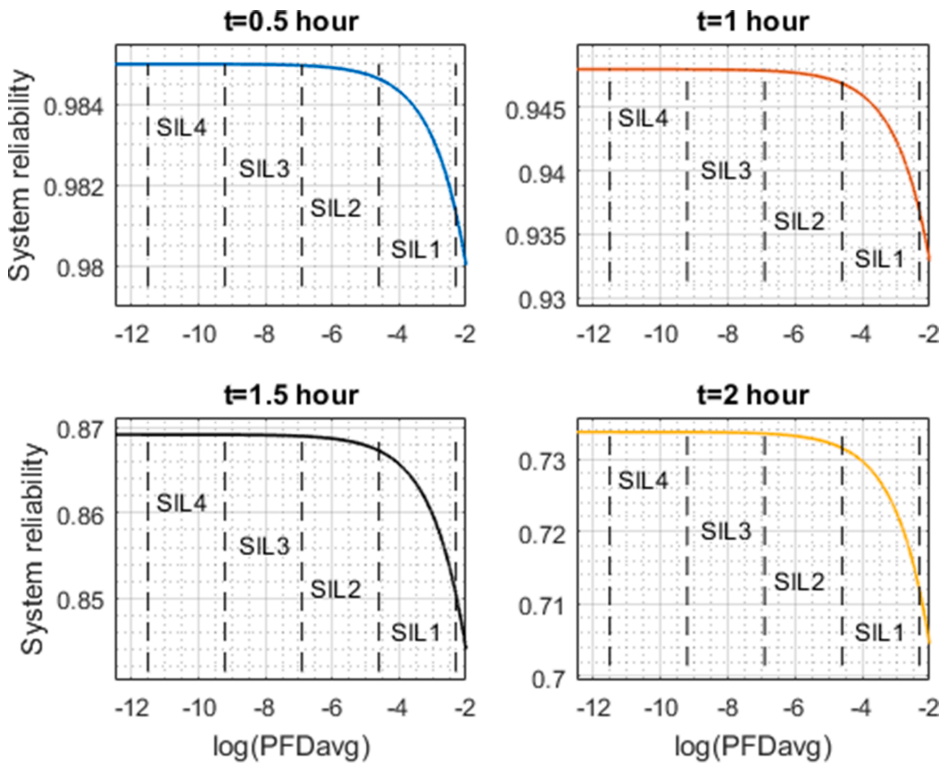


Fig. 12. System reliability considering PFD_{avg} of SISs for FOD.

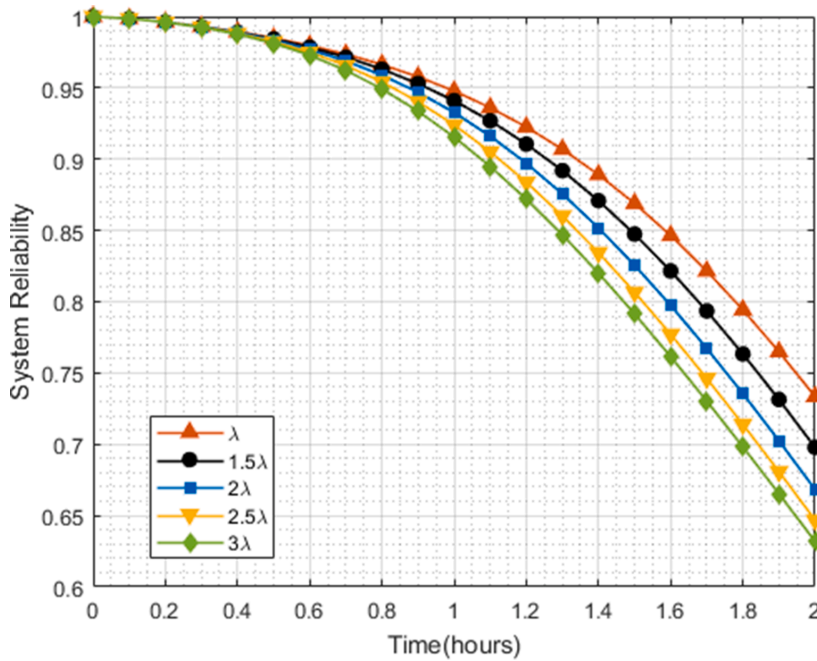


Fig. 13. System reliability considering scale parameters of SISs for FDD.

Table 4
Calculation results for different solutions at $t = 2$ hours.

No.	SIS	$R(t)$	$I^{RAW}(SIS t)$	cost	$I^{RAW}(SIS t)/a$
1	No	0.56	-	-	-
2	SIS_{24}	0.59	1.07	a	1.07
3	SIS_{25}	0.56	1.00	a	1.00
4	SIS_{64}	0.64	1.22	a	1.22
5	SIS_{67}	0.56	1.00	a	1.00
6	SIS_{24}, SIS_{25}	0.59	1.07	$2a$	0.54
7	SIS_{24}, SIS_{64}	0.68	1.38	$2a$	0.69
8	SIS_{24}, SIS_{67}	0.59	1.07	$2a$	0.54
9	SIS_{25}, SIS_{64}	0.64	1.22	$2a$	0.61
10	SIS_{25}, SIS_{67}	0.56	1.00	$2a$	0.50
11	SIS_{64}, SIS_{67}	0.67	1.33	$2a$	0.67
12	$SIS_{24}, SIS_{25}, SIS_{64}$	0.68	1.38	$3a$	0.46
13	$SIS_{24}, SIS_{25}, SIS_{67}$	0.59	1.07	$3a$	0.36
14	$SIS_{24}, SIS_{64}, SIS_{67}$	0.70	1.47	$3a$	0.49
15	$SIS_{25}, SIS_{64}, SIS_{67}$	0.67	1.33	$3a$	0.44
16	$SIS_{24}, SIS_{25}, SIS_{64}, SIS_{67}$	0.71	1.52	$4a$	0.38

where $h(0_{SIS}, R_S(t))$ denotes system reliability without an SIS, while $h(1_{SIS}, R_S(t))$ denotes system reliability with an SIS. When $I^{RAW}(SIS|t)$ is large, the status of SIS can result in a comparatively significant change in the system reliability significantly at time t .

By combining Eqs. (10) and (12), $I^{RAW}(SIS|t)$ is obtained in Table 4. The parameters are shown in Table 2 and Table 3. Solution No.16 with the four SISs has the most significant effects in achieving system reliability against CAFs. On the other hand, no. 7 (SIS_{24}, SIS_{64}) effects are found approximately the same as ones of three SISs in solution No.12 ($SIS_{24}, SIS_{25},$ and SIS_{64}). The reason is that the effects on preventing CAFs of solutions No.3 (SIS_{25}), No.5 (SIS_{67}), and their combination No.10 (SIS_{25}, SIS_{67}) are restricted. That implies that those SISs have less

influence on the system reliability in comparison with the others.

The cost of SIS deployment can also be considered in the analysis. We assume that the installation cost is roughly the same for all SISs and equal to a . Then, $I^{RAW}(SIS|t)/a$ reflects the improvement of system reliability by installing a SIS. The analysis results are summarized in Table 4. Solution No.4 (SIS_{64}) is the worthiest solution if only one SIS is considered. If two SISs are considered, the most efficient solutions are No.7 (SIS_{24}, SIS_{64}) and No.11 (SIS_{64}, SIS_{67}). This analysis can help the designers compare the effectiveness of solutions with a limited budget for installing SISs.

In addition to $I^{RAW}(SIS|t)$, we can also obtain the system reliability profiles to compare different solutions. For example, we consider two potential solutions: No.6 (SIS_{24}, SIS_{25}) and No.11(SIS_{64} and SIS_{67}). Fig. 14 indicates that the two solutions effectively improve system reliability, but solution No. 11 always has more significant effects in protecting against CAFs than solution No.6. It implies that SIS_{64} and SIS_{67} are more critical for the system reliability than SIS_{24} and SIS_{25} . In other words, SIS_{64} and SIS_{67} can more effectively protect the 1003 subsystem (i.e., EUC_5, EUC_6, EUC_7) from CAFs than the others.

6. Conclusions and future research

This paper has proposed a novel method to evaluate the performance of SISs that are employed to protect the EUC system against CAFs. The method considers failures of SISs in responding and after activation and so analyzes SIS reliability and durability in performance analysis. The proposed method can provide designers and operators with information for the SIS design and deployment, thereby improving the safety and reliability of the EUC system. This paper applies the proposed method to SISs and EUC systems, but it can also be adopted in other safety barriers in industrial series-parallel systems.

The method is verified through simple applications, but it efficiently manages large systems with a limited number of CAFs. If the number increases, the combinations of CAFs grow exponentially. In that case, the

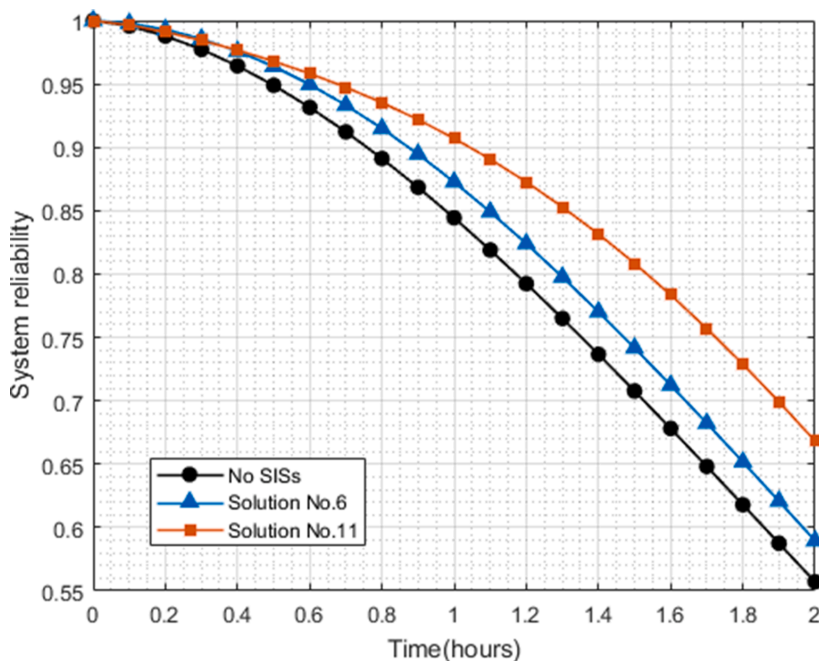


Fig. 14. System reliability of the two solutions.

calculation efficiency of the method is expected to be further improved. However, the method is applicable for systems incorporating a moderate number of CAFs in most cases.

This paper has focused on SIS reliability and durability, but the other indicators, such as response time, capacity, and robustness, can also be important. Hence, they can be the research in the future. In addition, the assumption of constant cascading probability is somewhat restrictive; statistical dependency (e.g., time-dependent cascading probability) can be considered. Another direction of future work is extending the method to more complex systems (e.g., network systems and hierarchical systems) to investigate more interdependent relationships between SISs and CAFs.

Authorship contributions

The specific contributions made by each author (Lin Xie, Mary Ann Lundteigen, Yiliu Liu) is listed as below.

Conception and design of study: Lin Xie, Mary Ann Lundteigen, Yiliu Liu;

Acquisition analysis and interpretation of data: Lin Xie, Yiliu Liu;

Drafting the manuscript: Lin Xie;

Revising the manuscript critically: Mary Ann Lundteigen, Yiliu Liu.

Declaration of Competing Interest

All the authors of this paper certify that they have NO affiliations with or involvement in any organization or entity with any financial interest (such as honoraria; educational grants; participation in speakers' bureaus; membership, employment, consultancies, stock ownership, or other equity interest; and expert testimony or patent-licensing arrangements), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

Acknowledgments

The authors appreciate Dr. Gregory Levitin's inspiration at the beginning of this work and valuable suggestions afterward. We also acknowledge the anonymous reviewers for their comments.

References

- [1] Rausand M. *Reliability of safety-critical systems: theory and applications*. Hoboken, New Jersey, USA: John Wiley & Sons; 2014.
- [2] Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliab Eng Syst Saf* 2014;121:43–60.
- [3] Xing L. Cascading failures in internet of things: review and perspectives on reliability and resilience. *IEEE Internet Thing J* 2020;8:44–64.
- [4] Cozzani V, Spadoni G, Reniers G. Approaches to domino effect prevention and mitigation. *Domino Effects in the process industries*. MA, USA: Elsevier; 2013. p. 176–88.
- [5] Abdolhamidzadeh B, Abbasi T, Rashtchian D, Abbasi SA. Domino effect in process-industry accidents—an inventory of past events and identification of some patterns. *J Loss Prev Process Ind* 2011;24:575–93.
- [6] Zhou J, Coit DW, Felder FA, Wang D. Resiliency-based restoration optimization for dependent network systems against cascading failures. *Reliab Eng Syst Saf* 2021; 207:107383.
- [7] Ash J, Newth D. Optimizing complex networks for resilience against cascading failure. *Physica A* 2007;380:673–83.
- [8] Motter AE. Cascade control and defense in complex networks. *Phys Rev Lett* 2004; 93:098701.
- [9] Wang J. Mitigation strategies on scale-free networks against cascading failures. *Physica A* 2013;392:2257–64.
- [10] Janssens J, Talarico L, Reniers G, Sørensen K. A decision model to allocate protective safety barriers and mitigate domino effects. *Reliab Eng Syst Saf* 2015; 143:44–52.
- [11] Khakzad N, Reniers G. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. *Reliab Eng Syst Saf* 2015;143:63–73.
- [12] Yang S, Chen W, Zhang X, Yang W. A Graph-based method for vulnerability analysis of renewable energy integrated power systems to cascading failures. *Reliab Eng Syst Saf* 2021;207:107354.
- [13] Wu Y, Chen Z, Zhao X, Gong H, Su X, Chen Y. Propagation model of cascading failure based on discrete dynamical system. *Reliab Eng Syst Saf* 2021;209:107424.
- [14] Landucci G, Argenti F, Tugnoli A, Cozzani V. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. *Reliab Eng Syst Saf* 2015;143:30–43.

- [15] Bucelli M, Landucci G, Haugen S, Paltrinieri N, Cozzani V. Assessment of safety barriers for the prevention of cascading events in oil and gas offshore installations operating in harsh environment. *Ocean Eng* 2018;158:171–85.
- [16] Korczak E, Levitin G. Survivability of systems under multiple factor impact. *Reliab Eng Syst Saf* 2007;92:269–74.
- [17] Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliab Eng Syst Saf* 2001;71:249–60.
- [18] Khakzad N, Khan F, Amyotte P, Cozzani V. Domino effect analysis using Bayesian networks. *Risk Anal* 2013;33:292–306.
- [19] Liu Y, Rausand M. Reliability assessment of safety instrumented systems subject to different demand modes. *J Loss Prev Process Ind* 2011;24:49–56.
- [20] Dhulipala SL, Flint MM. Series of semi-Markov processes to model infrastructure resilience under multihazards. *Reliab Eng Syst Saf* 2020;193:106659.
- [21] Rahnamay-Naeini M, Hayat MM. Cascading failures in interdependent infrastructures: An interdependent Markov-chain approach. *IEEE Trans Smart Grid* 2016;7:1997–2006.
- [22] Zou Q, Chen S. Enhancing resilience of interdependent traffic-electric power system. *Reliab Eng Syst Saf* 2019;191:106557.
- [23] Bao M, Ding Y, Shao C, Yang Y, Wang P. Nodal reliability evaluation of interdependent gas and power systems considering cascading effects. *IEEE Trans Smart Grid* 2020;11:4090–104.
- [24] Kong J, Simonovic SP. A model of interdependent infrastructure system resilience. *Int J Safety and Secur Eng* 2018;8:377–89.
- [25] Liu Y. Safety barriers: Research advances and new thoughts on theory, engineering and management. *J Loss Prev Process Ind* 2020;104260.
- [26] IEC61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: International Electrotechnical Commission; 2010.
- [27] Xie L, Lundteigen MA, Liu Y. Safety barriers against common cause failure and cascading failure: literature reviews and modeling strategies. In: 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM); 2018. p. 122–7.
- [28] Cai B, Li W, Liu Y, Shao X, Zhang Y, Zhao Y, et al. Modeling for evaluation of safety instrumented systems with heterogeneous components. *Reliab Eng Syst Saf* 2021: 107823. vol. pp.
- [29] Johansen IL, Rausand M. Barrier management in the offshore oil and gas industry. *J Loss Prev Process Ind* 2015;34:49–55.
- [30] Skjet S. Safety barriers: definition, classification, and performance. *J Loss Prev Process Ind* 2006;19:494–506.
- [31] Hauge S, Lundteigen MA, Hokstad P, Håbrekke S. *Reliability prediction method for safety instrumented systems-PDS method handbook 2010 edition*, 2013.
- [32] Zhang N, Fouladirad M, Barros A. Optimal imperfect maintenance cost analysis of a two-component system with failure interactions. *Reliab Eng Syst Saf* 2018;177: 24–34.
- [33] Liu Y, Rausand M. Reliability effects of test strategies on safety-instrumented systems in different demand modes. *Reliab Eng Syst Saf* 2013;119:235–43.
- [34] Alizadeh S, Sriramula S. Unavailability assessment of redundant safety instrumented systems subject to process demand. *Reliab Eng Syst Saf* 2018;171: 18–33.
- [35] Meng H, Kloul L, Rauzy A. Modeling patterns for reliability assessment of safety instrumented systems. *Reliab Eng Syst Saf* 2018;180:111–23.
- [36] Xie L, Lundteigen MA, Liu Y. Performance assessment of K-out-of-N safety instrumented systems subject to cascading failures. *ISA Trans* 2021.
- [37] Azizpour H, Lundteigen MA. Analysis of simplification in Markov-based models for performance assessment of Safety Instrumented System. *Reliab Eng Syst Saf* 2019; 183:252–60.
- [38] Ding L, Wang H, Jiang J, Xu A. SIL verification for SRS with diverse redundancy based on system degradation using reliability block diagram. *Reliab Eng Syst Saf* 2017;165:170–87.
- [39] Yu H, Zhao Y, Mo L. Fuzzy reliability assessment of safety instrumented systems accounting for common cause failure. *IEEE Access* 2020;8:135371–82.
- [40] Gascard E, Simeu-Abazi Z. Quantitative analysis of dynamic fault trees by means of Monte Carlo simulations: event-driven simulation approach. *Reliab Eng Syst Saf* 2018;180:487–504.
- [41] Guo H, Zheng C, Iu HH-C, Fernando T. A critical review of cascading failure analysis and modeling of power system. *Renew Sustain Energy Rev* 2017;80:9–22.
- [42] Wu S, Zhang L, Lundteigen MA, Liu Y, Zheng W. Reliability assessment for final elements of SISs with time dependent failures. *J Loss Prev Process Ind* 2018;51: 186–99.
- [43] Abdelmoez W, Nassar D, Shereshevsky M, Gradetsky N, Gunalan R, Ammar HH, et al. Error propagation in software architectures. In: 10th International Symposium on Software Metrics; 2004. p. 384–93.
- [44] Cozzani V, Gubinelli G, Antonioni G, Spadoni G, Zanelli S. The assessment of risk caused by domino effect in quantitative area risk analysis. *J Hazard Mater* 2005; 127:14–30.
- [45] Murthy D, Nguyen D. Study of two-component system with failure interaction. *Naval Res Logistic Q* 1985;32:239–47.
- [46] Xie L, Lundteigen MA, Liu Y. Reliability and barrier assessment of series-parallel systems subject to cascading failures. *Proc Inst Mech Eng, Part O: J Risk Reliab* 2020;234:455–69.
- [47] Levitin G, Xing L, Ben-Haim H, Dai Y. Reliability of series-parallel systems with random failure propagation time. *IEEE Trans Reliab* 2013;62:637–47.
- [48] Liu B, Wu J, Xie M. Cost analysis for multi-component system with failure interaction under renewing free-replacement warranty. *Eur J Oper Res* 2015;243: 874–82.
- [49] Rausand M, Høyland A. *System reliability theory: models, statistical methods, and applications*. 2nd. Hoboken, New Jersey, USA: John Wiley & Sons; 2004.
- [50] Jin H, Lundteigen MA, Rausand M. Uncertainty assessment of reliability estimates for safety-instrumented systems. *Proc Inst Mech Eng, Part O: J Risk Reliab* 2012; 226:646–55.

This page is intentionally left blank

Article VIII

Xie, Lin; Ustolin, Federico; Lundteigen, Mary Ann; Li, Tian; Liu, Yiliu. Performance analysis of safety barriers against cascading failures in a battery pack. *Submitted to Reliability Engineering and Safety System.*

This paper is awaiting publication and is not included

This page is intentionally left blank

ISBN 978-82-326-6376-7 (printed ver.)
ISBN 978-82-326-6373-6 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)



NTNU

Norwegian University of
Science and Technology