Doctoral theses at NTNU, 2021:36

Doctoral thesis

Aibo Zhang

Prognostics and health management of safety-instrumented systems

Approaches of degradation modeling and decision-making

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

NTNU
Norwegian University of
Science and Technology

Aibo Zhang

Prognostics and health management of safety-instrumented systems

Approaches of degradation modeling and decision-making

Thesis for the Degree of Philosophiae Doctor

Trondheim, February 2021

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

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Engineering
Department of Mechanical and Industrial Engineering

© Aibo Zhang

ISBN 978-82-471-4982-9 (printed ver.)
ISBN 978-82-471-4991-1 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2021:36

Printed by NTNU Grafisk senter

‘You took the sourest lemon that life has to offer, and turned it into something resembling lemonade.’

—This is us

Preface

This thesis is prepared in partial fulfillment of the requirements for the degree of Doctor of Philosophy at the Faculty of Engineering, the Norwegian University of Science and Technology (NTNU). The main work of the PhD thesis was carried out at the Department of Mechanical and Industrial Engineering (MTP), but I also spent six months at School of Mechanical, Materials, Mechatronic and Biomedical Engineering at University of Wollongong (UOW), Australia as part of my PhD study.

After I received my MSc degree from China University of Petroleum (Beijing), I got a job offer and had signed a contract with SINOPEC (Shanghai). There was a struggle choice process between the permanent job and accepting the offer to pursue a PhD abroad. Finally, I decided to embark on the journey fulfilling challenges and uncertainties, rewards and discouragements. Now looking back, I can not be totally sure whether it is the right decision. But, I have never regretted my endeavors I paid for my own decision. The journey from first stepping on the land of Norway to the very end of my PhD has been a unique experience in my life. Even though there were moments doubting myself to continue, the process cultivates self-adjustment ability strengthening me for future challenges. As the journey close to the end, and I will for sure look back at my time as a PhD candidate in the RAMS group with gratefulness and pride.

Trondheim, Norway
February, 2021
Aibo Zhang

Acknowledgments

I am deeply grateful to my supervisors, colleagues, friends and families who have contributed to this PhD research and supported me in this journey: It could not be carried out without support, guidance, and inspiration from you.

First and foremost, I would like to show my deepest appreciation to my main supervisor, Professor Yiliu Liu, for all his tireless guidance, enthusiastic encouragement and support during these years. He shared with me his knowledge on RAMS analysis, as well as his experience in doing research. Besides the role of supervisor, he is also a supportive friend. He devoted to me tremendous time and continuous energy on reviewing my papers and the thesis over and over again. It has been a great honor to pursue my PhD under his supervision.

I am deeply indebted to my co-supervisor, Professor Anne Barros, who has given valuable ideas and insightful feedback on degradation and maintenance modeling. Her encouragement has been inspired me to move forwards.

My grateful thanks are also extended to Professor Tieling Zhang, from UOW, Australia and Professor Yanfu Li, from Tsinghua University, China, for their professional guides and hosting during the visiting period. It was a great experience to work with them. Many thanks to Professor Elias Kassa for the financial support of the international exchange, which is beneficial for my future career development either in academia or industry.

A warm thank to my great colleagues in the RAMS group for the nice coffee breaks, social events, RAMS seminars and conferences we had and shared. The lovely Shenae Lee, thanks for remembering my birthday and the gift every year. Lin, thanks for being my supportive friend over these years and the 'Chief Entertainment Officer (CEO)' for RAMS group with organized many meaningful social events. 'Prof' Renny and Himanshu, thanks for being my friends and having either serious or aimless talks from now and then. Also thanks to other colleagues for joys and laughs we had. It is a good experience to work with you. I would like to thank administrative staff at department of Mechanical and Industrial engineering for the friendly working environment and helpful support.

I am especially thankful to my closest friends, Haoshui, Li, Yuequn, Siqi, Dongming, Xinge for friendship and happy moments together.

Last but not the least, I want to thank my families for their never-ending supports and unconditional love in my whole life.

Summary

Modern industries are developing towards a high-integrated direction with overwhelming complexities bringing benefits and potential risks with catastrophic consequences simultaneously. To reduce the occurrences of undesired events or mitigate their consequences, safety-instrumented systems (SISs), as a type of technical safety barrier, have been widely installed in different applications with the aim to protect people, the environment, and other valued assets. Examples of SISs can be emergency shutdown systems in oil & gas production, airbags in cars, fire sprinkler systems in buildings, etc.

Many SISs operate in a demanded mode, meaning that they are only activated to perform safety functions while the unexpected occurs. For such systems mainly dormant in normal operation, it is important to conduct proof tests for checking system states and following-up maintenance in case of failures, to keep SISs highly available so as to ensure safety. In current studies, these activities are assumed following a predefined scheme with fixed intervals, independent from the actual system state. However, when more SIS state information can be collected by sensors and in manual tests, the prognostics and health management (PHM) strategy is expected to be more reasonable and cost-efficient. This PhD project thus aims to explore a new approach to evolve the SISs management from time-based to performance-based taking the technological advancement in data collection. This primary objective is then divided into five sub-objectives from the modeling approach and decision-making aspects that are addressed in the form of four journal articles and two conference papers.

This PhD thesis bridges SISs performance assessment and degradation process through addressing different influence factors in the operational phase, including aging, and impact of demands, etc, for the decision-making in PHM by proposing:

1. A stochastic process-based degradation model with a specific threshold to describe the time-dependent system performance deviations with the target performance requirement. This model releases the as-good-as-new assumption even though the system is verified as being functional in tests. The proposed stochastic process-based degradation model provides an advantage of calculating the conditional system performance based on the collected information in tests.

2. An approach to quantify the side-effect of operational history on system degradation by introducing abrupt Gamma-distributed increments following a homogeneous Poisson process with arrival rate λ_{de}. Impacts of random demands are thus

considered in performance evaluation.

3. A maintenance strategy with multiple follow-up actions to adapt the manifested system state in tests. The role of preventive maintenance on SIS management is emphasized in the operational phase. Relying on effective collected information contributes, such a strategy helps to keep an SIS at the required safety level while reducing the frequency of corrective maintenance.

4. A new decision-making support tool on updating testing and maintenance activities with coordinating the system unavailability and life cycle cost. The conditional system unavailability in the required safety integrity level will be the priority principle for updating test intervals, accompanying lower estimation intervention cost in the life cycle.

The practical utility of the thesis resides in the provision of a comprehensive consideration of the time- and event-dependencies of SIS performance, as well as safety and economic meanings of testing and maintenance activities. In particular, the first is to provide hints of system deterioration and relevant health management to reliability analysts when they evaluate SIS design. The second is for operational managers of SISs as the decision-makers, to help them to update testing and maintenance plans and identify the optimal intervention opportunities.

To conclude, this thesis will contribute to the implementation of PHM on SISs and other systems with similar operational characteristics. The research results on degradation assessment and predictive maintenance optimization can be generalized to more applications where production and maintenance need to be in synergy in consideration of safety and economics. Further research is, however, necessary for testing and validating the proposed methods with practical cases.

Contents

List of Tables

List of Figures

Part I

MAIN REPORT

Chapter 1

Introduction

1.1 Background

To fulfill the expanding demands on functionality and quality, modern industries are often built with overwhelming complexities [1]. Benefits made with these high-integrated systems are accompanied by concerns about the potential risks and the catastrophic consequences. Although a general definition is absent, the risk for engineered systems is related to accidents where an abrupt event may give negative outcomes, e.g. loss or damage [2]. When faced with unpredictable risks, the question is how well we have prepared to manage them.

Management of risk is in an evolving scenario, and ISO 31000 [3] provides principles and generic guidelines for organizing these works as a cycle process including risk identification, assessment, treatment, and monitoring and review. Risk identification, analysis, and evaluation provide the basis for decisions about the treatment which refers to the process to modify risk [4]. Risk treatment depends on the type and nature of the risk from two dimensions including the likelihood of hazardous events and the consequences that could occur.

With the purpose to reduce the occurrences or mitigate the consequence on people, the environment, and other assets in case that the undesired event occurs in a system under control (EUC), protection equipment or familiar features have been installed [2]. Fortunately, severe accidents have a low probability of occurrence thanks to multiple barriers in place [5], and thus the importance of safety barriers is demonstrated when they are absent or inefficient, through tragic accidents range from single-person accidents up to disasters such as the Fukushima Daiichi nuclear power accident in Japan, the high-speed train crash in China, and the Macondo accident in the Gulf of Mexico.

The scope and types of safety barriers are upon the industries, also with ambiguous classification principles, e.g. operational types, bow-tie model, etc [6], [7]. For example, the concrete obstacles on bridges and road edge for avoiding driving out of way in road transportation, airbag and brake in automobiles, etc. When safety barriers are technical systems, whose failure may lead to harm to people, economic loss, and /or environmental damage, they can be called safety-critical systems, e.g. emergency shutdown system in process industry, traffic signal system in railway and fire & gas detection system.

Safety-critical systems that are based on electrical, electronic, or programmable electronic (E/E/PE) technology are called safety-instrumented systems (SISs), especially in process industries [8]. E/E/PE devices of SISs interact with mechanical, pneumatic, and hydraulic systems [9]. Consistent with the purpose of safety barriers, an SIS is installed to bring the equipment under control (EUC) to a safe state given that a hazardous event occurs. Normally, an SIS can be functionally divided into three subsystems: sensor subsystem to detect the abnormal state of EUC, e.g. high pressure or high temperature; logic solver subsystem to receive and deal with the signal from sensor subsystem, and send an instruction to the final element; final element subsystem to be activated and implement the predefined function as a response. These three subsystems are used to perform safety-instrumented functions (SIFs).

Each SIS can be allocated with specific requirements in terms of risk reduction in the design phases. However, in the operational phase, its performance in fulfilling the above requirements is not immutable with the influence of factors, e.g. demand rates and operation conditions, etc., as they may fail or not be strong enough to implement predefined functions. To keep the required functions of SISs available, a diversity of activities are therefore conducted, e.g, for the oil & gas industry, including operation, testing and maintenance, monitoring and verification, and management of change, throughout the operational lifetime [10].

Testing and maintenance activities are of vital importance in keeping SIS performance and preventing failures [8]. Like most other systems, an SIS, especially in its final element, is subject to degradation and failures, and testing and maintenance are thus helpful for examining the system state and slowing/stopping the degradation processes. Negative consequences of degrading or failed components in SISs can be mitigated or even eliminated [11]. However, to date, existing testing and maintenance decisions are made in a conservative open-loop fashion, referred to as time-based proof testing and maintenance. That is, a predefined intervention interval is strictly followed, where the actual state of the SISs after proof test does generally not influence these decisions. Such an approach can result in unnecessary proof tests and expense intervention cost of EUC, which does not need it. Thus, the management of SISs calls for an upgrade that shifts from time-based proof testing and maintenance approach moving forwards toward a performance-based transformation, resulted from several following prerequisites:

1. More frequent testing and maintenance are not always beneficial. Such activities can bring in not only higher costs but losses and new hazardous events in EUC. SISs interact with the EUC directly. The tests of SISs may suspend the production process and lead to losses and costs. The existence of conflict is confirmed between the need for realistic proof testing and the need to minimize downtime, particularly within high throughout continuous processes such as refining and bulk chemical manufacture [12]. Additionally, shutdown and restart are sometimes hazardous operations with increasing the EUC risk during these operations [8];

2. Failures of SISs can occur due to degradation. A more important reason for updating SIS management is that the failure of SISs may lead to significant consequences, as the aforementioned painful disasters. Thanks to some unavoidable degradation mechanisms, especially for mechanical units, periodic tests are not always applicable after a certain service time;

3. Reliability assessment is insufficient in considering degradation. Planned periodical proof tests and immediate follow-up maintenance are assumed in most studies related to SISs whose reliability analysis relying on lifetime distribution, but they are not always effective in controlling the failure probability of SIS when degradation is taken into account.

4. Advanced sensors and computer systems have provided possibilities to make more condition and operational information acquired during tests available to model the SIS degradation process. Numerous parameters, such as lubricant ingredient, corrosion extent and so on, can be measured and utilized for failure prediction and diagnosis [13]. From these possible information, an ideal health indicator can be extracted to represent the system status, e.g. leakage rate, the closing time for valves [14], [15].

Up to this point, one may have a question: is it possible to minimize the intervention of EUC, e.g. testing and maintenance, and meanwhile to guarantee the predefined functions of SISs? The answer to this question has existed in many applications: yes, a well-developed framework-prognostics and health management (PHM), which is most desired in mission-critical applications [16], e.g. aerospace [17], lithium-ion battery [18], has the potential to emerge as a solution toward proactive SISs management. According to CALCE (Center for Advanced Life Cycle Engineering), PHM is the means to predict and protect the integrity of equipment and complex systems, to avoid unanticipated operational problems leading to mission performance deficiencies, degradation, and adverse effects to mission safety [19]. Haddad et al [20] regard PHM is a discipline that uses for (1) evaluating the reliability of systems of their life cycle; (2) determining the possible occurrence of failures and risk reduction; and (3) highlighting the remaining useful lifetime (RUL) estimation.

In view of successful applications in other fields, PHM is expected to be able to provide a new paradigm for SISs management. The framework of PHM will give a much-needed boost to the management of SISs shifting from the acknowledged time-based to performance-based testing and maintenance. However, PHM is not tailor-made for SISs. To transplant PHM on SISs, at least the following gaps need to be addressed:

1. Lack of system behavior description method. It is undoubtedly that the performance of SISs in the operational phase is subject to both intrinsic (e.g. material) and extrinsic (e.g. operating condition) factors [21]. These factors result in typical failure mechanisms that could contribute to the degrading performance of SISs. For example, valves used in offshore oil platforms could undergo erosion caused by the sand grains transported by the oil-water-gas mixture extracted from the well [22].

A primary issue is how to develop lifetime models based on the information on the SIS degradation trend during operation.

2. Absence of holistic decision-making approaches. The SISs are designed and implemented to protect EUC. It is unreasonable to isolate the decision-making of testing and maintenance on SISs from the protected EUC. In terms of intervention actions, ‘too often’ testing and maintenance lead to a major economic consequence, while major consequences in relation to safety for ‘too less’ ones. This trade-off between economic and safety also exists when conducting the update for upcoming testing intervals based on actual performance in prior tests. Therefore, a novel holistic decision-making rule is of priority to investigate.

As a response to the summarized gaps, the ambition of this PhD project is to model SIS operations relying on the system condition and performance monitoring, and design condition-based and dynamic testing and maintenance policies in the life cycle of SISs. The ultimate objective is to achieve a performance-based management of SISs, reference to the procedures and methods of PHM, to reduce interventions including testing and maintenance while keeping sufficient safety integrity.

1.2 Objectives

The primary objective of this PhD thesis is to design tailor-made models and tools to implement PHM for SISs. A particular focus is given to the mechanical final element which is the main contributor to system degradation and failures.

To realize the primary objective, the following specific research tasks will be conducted:

1. Developing a performance-based management approach for SISs under the scope of PHM procedures.
2. Proposing new lifetime models based on the system deterioration trend to investigate the effects of certain factors, e.g. continuous degradation, operational history, and consequent to estimate the remaining useful life.
3. Regulating testing and maintenance schedule based on data analysis and system condition information collected in prior proof tests.
4. Providing new decision-making support rules for proof testing and maintenance of SISs, to ensure compliance and cost-effective operation.

1.3 Structure of the thesis

The thesis consists of two parts: Part I Main report, Part II Articles.

Part I introduces the background of the research, how the research has been conducted, and highlight the overall contributions of this thesis.The remainder of Part I is structured as follows:

- Chapter 2 summarizes the theoretical background of the research;

- Chapter 3 describes the research questions and objectives of the thesis;
- Chapter 4 outlines the research methodology and work process;
- Chapter 5 discusses the main results;
- Chapter 6 presents overall conclusions and future work.

Part II includes the 6 research articles that have been published or under revisions during the PhD project, in peer-reviewed international journals or conference proceedings.

Table 1.1: List of articles in Part II

Article	Type	Title	Reference
Article I	C	Prognostic and health management for safety barriers in infrastructures: Opportunities and challenges.	[23]
Article II	J	Performance analysis of redundant safety-instrumented systems subject to degradation and external demands	[24]
Article III	C	A degrading element of safety-instrumented systems with combined maintenance strategy	[25]
Article IV	J	Optimization of maintenances following proof tests for the final element of a safety-instrumented system	[26]
Article V	J	Study of testing and maintenance strategies for redundant final elements in SIS with imperfect detection of degraded state	[27]
Article VI	J	Optimal activation strategies for heterogeneous channels of safety instrumented systems subject to aging and demands	[28]

C-Conference paper; J-Journal paper

Chapter 2

Theoretical Background

The intention of a theoretical background review chapter is twofold. The first is to extract the research questions based on the systematic understanding of state-of-the-art within the relevant field. The second is to provide a foundation for choosing appropriate approaches and methodologies to solve extracted research questions.

Section 2.1 introduces a general review of risk and risk analysis, and emphasizes the role of safety barriers in risk treatment;

Section 2.2 presents a sketch review of safety barriers and classification and anchor SISs under the umbrella, followed by the failure analysis of SISs;

Section 2.3 provides an overview of the current studies on the performance measures of SISs;

Section 2.4 outlines the main activities to maintain the integrity and monitor SISs performance in the operational phase;

Section 2.5 summarizes and discusses the uncontrollable and controllable influencing factors related to SISs performance;

Section 2.6 reviews the maintenance transformation in industries and illustrates the procedure PHM, with the focus on the advantages and challenges of adopting PHM on SISs;

Section 2.7 states the scope and limitations of this PhD thesis.

2.1 Risk and risk analysis

In the last decades, industries are undergoing rapid changes in technology and business management. Along with considerable advantages of superior products and services, hazards have changes and the risk of large-scale accidents with significant losses has increased given an increase of complexity of processes and systems in operation [29].

In this evolving scenario, risk management is of importance to ensure that adequate measures are taken to protect people, the environment, and assets from harmful consequences of the activities being undertaken, as well as balancing different concerns, in particular, HSE (Health, Safety, and Environment) and costs [30].

ISO 31000 [3] provides principles and generic guidelines for organizations on risk management with a brief process depicted in Figure 2.1, which is a cycle process includes risk identification, assessment, treatment and monitoring and review.

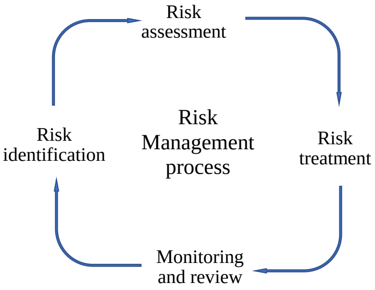


Figure 2.1: Risk management process

Since identified risks may have a varying impact, each risk should be assigned a combination of treatments that best suits both the risk itself and an organization's ability to influence the factors contributing to and the outcomes associated with the risk. The sequence of risk control should follow the prioritization of hazardous events that are ranked by the quantitative product of consequences and likelihood dimensions. The acknowledged risk treatment strategies are illustrated in Figure 2.2, and explained [31] as follows:

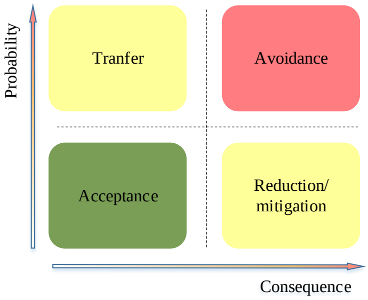


Figure 2.2: Risk treatment strategies

1. Avoidance: eliminate the threat normally by removing the cause of the threat altogether (e.g., remove activities);
2. Transfer: shift the impact of the threat to a third party (e.g., insurance, agreements);
3. Reduction/mitigation: reduce the probability or impact of a threat (e.g., requirements review, testing);
4. Acceptance: acknowledge the risk but take no action unless the risk occurs.

Risk reduction/mitigation, referring to measures to reduce the frequency or severity of losses, is necessary when it is possible in controlling unacceptable risks. To reduce/mitigate risks, different methods are used throughout the life of a system and categorized into inherent safety design and safety barriers. The former focus on early in the design process. When hazards to a system cannot be completely eliminated with their design, the latter will be supplementary measures [7], [32].

As a precondition for ensuring good risk management in industries, it is crucial for practitioners to have an understanding of why barriers are established and of which performance requirements have been specified for the barrier elements intended to realize the barrier's function.

2.2 Safety barriers and safety-instrumented systems (SISs)

2.2.1 Definition and classification of safety barriers

The concept of safety barrier is based on protection layers in the Layers of Protection Analysis (LOPA) method, which is used in risk analysis with a series of hierarchically organized protective layers to lower the risk of undesired events [33]. Process industry, like nuclear, aviation, and others, faces the risk of major accidents, i.e. accidents with a major consequence - typically multiple fatalities and/or massive oil spills [34]. Therefore, multiple safety barriers have been carried out to reduce the risk of these accidents. A general risk reduction framework is presented in IEC61508 to achieve tolerable risk, as shown in Figure 2.3.

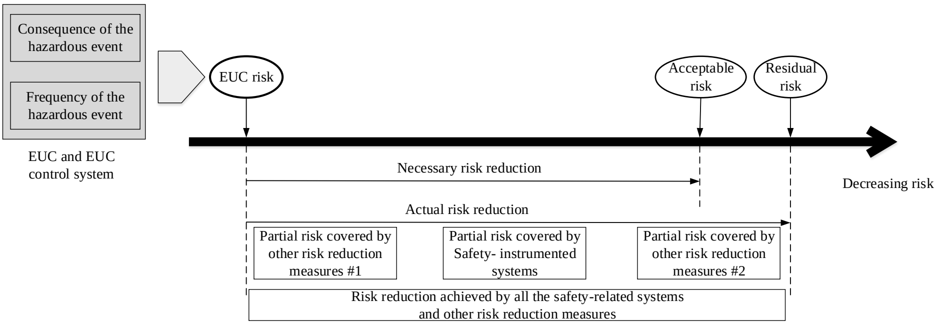

Consequence of the hazardous event
Frequency of the hazardous event
EUC and EUC control system
EUC risk
Acceptable risk
Residual risk
Decreasing risk
Necessary risk reduction
Actual risk reduction
Partial risk covered by other risk reduction measures #1
Partial risk covered by Safety- instrumented systems
Partial risk covered by other risk reduction measures #2
Risk reduction achieved by all the safety-related systems and other risk reduction measures

Figure 2.3: The framework of risk reduction

Safety barrier is also based on the energy-barrier model, where the identification of possible barriers is the prerequisite of preventing the undesired accidents by building a firewall between energy as a threat to potential victims [35]–[37].

To today, an industrial consensus is yet to be reached with regard to the definition and classification of safety barriers. The common ground in the existing definition is that a safety barrier is a measure to prevent or protect against hazardous events [6], [38]–[40]. In order to be effective, safety barriers often rely on a combination of physical, function, symbolic and incorporeal barrier systems [41]. One safety barrier can perform one or more safety functions, which determine the purpose of the barrier [42]. Barriers can be classified in different ways. An acknowledged criterion is based on the widely used bow-tie model in risk analysis. As shown in Figure 2.4, barriers, like B1 and B2, between threats and hazardous event (the cause side) are proactive barriers or preventive barriers, to reduce the probability of the hazardous event; While the barriers, like B7 and B8, between the hazardous event and consequences (the consequence side), are reactive barriers or protection barriers, for reducing the consequences of the event [6]–[8], [43]. In addition, several selected classification methods are introduced briefly in Table 2.1.

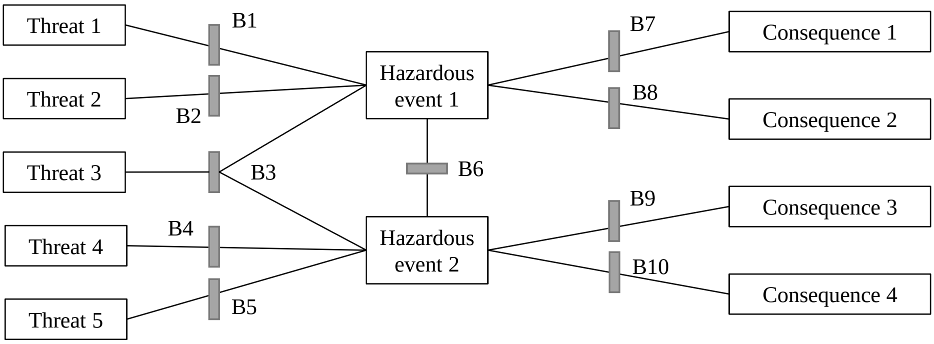


Figure 2.4: An extended bow-tie model

Table 2.1: Selected barrier classification methods

Method	Result	Description
Operational modes [2], [44], [45]	active	Dependent on some energy sources and a sequence of detection-diagnosis-action to perform its function
	passive	Does not require any human actions, energy sources, or information sources to perform its function
Time-sensitivity[46]	static	With constant performance
	dynamic	With performance degradation rate
Time aspects[47]	on-line	Continuously functioning
	off-line	Need to be activated

A systematic classification method is recommended by Sklet [6], [40] is shown in Figure 2.5. The classification of the active, technical barrier is in accordance with IEC 61511 [48]. The technical barriers are further divided into three groups: Safety Instrumented System (SIS), meaning that a technical barrier which involves the electric, electronic, and programmable electronic (E/E/PE) technologies, other technology safety-related systems and External risk reduction facilities.

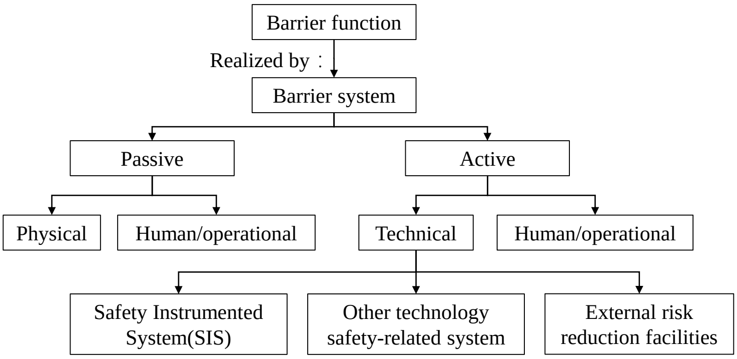


Figure 2.5: Classification of safety barriers

2.2.2 Safety-instrumented systems

Safety barriers are versatile, this PhD thesis will pay more attention to a type of technical safety barriers with the term as safety-instrumented system (SIS), or E/E/PE safety related system given the involved technologies. A simple SIS functionally consists of three subsystems: sensor, logic solver and final element subsystem, as shown in Figure 2.6.

1. *Senor subsystem* — detects the abnormal situations in EUC and produces a signal sent to the logic solver, such as pressure transmitters, temperature sensors, level sensors and so on;

2. *Logic solver subsystem* — initiates an instruction for the action of the final element based on predefined logic as a response to the detected abnormal situation in EUC.

3. *Final element subsystem* — performs the safety function. Examples of final elements are shutdown valves, circuit breakers, fans, and so on.

A typical example here is a high integrity pressure protection system (HIPPS) in the process industry with the fundamental task to close the flow in the pipeline when the pressure beyond the specialization, whose architecture is shown in Figure 2.7. Redundancy with two or more items, referred to as fault tolerance, is often employed to continue system function in case of one item fails, e.g. three pressure transmitters (PTs) and Valve 1, Valve 2 in the HIPPS.

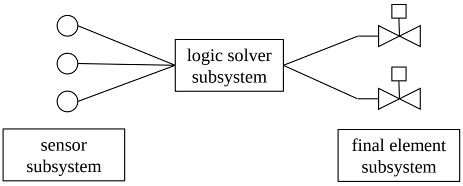


Figure 2.6: Sketch of a simple SIS

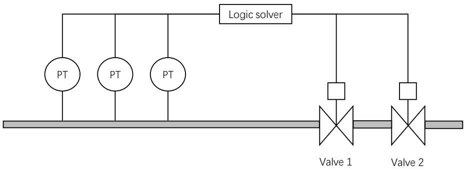


Figure 2.7: Example of a HIPPS

A complete safety instrumented function (SIF) for the HIPPS originates from the detection of abnormal situations in EUC (high pressure in the pipeline) by sensor subsystem-pressure transmitters. An action instruction is initiated based on predefined logic in the logic solver subsystem as a response to the detected abnormal situation in EUC, then, the function (close the flow) is executed in the final element subsystem (Valve 1 and Valve 2) if it is necessary.

An event or a condition that requires a SIF to be activated is called demand. The frequency that an SIF is demanded varies from system to system. Following the different demand frequencies, IEC 61508 defines three modes of operation for SISs, including low-demand, high-demand, and continuous mode. The so-called low-demand means that the frequency of demands on an SIS is up to once a year.

When an SIS is regarded as operating in a demanded mode, especially in a low-demand mode, it stays in a dormant state without performing any active function during normal operation but is an add-on to the EUC and is only called upon when demands occur. In case of occurrences of failures, e.g. failure of a shutdown valve to close when it is needed, these negations are unknown and remain hidden until demands come. In practice, to manifest the ability to perform the required SIF, proof tests are also arranged in advance to verify the SIS.

2.2.3 Failure analysis of SISs

The objective of an SIS is to bring the EUC into a safe state when demand occurs. Normally, the performance criteria in terms of a certain SIF is a target value with deviation, which to some extent relies on specific working conditions. If the actual performance is within the acceptable limits of deviation from the desired performance (target value), the performance of SIS is acceptable and the SIS can be qualified as functioning. If the actual performance is beyond the acceptable limits, the SIS is not effective any longer in terms of the required function for risk control. The SIS will be in a failed state until manifested in the proof test or real demand. The relation among performance, acceptable deviation, and failure are depicted in Figure 2.8 [8].

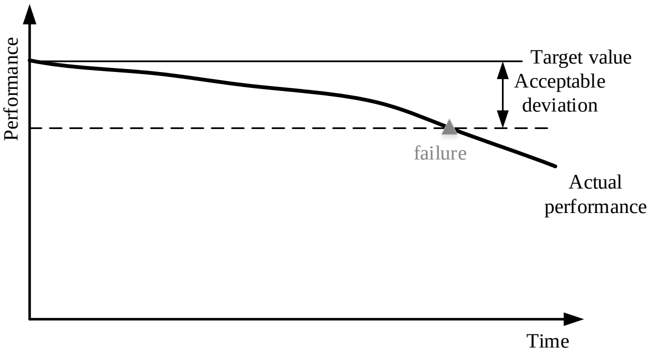


Figure 2.8: Performance, acceptable deviation, and failure

Based on consequence and detectability, failures in an SIS could be classified into four categories:

1. *Dangerous undetected* (DU) failures have the potential to put the SIS in a hazardous or fail-to-function state and are revealed only by proof-testing or a real demand occurs, such as leakage (through the valve) in the closed position (LCP), closing too slowly (CTS) for a shutdown valve.
2. *Dangerous detected* (DD) failures are detected a short time after occurring by the installed automatic self-testing modules which have a diagnostic function and detect some failures, such as signal loss, signal out of range, and final element in the wrong position.
3. *Safe undetected* (SU) failures do not have the potential to leave the SIS in a hazardous or fail-to-function state that is not detected by the installed automatic self-testing modules, such as failure to open.
4. *Safe detected* (SD) failures do not have the potential to leave the SIS in a hazardous or fail-to-function state that is detected by the installed automatic self-testing modules, such as a spurious trip.

However, in terms of dangerous failures, currently, DU failures that limit SIS required safety functions are dominant in the performance evaluation, and regular proof tests are still the main approach to ensure SIS high availability and EUC safety [48], [49]. To narrow down the scope, this thesis will focus on DU failures in low-demand which directly affecting the required functions.

2.3 Performance measures of SISs

Ideally, no accident would occur since there is a barrier, but in most cases, barriers, especially for SISs with mechanical and electronics elements, are not 100% reliable, e.g. fault state or not sufficient enough, some demands may pass the SISs and have negative effects on the EUC. Assessing the performance of SISs is of importance in preventing the potential undesired technological accidents [50].

Performance measures or indicators reflect how well SISs perform their predefined functions. Performance measures of SIS should be consistent with broad measures for safety barriers to some extent. The fulfillment of several requirements is the prerequisite of identifying as a relevant barrier, including effectiveness, response time, and level of confidence (reliability) [45]. Two quantitative indicators, availability and effectiveness, are considering in the prevention of domino scenarios triggered by fire [51]. Complexity and a proposed three-point scale of effectiveness (high, medium and low) in case of a threat initiation are two parameters to describe barriers [52].

With relation to the Norwegian Offshore Industry, five parameters are identified to characterize barrier performance as follows: functionality/effectiveness, reliability/availability, response time, robustness and triggering event/conditions [6], [53], [54]. The performance of SIS can be seen as comprising three elements, including functional, integrity, and vulnerability requirements, in accordance with the regulations of Petroleum Safety Authority (PSA) in Norway [55], [56].

To quantify and qualify the performance of SISs, several performance criteria is considered [2], [6]–[8]:

- *Functionality/effectiveness* refers to the ability to perform a specified function with meeting a certain requirement under given working conditions [6]. A comprehensive review of this term is summarized in [7] including similar terms in literature, e.g. efficiency or sufficiency. In many cases, effectiveness is linked with the response time which refers to the time for a safety barrier to fulfill the specified barrier function from a deviation occurs. The response time for the HIPPS is the time to closure the valves to fulfill the function of 'stop flow'.

- *Reliability/availability* is popular for active barriers that focus on quantifying its ability to perform its function or remain to be effective while needed, or on demand. The average reliability/availability of SISs to perform the required SIFs within a period of time is described as safety integrity in IEC 61511 [49] with four levels, with safety integrity level 1 (SIL1) being the least reliable and SIL 4 being the most reliable.

  When determining SIL with quantitative approaches, IEC standards and a lot of literature have adopted probability of failure on demand (PFD) for SISs in low-demand mode, with several scientific methods, including simplified formulas [8], [47], reliability block diagram [57], PDS method [58], Markov model [59]–[62] and Petri net [63]–[65], etc.

  PFD refers to the probability that a dangerous fault is present such that the SIF cannot be performed. Then we can have the PFD at time t as

  $$\mathrm{PFD}(t) = \Pr(\text{the SIF cannot be performed at time } t) \tag{2.1}$$

  In many case, it is sufficient to have an average value in a test interval (t_1, t_2). The long-term average PFD ($\mathrm{PFD_{avg}}$) between t_1 and t_2 can be expressed as

  $$\mathrm{PFD_{avg}} = \frac{1}{t_2 - t_1} \cdot \int_{t_1}^{t_2} \mathrm{PFD}(t)dt \tag{2.2}$$

  Normally, the SIF is proof-tested with a regular interval τ. It is quite obvious that $\mathrm{PFD_{avg}}$ will keep a constant value in each test interval with the assumption of exponential lifetime distribution and as-good-as-new after each test.

  Each SIS is designed to protect EUC given a specific SIL, to fulfill the requirement, the SIS in low-demand mode must have a $\mathrm{PFD_{avg}}$ in the corresponding interval specified in Table 2.2.

- *Robustness* is the ability to resist given accident loads and function as specified during the accident sequence. It emphasizes the ability of a safety barrier to withstand extreme events and resist being disabled by the activation of other barriers [2], [7].

Selecting meaningful and effective performance measures is of importance due to the involvement of SIS design, operation and maintenance activities [66]. Therefore, given the acknowledgment in industries and the advantage of quantitation, in this PhD thesis, $\mathrm{PFD_{avg}}$ will be used as the performance measure for SISs.

Table 2.2: SILs for low-demand SISs

SIL	PFD_{avg}
SIL 4	10^{-5} to 10^{-4}
SIL 3	10^{-4} to 10^{-3}
SIL 2	10^{-3} to 10^{-2}
SIL 1	10^{-2} to 10^{-1}

2.4 Activities to maintain SIS availability

To underpin the SIL requirement throughout the operational lifetime after installation, several activities are associated with SISs in the operational phase including operation, maintenance, monitoring, and management of change [67], [68]. The relationships among these activities with activities description are discussed in [68] and illustrated in Figure 2.9. During the operational phase, activities related to maintaining the SIL can be split into two categories based on the activities: (1) operation, maintenance, and modification; and (2) monitoring and verification. These two categories respectively correspond to 'maintain' and 'monitor' in Figure 2.9 with thoroughly discussed as follows.

2.4.1 Activities to maintain integrity

Activities related to maintaining integrity, including SIS operation, maintenance, and modifications, are explained here:

SIS operation: The installation of SISs is determined based on a hazard analysis and risk assessment, combined with risk acceptable criteria [69]. It implies that the context of hazard analysis presets the working conditions of SIS in the operational phase. SISs should be operational, regarding the allocated functions, for a certain service time within its specified in-service conditions. Therefore, in order to keep SISs reliable, several prerequisites need to be put on the table and classified after the design phase [70].

1. 'Intended function': The intended function of an SIS is predefined action in terms of undesired scenario in EUC and to bring the EUC into a safe state with a deliberate design [71]. While, the safe state is a relative condition which is based on a judgment of the acceptability of risk [2], at a certain level where is as low as reasonably practicable (ALARP) and the remaining risk is generally accepted. This involves having the design by qualified and competent engineers carrying out processes to a recognized functional safety standard, e.g. IEC 61508 and IEC 61511.

2. 'When the system is required to function': It is well known that the related SIF will be activated by the occurrence of abnormal deviation in EUC. The exact trigger point of activating one or more SIFs is required.

3. 'Satisfactory performance': To reduce risk, the SIS must often be activated quickly. For example, if 'valve A' actually closes with 10 seconds exceeding the required 8

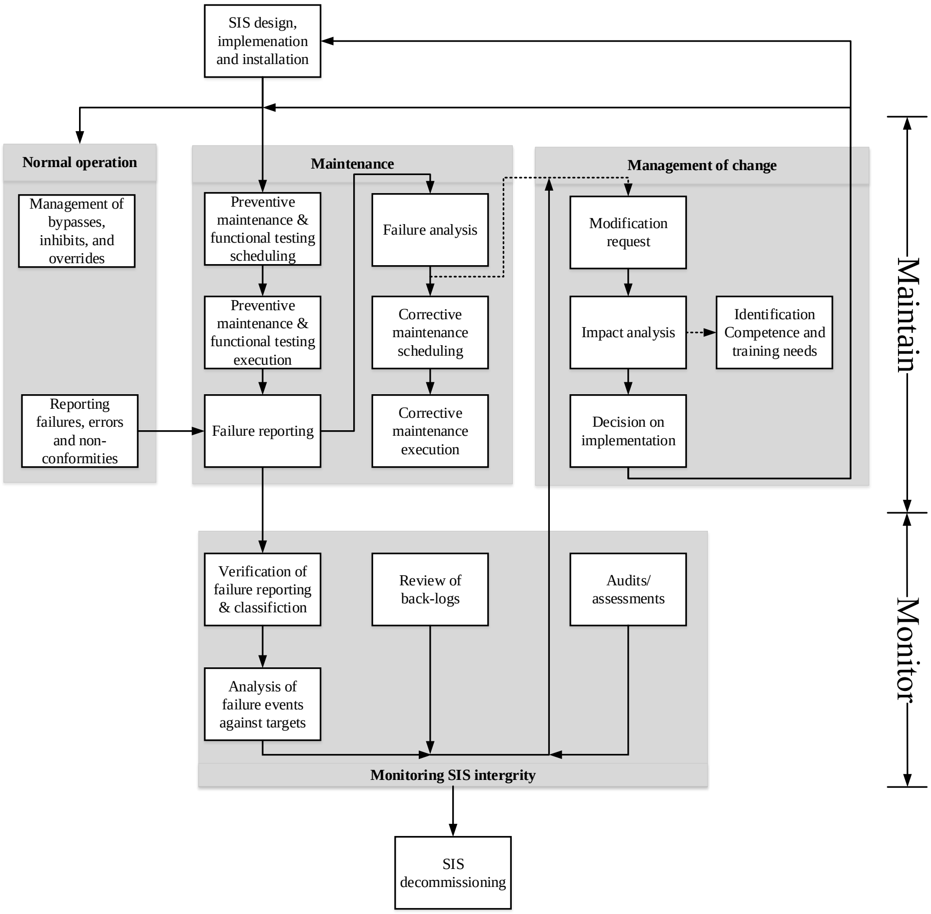

SIS design, implemenation and installation
Normal operation
Management of bypasses, inhibits, and overrides
Reporting failures, errors and non-conformities
Maintenance
Preventive maintenance & functional testing scheduling
Preventive maintenance & functional testing execution
Failure reporting
Failure analysis
Corrective maintenance scheduling
Corrective maintenance execution
Management of change
Modification request
Impact analysis
Identification Competence and training needs
Decision on implementation
Maintain
Verification of failure reporting & classifiction
Analysis of failure events against targets
Review of back-logs
Audits/ assessments
Monitoring SIS intergrity
Monitor
SIS decommissioning

Figure 2.9: Illustration of SIS activities in the operation phase

seconds, it will be treated as unsatisfactory performance because it will not protect a compressor separator from overfilling. When the proof test reveals that a valve has a slightly too long closing time, but still close to the boundary of acceptable limits, which could contribute to the postponed repair [8].

4. ‘Specified design limits’: Note that all claims for SIS performance can be valid only if the system is operated within its working environment limits and for the specific medium [72].

5. Device design lifetime: Many technical systems are subject to aging and deterioration, consequently, the reliability and availability degrade along with time during their design lifetimes, e.g. around 25 years [73], [74]. Both the recommended design lifetime and elapsed operating lifetime needs to be considered since several actions are linked, e.g. upcoming testing and monitoring, degradation mechanisms

modeling, etc.

Therefore, in the operational phase, improper actions should be avoided or at least strictly controlled, e.g. bypasses, inhibits, etc, given the possibility of introduction of systematic failures. In the event of an SIS failure, details regarding compensating measures, failure analysis, and relevant activities should be recorded.

SIS testing and maintenance: The SIS shall be regularly tested and inspected according to the manufacturer's safety manual. Taking these routine recurring work to keep SIS in its designed performance requirement. In the existing reliability assessment, it is often assumed that the proof test is perfect. It means that all DU faults are revealed during a proof test and the item is restored to an as-good-as-new condition. In the operational phase, several reasons challenge the assumption of perfect proof test [8], [68]:

1. A proof test is carried out under conditions that may never able to fully represent a real demand;

2. A proof test is inadequate to reveal all types of DU faults;

3. A proof test is stressful for the mechanical item of SISs and can introduce new failures [75].

The primary purpose of proof tests is finding weaknesses in maintenance strategy and root-cause identification with subsequent changes in the specification, design, installation, or strategy [70]. Meanwhile, any failure found in proof tests should be treated seriously, requiring immediate compensating measures to prevent failure failures.

Detailed maintenance procedures, supplied in the manufacturer's safety manual, may be categorized into preventive maintenance and corrective maintenance, including:

1. Preventive maintenance (initiated before failure): to extend the useful time of the system when some channels have a shorter life or a deteriorating performance, e.g. testing, inspection and lubrication [8]. PM actions are usually executed according to calendar time or operating hours based on the recommendations from manufacturers or user experience.

2. Corrective maintenance (initiated after failure): to execute repair actions in a timely manner to restore the failed channel to a functioning state after revealing faults in either proof testing or on-line diagnostics.

SIS modifications: The objective of modification is to address performance deviations and management activities to ensure the functional safety objectives. Several vital issues should be addressed before modification, including the initiation criteria, impact assessment, and gap analysis, etc.

2.4.2 Monitoring SIS performance

The monitoring of SIS is intended to maintain system integrity on the basis of information provided by some indicators on how the SIS complies with the specified safety requirement [76].

To manage risk during operation, the status and performance of SISs must be continuously and systematically verified and directly linked to the identified performance requirements of each element. Maintaining the performance shall from monitor the actual performance to verify and evaluate the performance, including, e.g. condition monitoring, testing and inspections, repair, overhaul, and replacement [5], [77].

During the operational phase, we should have both short-term and long-term perspectives for the performance monitoring of SISs.

1. Short-term perspective: Be aware of which item is not functioning or has been impaired (updating failure rates); Based on operational experience with the SIS, system performance that incorporates the new information should be updated periodically. The updated system performance helps practitioners to understand SIS status well consequently, provides clues for further planning maintenance actions.
2. Long-term perspective: Verify the performance requirements and update test intervals; Having collected the latest system performance information and updated system status, an interesting extension is to consider the length of the test interval. The core of updating test intervals strictly depends on the estimated performance by taking credit for collected information. Specifically, it depends on the updated $\mathrm{PFD}_{\mathrm{avg}}$ and the required SIL.

2.5 Influence factors of SIS availability

Considering the significant role in the safety of EUC, several industries, therefore, invested efforts in the field of SIS performance assessment, e.g. the nuclear industry and the process industry. The nuclear industry has pioneered in the development of methods for reliability and availability analysis, and the process industry has taken several initiatives to data acquisition [66], and some of these are published in generic data sources, such as Offshore Reliability Data (OREDA) and Process Equipment Reliability data [66]. Several handbooks provide a basis for performance analysis [78]–[81].

The availability and performance of SISs depend on multiple factors, which can be further divided into two categories, uncontrollable and controllable factors, on whether the intervention of humans is effective.

2.5.1 Uncontrollable factors

Uncontrollable factors originate from the working conditions of SISs quantifying as demand rates in performance evaluation. Aside from the real demands on SISs, the process parameters, e.g. temperature, flow, medium, etc, would leave side-effects on the subsystems of SISs in varying degrees, which result in degradation phenomena in SISs.

1. ***Demands***: The intention of an SIS is to be activated as a response when demand occurs. It means that how often an SIS is demanded varies from system to system. The main discussion related to demands locates on the effect of system and demand rates.

   Bukowski [82] proposes a model to incorporate process demand into the Markov model to assess system performance by calculating the state probability PDPRS, which stands for the process require shutdown (PRS) while the system is in a failure dangerous (FD) state, with the conclusion questioning the insufficiency of arbitrary division between high-and low-demand. Taking the advantage of the Markov model, Jin, Lundteigen and Rausand [83] quantify SIS reliability for both low-and high-demand operation; Liu and Rausand [64] explore the relationship between SIS reliability and demand rates and conclude that there is a rather long interval where the demand rate is neither high-demand nor low-demand. A further study is conducted to explore the relationship between common cause failures (CCFs) and SIS reliability and safety performance with the incorporation of both the demand rate and demand duration [84].

   Meanwhile, the occurrences of real demands are the windows of opportunity to check the system state. Hokstad [85] states that an actual demand (e.g. a gas leak) also can reveal the state of some units, consequently, proposes new approximations for $\mathrm{PFD}_{\mathrm{avg}}$ and hazard rate of an SIS with the assumption that demands serve as a functional test. Jin [86] argues the existence of differences between tests and demands in several aspects, such as, a test is pre-scheduled, while a demand occurs randomly; a test is a proactive approach, while demand may cause a failure, and so on.

2. ***Degradation***: The degradation in SIS here emphasizes that the mechanical items can become vulnerable with time, which contributes to deteriorating performance.

   A commonly accepted assumption in most existing studies is that the performance of SISs is independent with time. This assumption implies that the SISs do not show any deterioration and that they are as-good-as-new as long as functioning, which is inadequate for mechanical items. For such cases, researchers have identified that the failure rates of these items are non-constant, and they have chosen the Weibull distribution in reflecting the failure process [65], [87], [88]. Meanwhile, several dynamic reliability methods, e.g. multiphase Markov process, stochastic process, have been applied to SISs for reliability assessment. Srivastav, Barros and Lundteigen [61] consider the side-effect of proof tests on SIS performance by adding discrete degraded states with increasing transition rates, to optimize the periodic inspection time [89]. Zhang, Zhang, Barros *et al.* [26] propose a stochastic model to describe the degradation process and seek the optimal maintenance strategies with modeling the degradation of SIS final element as a stochastic process. Further, the same authors consider the effect of demand on degradation in performance analysis in redundant structure and propose an algorithm to calculate condition $\mathrm{PFD}_{\mathrm{avg}}$ based on the collected information in the prior test [24]. Several studies are conducted in the nuclear sector to quantify the degradation of safety components with undergoing tests and demands [90], [91].

2.5.2 Controllable factors

Compared to uncontrollable factors, control factors exist in both the design and operational phases throughout the life cycle of SISs. Redundancy structures are allocated in the design phase to improve system reliability, while more activities in the operational phase are recommended to maintain integrity and monitor performance, e.g. testing and maintenance. A detailed literature review is conducted here for selected controllable parameters.

1. ***Structure***: A reliable structure of an SIS can reduce the risk of EUC. Redundancy is a common approach to improve structural reliability by providing the opportunity for the system to be functional by using the other item if one item fails. Redundant structure brings new challenges as well, e.g. CCFs, cost, etc.

   Several studies have been made on deriving PFD formulas for $K\text{oo}N$ configuration [8], [92]–[95]. Torres-Echeverría, Martorell and Thompson [96] introduce a new development for modeling the time-dependent PFD of redundancy structures to evaluate the effects of different testing frequencies and strategies (i.e. simultaneous, sequential, and staggered testing). The same authors extend the research to study PFD and spurious trip rate of SISs including voting redundancies in their architecture [97]. Furtherly, the optimization of design and test policies of $K\text{oo}N$ voting redundancies in SISs are presented with a multi-objective genetic algorithm, which includes PFD_{avg}, spurious trip rate and life cycle cost [98]. A new generalization for PFD_{avg} of $K\text{oo}N$ architecture is proposed in [99] with taking into account the contributions of partial stroke testing (PST) and CCFs. Courtois and Delsarte [100] propose an optimal algorithm to optimize the periodic preventive interval by balancing the loss of redundancy during inspections against the reliability benefits of more frequent in inspections. A study about seeking optimal time interval for redundant systems with maximize availability and minimize costs is proposed in [101].

   The attention of the heterogeneity of items in redundant structure rises in recent years. Systems with non-identical items in different failure rates are studied using Markov models [102], showing the close relationship between the diversity of the items and the system PFD_{avg}. To study the general redundancy mechanisms, copula functions are adapted to represent the system structure with dependent items and consequent to determine the minimal repair procedures [103].

2. ***Testing and maintenance***: Testing and maintenance are key activities to ensure that an SIS achieves and maintains the required performance. Tests address the execution of a function of SIS to confirm consistency with the requirements, and maintenance intends to keep the system in a state to perform the required function. Several factors are addresses here, including imperfect testing, PST, tests with constraints, and maintenance.

   As mentioned in Section 2.4, the proof tests in practice are however difficult to comply with the perfect testing assumption in the operational phase. It implies that the system unavailability does not equal zero necessarily even after the proof testing.

The final element may be not as-good-as-new even though it is qualified as functioning in a proof test. A common approach to model imperfect testing is to split the failure rate into revealed and non-revealed by proof test [8].

A detailed study of imperfect testing, including causes and impact, on PFD is conducted in [104], the causes of imperfectness are summarized in five M-factors: method, machine, manpower, milieu, and material. A Markov model with four states, including as-new, intermediate, dangerous, and fault, is proposed to quantify the imperfect proof test [105]. A holistic approach based on Switching Markov chains is proposed to model $\mathrm{PFD}_{\mathrm{avg}}$ with the integration of several parameters including imperfect test rate, test interval and the probability of failure due to test and so on [106].

Partial proof-testing is recommended as a supplementary between full proof tests in revealing one or more specific types of DU faults of a channel without significantly disturbing the EUC. Categorization of imperfect tests are outlined in [107], meanwhile, a simple and analytical model utilizing partial tests and mean partial test time (MPTT) is suggested to reduce the unclarity of estimate for $\mathrm{PFD}_{\mathrm{avg}}$. Lundteigen and Rausand [108] consider the pros and cons of PST of process shutdown valves and suggested a new procedure for how to determine the PST coverage factor. Brissaud, Barros and Bérenguer [109], [110] propose analytical formulas to assess the availability of redundancy architecture systems subject to the partial and full test. Jin and Rausand [57] develop simplified formulas in the $\mathrm{PFD}_{\mathrm{avg}}$ calculation taking both partial and proof testing into consideration, CCFs modeled by β-factor model as well. A generalized $\mathrm{PFD}_{\mathrm{avg}}$ formulas for SIS is proposed based on multi-phase Markov process including full and partial periodic tests and accounting for the different repair times as well [111]. Wu, Zhang, Barros *et al.* [112] propose a state-based approach for unavailability analysis of blind shear ram preventer during proof and partial testing phase.

Although periodic tests can detect some hidden problems, they can also increase costs and can heighten risks during their execution. Rouvroye and Wiegerinck [113] evaluate the impact of different testing strategies of a redundant configuration on $\mathrm{PFD}_{\mathrm{avg}}$. There are also several conducted studies for determining the optimal testing interval with considering constraints, e.g. cost and risk. A model using fault trees and a genetic algorithm is proposed to maximize the benefits and minimize costs related to guaranteeing the integrity of SISs [114]. When considering maintenance human error and public risk perception of the nuclear power plant, an optimization algorithm for periodic testing intervals by balancing risk and cost of tests is proposed [115].

In terms of maintenance of SISs, several studies are conducted on the optimization of the maintenance schedule of SIS. In [60], an optimal control methodology is employed to find the optimal time instants for maintenance tests regarding an SIS with preventive maintenance tests as a switched linear system with state jumps. Redutskiy [116] proposes a model to reflect the divergent perspectives of the main parties involved in oil and gas projects to account for device failures, technological incidents, continuous restorations, and periodic maintenance for a given process and safety system configuration using a Markov model.

Therefore, the aforementioned main influence factors of system availability in the operational phase can be concluded and depicted as in Figure 2.10.

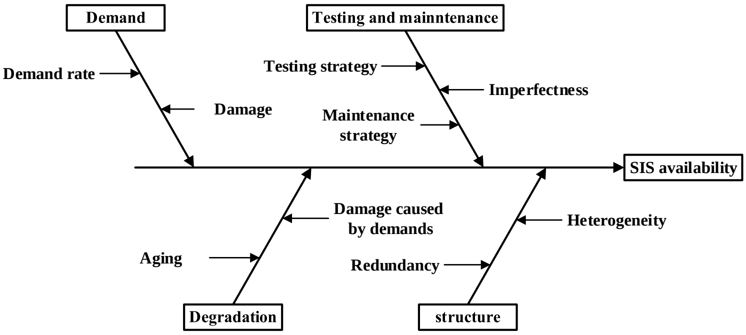


Figure 2.10: Influence factors of system availability in the operational phase

Given the insufficiency of failure rate-based in modeling degrading performance, the time-based testing and maintenance methods seek a shift to incorporate these factors in the operational phase. Integration of technology and visibility of system status information during the operational phase will be the future that SISs are managed and maintained.

2.6 Prognostics and health management on SISs

2.6.1 Maintenance transformation

The maintenance strategy has been transforming along with technology to feed the needs of industrial systems in the last decades. It ranges from reactive maintenance (run-to-failure), preventive maintenance, condition-based maintenance (CBM) to prognostics and health management (PHM).

Acronym PHM consists of two elements [117]–[119]:

- Prognostics refers to a prediction/ forecasting/ extrapolation process by modeling fault progression, based on current state assessment and future operating conditions;
- Health management refers to a decision making capability to intelligently perform maintenance and logistics activities on the basis of diagnostics/ prognostics information.

PHM is a framework of methodologies that permit the reliability of a system to be evaluated in its actual life cycle conditions, to determine the advent of failure, and mitigate the system risks [120]. There are three main issues to be considered: current state estimation, future state along with to fail time prediction and impact determination of a failure on system performance [121].

CBM and PHM, widely used in critical industries which require high-reliability level, are potential as the future of SIS health management. The differences between CBM and PHM mainly locate on that the former is diagnostic in nature with the purpose of identifying appropriate maintenance actions to detect a fault condition before it turns into a failure, and the latter is predictive in nature aiming to determine how long from now will a fault happen in a system given the current operating conditions [23], [122], [123]. The relative placement of detection, diagnostic and prognostic can be explained in Figure 2.11.

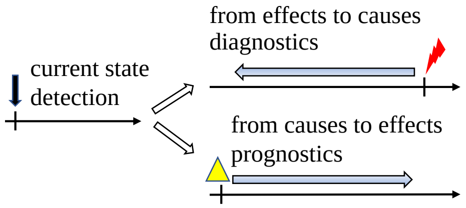
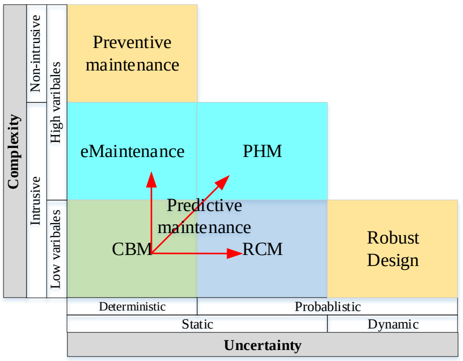


Figure 2.11: Complementarity of detection, diagnostic and prognostic activities

A systematic maintenance transformation map is depicted in [123] considering diverse maintenance strategies from the dimensions of system complexity and uncertainty, as shown in Figure 2.12. CBM can be applied in systems that are deterministic or static to some extent with extracted health indicators. PHM is more flexible in probabilistic and high variables than CBM, still, the input for the prognostics and decision-making model in PHM may come from CBM techniques.



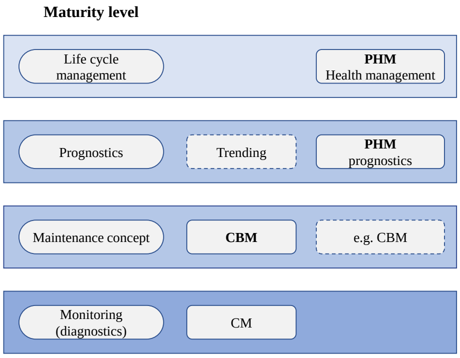


Figure 2.12: Maintenance transformation map

Figure 2.13: relation between CBM and PHM

From the maturity level, PHM is acting on a somewhat higher level than CBM including a prognostic capability aiming to provide guidelines for managing the health of the system, as described in Figure 2.13. PHM, as a philosophy to perform life cycle management, has a strong ambition on the predictability (i.e. prognostics) of failures and maintenance, while CBM is mainly diagnostic [125].

2.6.2 PHM procedure

Data acquisition, data preprocessing, prognostics, and maintenance decision-making are the four key elements of a PHM flowchart [126], as shown in Figure 2.14, which means a complete process from capturing the data to decision-making.

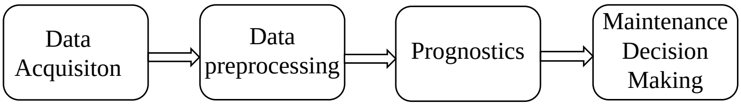


Figure 2.14: Four elements in a PHM flowchart

The main aspects of each step are discussed as follows:

Data acquisition is the process of collecting and storing useful data from the targeted component/ system for further diagnostics and prognostics. The data collected for PHM can be categorized into two types: 1) event data and 2) sensory data [118], [121], [127].

1. Event data: include the information what happened (e.g. failure, breakdown, installation, overall, etc.) and/ or what was taken by the maintenance technician on events (e.g. preventive maintenance, repairs, oil change, etc.) with respect to the targeted component/system.

2. Sensory data: also remarked as condition monitoring data. Sensory data are the measurements related to the health condition/ state of the system via installed sensors. Versatile data could be collected upon the system, e.g. vibration data, acoustic data, temperature, pressure even environment data, etc.

Data preprocessing normally involves cleaning and analysis of redundant and noisy raw data acquired from the system. This phase can be described as a process to extract/ select features from raw data that indicate the failure progression of the monitored system. The effectiveness of a prognostics model is highly related to the quality of features, consequently, impact the accuracy of RUL prediction.

Prognostics is ‘the estimation of time to failure and the probability of one or more existing and future failure mode’ [128]. The most obvious and desirable type of prognostics emphasizes predicting how much time is left before the system loss its particular function given the current condition and past operation profile. An alternate goal of prognostics, which attracts less attention, is to predict the chance that a system operates without a fault or a failure up to some failure time given the current condition, especially for systems with catastrophic failures, e.g. unclear power and fighter aircraft in combat [127], [129].

From these descriptions, it is obvious that prognostics is directly linked with a certain function of the system. It implies that prognostics should be based on evaluation criteria both from the monitored system and performance targets.

Decision making aims to provide support for maintenance technicians to take logical and/ or right maintenance actions among several alternatives. Maintenance technicians should be able to estimate the outcomes of each alternative including both negatives and positives. The main objective of prognostics incorporating decision-making is to optimize the maintenance policies when several aspects are involved such as risk, cost, reliability, and availability.

2.6.3 Potential benefits of PHM on SISs

As mentioned in Section 2.5, there are multiple factors influencing the system performance. Similar to usual mechanical and electrical systems, SISs are subject to unavoid degradation mechanisms, e.g. gradual erosion and wear, that will gradually lead to degrading performance and ultimately interrupt their predefined operation/ function. Meanwhile, the deterioration procedure varies and is subject to harsh operating conditions such as load, environment, etc [130], [131]. Degrading subsystems in SISs only offer a reduced risk reduction benefit and hence the risk level of a EUC can be no longer at expected baseline levels. Conventionally, reliability analysis relying on exponential lifetime distribution only provides an overall reliability estimate that takes the same value of $\mathrm{PFD}_{\mathrm{avg}}$ for the entire population in the whole life cycle. The applicability of failure-rate based methods is in question when quantifying the degrading performance.

The activities on SIS can have far-reaching consequences for both itself and EUC, implementing too often can mean a waste of resources and unnecessary economic loss induced by interruption of EUC, and implementing too seldom can cause catastrophic failure when the undesired event occurs on EUC with the absence functioning of SIS. Additionally, shutdown and restart of EUC are sometimes hazardous operations with increasing risk [8]. Nowadays, testing and maintenance of SISs are made in a conservation open-loop fashion, referred to as time-based actions, where the actual state of the system does generally not influence these decisions. Maintenance actions are only conducted when a DU fault has already occurred and been revealed in a proof test, which is a reactive process maintenance decision.

With the development of sensor technologies, more data about operation conditions and system status in operation can be collected. Numerous parameters such as lubricant ingredients, vibration signal, thermography picture, corrosion extent and so on can be measured, analyzed and compared to conduct failure prediction and diagnosis [13]. These advancements provide an opportunity to prevent downtime as well as the corresponding expense from happening. It means that there is an opportunity to shift maintenance into a proactive way, namely, a transformation on maintenance strategy from the traditional failure-based (diagnostics) to a predict-and-prevent methodology (prognostics) [123]. Prior studies related to choke valve performance assessment based extracted health indicators from the process parameters strength the basis for the performance-based management of SISs [14], [15], [132], [133].

Taking the advantage of PHM procedures to fill up the vacancy of performance-based testing and maintenance approach, there are main functions and potential benefits, such as [23], [134]:

1. A more representative picture of SISs current status based on the measured data at the testing time. Prognostics can evaluate the degradation of the SIS, so as to detect incipient deviations. This offers an advance warning of failures for maintenance staff regarding the operational conditions to take actions before a failure occurs.

2. Forward prediction of SIS status to some point in the future which provides clues for effective planning and strategic decision making. Based on the capability of estimation of remaining useful lifetime (RUL), unnecessary activities can be eliminated compared to time-based testing and maintenance policies while keeping the SIS effective.

3. Planning logistic support in advance and cost reduction. Performance-based algorithms can tell practitioners when and how the failures will occur, and make the identification and repair of failed items easier. The available time of SISs will be increased as reduced lead time. Moreover, the 'just-in-time' maintenance based on prognostics will contribute to the decrement of unnecessary costs caused by scheduled testings and interruptions of EUC.

To conclude, the implementation of PHM on SISs not only benefits asset owners and operators economically but also improves system performance. Therefore, from both economics and safety perspectives, improving the efficiency of testing and maintenance is instrumental for SISs management in the future.

2.6.4 Key issues and challenges

The main purpose of SISs management in the operational phase is coordinating activities to establish and maintain safety functions. The ultimate target for upgrading SIS management is how to reduce unnecessary interruption of EUC and managing risks while maintaining the safety functions meeting required SIL.

Therefore, the main issues originated from this target can broadly be summarized into two categories 'Is the SIS (still) sufficient to implement the predefined functions based on the collect information?', 'How should activities be scheduled and coordinated to ensure that the SIS remains at the required integrity level?'. The former depends on the diagnosis of the current health condition of SISs from the prior tests, while the latter focus on the consequences of various decision options.

From the detailed discussion of operational activities in Section 2.5, several influencing factors of SIS performance are in priority to be addressed, such as structures, demands and degradation and so on. It is acknowledged that the SISs interact directly with the process, especially the final element subsystems. These items, therefore, are rather vulnerable to creeping degradation processes resulting from possible factors, e.g. the force and motion, the fluid composition in the EUC, etc. A related question arises and yet be solved: is it possible to find a quantitative way to model the degrading performance based on the information from periodical tests? Different from a continuous working system, a low-demand SIS will change from a dormant state to an active state in case a demand occurs. This state shift also means that the working condition of SISs jumps to a harsher condition which rapidly increases the stress for the mechanical items in SISs. It implies that if the item keeps a continuous degradation process in the dormant state, then an abrupt increment could be added on thanks to the demand. Meanwhile, subsystem in the SIS is normally allocated with redundant structures. Following the non-negligible assumption of demands, the further consideration is about how to study and allocate prior demands for the redundant structure in terms of exerted history, should be distributed equally for all items or only exerted on activated ones? In terms of the performance assessment for SIS, $\mathrm{PFD}_{\mathrm{avg}}$ has been a well-known measure even in international standards. To evaluate the effectiveness of a PHM program, a question seeks the solution: how to utilize this measure and build a relation with degrading performance.

According to the aforesaid discussions, key issues and challenges for PHM-driven SIS management can be summarized, but are not limited to, including:

1. Lack of models to quantify clearly reflecting the degrading performance;
2. Absence of algorithms to incorporate redundancy structures in system degrading performance modeling and analysis;
3. Separation between the degrading performance and the performance measures for SISs;
4. Incapacity of regulation on testing and maintenance schedule based on the analysis of system condition information collected in prior proof tests.

2.7 Scope and limitation

The motivation of this thesis is to explore the applicability of PHM to SISs. The main discussions locate on the performance of final elements which is the main contributor to whole SIS system failure. Other SIS subsystems, including sensors and logic solvers, are important but not explicitly addressed since the exponential lifetime distribution is reasonable and adequate in performance assessment; This PhD thesis is centered on developing decision-making of SISs for better performance both on safety and economic aspects.

The discussions and proposed models in this thesis are mainly focused on how to quantify the degradation in SISs and provide clues for decision-making for testing and maintenance. In terms of PHM procedure as discussed in Section 2.6, the data acquisition and data preprocessing are skipped in this thesis. Meanwhile, the results based on proposed modeling and methods have not been extended/ validated with realistic issues of multiple SISs in the context of risk-based EUC.

To address the identified issues and challenges, the following assumptions have been made for further study.

1. The operation records contain all relevant information reflecting degradation performance about SIS, including sensory information and event data;
2. It is assumed that the health indicator is extracted to represent the system conditions in operation;
3. The health indicator is detected perfectly and consequently the system degradation level is known during tests;
4. The failure mechanisms under investigation is dominant that limits the functional capability of the system.

Chapter 3

Research questions and objectives

3.1 Research questions

The background research in Chapter 2 reveals that even though SIS performance assessment has received increasing interest in recent years, the focus is mainly on failure rate-based methods and open-loop fashion testing and maintenance, referred to as time-based actions. The main objective of this PhD thesis is to explore the way to shift SIS management from time-based testing and maintenance to PHM-driven methods with the advancement of technology in collecting information in tests.

The primary research question generated from this objective is: how can we build effective models that are capable of predicting the evolution of degrading features under anticipated operations to play a basis for decision-making?

The development and deployment of PHM solution for SISs necessitate a good knowledge of existing techniques in characteristics of SISs. To achieve the tailor-made PHM on SIS, based on a thorough literature survey, the specific research challenges are identified and thus sub-questions are raised.

3.1.1 Degrading performance

Prognosis of future fault progressions, as published in standard ISO 13381-1 [128], requires foreknowledge of the physical underlying the failure modes as well as the relationships with future operating conditions. The primary aim of data acquisition and data preprocessing is to provide a model based on the extracted health indicator to describe whether and how much the health of the monitored SIS has degraded. The model receives data from different condition monitoring or from prior proof tests to analyze the degradation mechanisms that will affect the system performance by taking into account the material properties, the boundary conditions, and the operating and environmental conditions [135]. Therefore, good knowledge of degrading performance and mechanisms is fundamental for establishing a reliable model.

The main uncontrollable factors that influence SIS performance in the operational phase originate from the working conditions. For low-demand SISs, the main reasons for degrading performance can be summarized as natural aging and the impact of demands.

Natural aging

As stated in Section 2.5, the SIS interacts directly with the process, especially the mechanical final element subsystem. For instance, like actuated valves involving electro-mechanical and/ or hydraulic-mechanical components working in a subsea environment, they are exposed to harsh working conditions and direct interactions with the process in EUC. This interaction with process/ environment could lead to a loss of material and/or desirable properties of the mechanical material, consequently, the valve may operate less efficiently [130]. These harsh conditions sustained over years of continuous operation can result in age deterioration of the mechanical components, such as corrosion, wear, fatigue, fouling, etc [136]–[138].

The typical failure mode of valves is the LCP which is likely caused by the erosion in the gate sealing area. The progressive erosion is unable to be revealed by visual inspection until reaching a predefined level. When erosion reaches the predefined level, the state of the valve is judged as failed which will be hidden until manifested in the next proof test since the actual performance is out of the accepted performance criteria.

Therefore, there is a need for a quantified approach based on health indicators to model the aging degradation process of the system.

Impact of demands

Another notable factor leading to degrading performance is the demands which contribute to the SIS activation. From this point, demands on SISs can come from the scheduled proof tests and random external hazardous events. Several researchers addressed the negative impact of proof tests with introducing extra stress on the tested system [61], [66]. However, random demands are more worthy of study in terms of system performance assessment in many aspects. Proof tests are performed by simulating real demand situation to test system performance, however, the system is normally in a more severe stress situation in demands than tests with certain demand duration. The system shifts from dormant to the active state as demand occurs which abruptly harshen the stress. Potentially, the state shift could speedup the existing degradation process in the system. Also, a demand comes randomly, whereas a test is pre-scheduled. It is reasonable to understand that system capability is becoming vulnerable to upcoming demands after activation response to the suffered ones. Therefore, it needs to be considered that how much the impact of past demands on degrading performance in SISs.

The relevant research questions related to degrading performance can be concluded as:

Q1 : How to model the SIS performance with a predefined failure level subject to the continuous aging process?

Q2 : How to utilize the collect information to bridge SIS degrading performance with performance indicator $\mathrm{PFD}_{\mathrm{avg}}$?

Q3 : How to incorporate the suffered demands in the past into system performance evaluation?

3.1.2 Structure

Redundant structures are often used in SISs to improve system availability and so to enhance safety. In the current studies, items in a redundant structure of an SIS subsystem are always assumed identical in terms of failures. It is fine to use the same aging degradation models thanks to the heterogeneous properties, yet differences should also be considered.

The theoretical design of the redundant structure is to take advantage of fault tolerance from two or more items, namely if one item fails, the system can still continue to function by using the other item(s). Consequently, a problem rises along with this non-negligible damage assumption of random demands: how to quantify the effect of random demands on each item from records of operational history, especially the executed demands?

The first place of this consideration is that since SIS availability in particular if errors are inevitable, they should be on the conservative side with respect to safety. From this aspect, it is absolutely reasonable to assume that all items in the final element subsystem would suffer from the same demands in terms of amount and magnitude of damage.

On the other side, the redundant structure is designed for fault tolerance. Considering a 1oo2 structure, the response of any of them to demand is enough to protect the EUC. Following the nonnegligible damage of demand on an item, a question is generated: which of the two items should be activated. For one certain item, the more demands it suffered, the more fragile it is for upcoming ones. How to reach the optimal system performance by controlling the activation strategies of redundant structure?

This poses the research questions:

Q4 : How to quantify the effect of suffered demands on different items in redundant structure in system performance assessment?

Q5 : How to control the activation strategies of redundant items to reach the optimal system performance?

3.1.3 Evaluation criteria

With the capability of performance prediction, when any deviation from the normal, or early-phase signal of failure is identified, the upcoming tests and following maintenance actions need to be re-scheduled. Actually, the decision-making for re-scheduling is a two-fold consideration from safety and economic perspectives:

The first principle is to meet the required performance, as SISs are designed and installed to protect the EUC. The test interval is the main contributor to system performance. The more proof tests conducted, the more information on the system could be collected. Consequently, the EUC is facing with lower risk since the SIS is reliable with a lower $\mathrm{PFD}_{\mathrm{avg}}$. The result is also capable of redundant structures with several testing strategies including simultaneous, staggered, and sequential testing. Accompanying with the recognizable degradation level of the system, different follow-up options after a proof test are possible:

(1) no action if the system in the test is working well; (2) PM if a certain degradation has been identified; and (3) CM if it is failed. Compared to as-good-as-new after CM, PM aims to mitigate degradation level and consequently reduce failure probability in the next test interval. Then, the challenge of when and how to conduct PM actions also needs to be addressed.

The second challenge introducing by the three states of the system is about the revealing of the system state from the collected information. The assumption of perfect revealing state, especially for the degraded state, is not always applicable for SISs since the degradation level is determined by the difference between a reference value and an estimated value of the state rather than observed directly, while the estimated value is calculated from some relevant process parameters [14], [15]. When the collected data in a proof test is imprecise or different from working conditions, these inaccurate measurements will be passed into the physical condition estimation for valves. These unintended errors can be amplified or diminished in the calculation of the actual status of valves, consequently, affecting the follow-up activities.

Even more frequent proof tests are regarded to lower risks, but some practical issues can waken such a conclusion and lead to different decision-making. If a proof test of SISs fully stop the process in EUC, or complete a whole trip of shutdown, stoppage and restart of the process will cause production loss, especially in offshore engineering and facilities [47]. In addition, such a whole shutdown trip may also damage the SIS to some degree due to high stress level [65], [108]. The consideration from economic aspects limits the frequency of proof tests.

Hence, it is reasonable to consider how to utilize given proof test information to schedule future tests more effectively (e.g. to avoid unnecessary tests), while keeping the SIS availability meeting at the required level.

Potential research questions can be summarized as:

Q6 : When are the PM and CM actions needed and what is the optimal degree of PM that can balance maintenance cost and system availability?

Q7 : How can we deal with the imprecise testing information in testing for performance assessment?

Q8 : How can we incorporate the testing strategy and induced intervention costs of the system in the decision-making regarding the rescheduling of tests?

3.2 Research objectives

The primary objective of this PhD thesis is to explore new methods of performance assessment and decision-making, as the basis to shift the time-based testing and maintenance strategies in SIS operations to PHM. The knowledge generated in the PhD project should give rise to more rational decision-making related to SIS performance in the operational phase, hence contribute to the overall strategy for major risk prevention, which is in the main phase 3 and 4 in Figure 2.14.

To avoid being too general or losing focus in the context of SIS performance assessment, more specific objectives are defined based on these proposed research questions. They are presented in two categories:

3.2.1 Modeling approach

Driven by the summarized research questions in Section 3.1.1 and 3.1.2, the objectives in modeling approach aims at proposing:

- Objective 1: Evaluation models of continuous aging on time-dependent SISs degrading performance
- Objective 2: Models of hybrid effects of continuous aging and random demands on SIS deterioration
- Objective 3: New assessment method considering the effectiveness of collected information in tests

3.2.2 Approach for decision-making

Guided by the research questions related to Section 3.1.3, the objectives here is decomposed into the following objectives to develop:

- Objective 4: New decision-making method for scheduling SIS tests based on collected information in tests
- Objective 5: New method for balancing SIS performance and economic targets in operational decision-making

Chapter 4

Research methodology and approach

A Doctor of Philosophy is the highest university degree that is conferred after producing original research that expands the boundaries of knowledge. The process of pursuing a PhD degree provides an opportunity for systematic training in research skills, from proposing a research proposal, planning and executing a research plan, writing academic articles and presenting ideas and results, etc.

This chapter documents the entire research during the PhD study period the involvement of formulation research problems and objectives, and the presentation of research results, along with detailing out how research outcome is obtained to feed these proposed research objectives in this PhD.

4.1 Classification of research

Research comes in many shapes and sizes. A straightforward understanding of 'research' is a logical and systematic search for new and useful information on a particular topic. Research can be defined as 'an activity that involves finding out, in a more or less systematic way, things you did not know' [139]. Here are several accepted principles for research classification.

The research is broadly classified into fundamental or basic research and applied research. The former emphasizes the investigation of basic principles and reasons for the occurrence of a particular event or process or phenomenon, while the latter focuses on solving certain problems employing well-known and accepted theories and principles. This PhD project aims to develop suitable models and methods in PHM (which belong to accepted theories and principles) to adapt to SISs (which are recognized as certain problems). It falls into the category of applied research.

Phillips and Pugh [140] point out that the distinction between functional or basic research and applied research is too rigid to characterize what happens in most 'real-world' research. A threefold research classification from the perspective objectives is recommended as exploratory, testing-out, and problem-solving. Details of each classification are defined as following: 1) exploratory research is involved in tackling a new problem/ issue/ topic with little known, which contributes to a poorly formulated research idea at the beginning; 2) Testing-out research is targeting to find the limits of previously proposed generalizations; 3) Problem-solving research starts from a particular problem in the real world and brings together all the intellectual resources that can be brought to bear on its solution. The basic elements include the definition of the problem and the discovery of the solution method. In terms of this PhD project, the adjustment of the general PHM procedure (the existing intellectual resources) to meet the requirement of SISs (the particular problem in the real world) belongs to the scope of problem-solving research.

In terms of research methods, functional or basic research and applied research can be further inducted as quantitative, qualitative, and mixed-methods research, which is over-simplistically distinguished for easy understanding by whether they focus on numbers, words, or both. When it comes to this PhD project, the detailed research objective is to study the dynamic SIS reliability based on probability theory with the involvement of operation history and physical states. Therefore, quantitative methods are adopted here.

A summary of the research types of this PhD project is given in Figure 4.1.

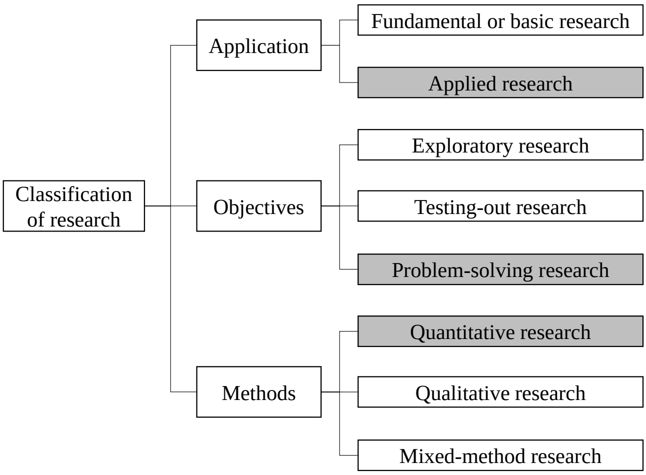


Figure 4.1: Research types of this PhD project

4.2 Research methodology

'Methodology is the philosophical framework within which the research is conducted or the foundation upon which the research is based' [141]. It means that research methodology is about how the researcher systematically identifies, selects, processes, and analyses a certain topic to ensure valid and reliable results that address the research aims and objectives.

There are five typical and major steps in the most research process as follows:

1. *State of Research problem.* A clear definition and statement of the research problem well put is half solved. The formulation of a research problem usually requires

a two-step procedure from an overview of the problem and narrowing it down to specific aspects of the problem. The primary problem of this project is to modify acknowledged SISs reliability analysis to match with PHM procedures. The narrowed process has been discussed in Chapter 3.

2. *Survey of Related literature.* The explosion of published sources benefits researchers in the investigation and outline of what has been done in certain topics. Followed with a shortcoming, few hundreds of citations and sorting with limited relevance appear evidently when the search keyword is abroad and general, e.g. safety barriers and SISs. So that, featured keywords are of importance in collecting literature. The next step of the literature review is to organize and evaluate efficiently these identified important previous studies and to shed light on proposed topics. The survey of literature review in this PhD project starts with the two main keywords: PHM and safety barriers. The former focuses on the methodology and procedures and the latter on the classification and performance analysis.

3. *Theoretical model: Formulation of hypothesis.* After the previous processes, several research problems with the ascertained investigation on prior study need to be conceptualized. The conceptualized objectives have been listed in Chapter 3. For the sake of easily conducting studies, fine-tuning was taken to operationalize the concept in measurable terms, e.g. complex configuration to $K\text{oo}N$, random demands to Poisson process, etc. The primary hypothesis is the applicability of degradation modeling in SISs performance analysis.

4. *Testing of hypothesis.* The fine-tuning of variables provide the chance to test and validate the proposed hypothesis. The existing reliability assessment and examples for SISs played a role in the verification of new methods. The validation is achieved by conducting case studies in each outcome. It is worth admitting that the errors between existing studies and proposed methods have not been quantified since each paper has been conducted on proposed assumptions.

5. *Write-up Research report.* The final step is to explore the strengths and limitations of the new methods, document them in scientific articles, and seek the potential for improvement; first by individual and group-level discussion, and then by exposure to peer review and critique in the scientific community.

4.3 Overall process of work

The primary topic of this PhD project is to employ PHM on SISs to offset several existing limitations in time-based SIS management. Generally, the PhD process can be summarized as four stages with their respective research approaches, as shown in Figure 4.2:

Stage 1: Courses The project started with fundamental PhD courses related to the reliability of safety-critical systems and maintenance optimization. Acknowledged reliability assessment methods and maintenance algorithms provide a solid foundation for further study. In this stage, collaboration such as seminars, academic discussions among PhD candidates in the RAMS group, played an unignored role in generating research ideas.

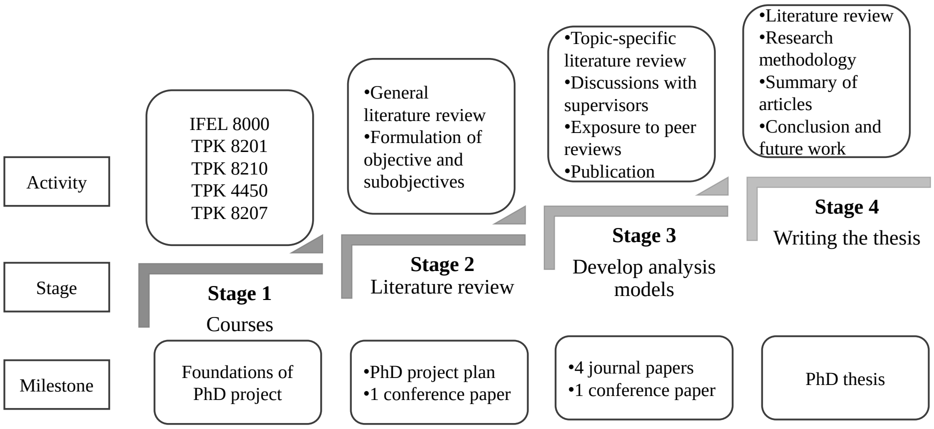


Figure 4.2: Overall process of this PhD project

Stage 2: Literature review Understanding this research topic comprehensively, however, requires substantial knowledge of both PHM procedures and SISs performance analysis. In implementing the literature review, a co-review with PHM and SISs has been conducted to extract opportunities and challenges. Unique characteristics of SISs, which contribute to the main challenges of application PHM, have been drafted as four research objectives in this PhD project as a conclusion. The literature review has been published as a conference paper [23], see the attached paper ESREL2018 in Part II. In addition, a deeper review of each certain characteristic of SISs has been supplemented in Chapter 2 leading to the aforementioned research questions and objectives in detail.

Stage 3: Development of analysis model Following the summarized research objectives, a basic direction is to model and quantify the degrading performance of SISs both in unit-and system-level with taking complex configuration into consideration. In terms of degradation mechanisms, the commonality of mechanical units has been addressed in the first place, as typical corrosion, erosion, etc.

For SISs, degradation occurs on a certain mechanical component with contributing to a time-dependent system performance externally. The chosen of homogeneous Gamma process is based on the widely demonstrated match on similar degradation mechanisms. Meanwhile, the discrete state methods generalized system performance into the finite state, which makes the application and understanding easier for practitioners in system reliability. These methods feed into research questions provide the basis for the development of research articles. Selected article articles have been enclosed in Part II. These research articles are developed following the outlined research objectives and questions in Chapter 3. All enclosed articles have been subject to extensive peer-reviews, and have been revised based on the reviewers' comments.

Stage 4: Finalization and writing this thesis The fourth and last stage of the PhD project is to summarize the findings and contributions in terms of a PhD thesis. This is a whole process to reconsider the motivation and background PhD topic, research questions and objectives, and how research results in Part II are related. With the review, either finished or unsolved relevant questions surfaced.

Chapter 5

Main results

5.1 Overview

The main results of this PhD project are documented in the form of six articles, among which, three articles have been published in relevant international journals, one is currently under revision and the other two have been presented in peer-reviewed international conferences and published in the conference proceedings. These articles are written and organized to address the research questions identified in Section 3.1, With the six articles, we aim to achieve the five research objectives stated in Section 3.2.

In this chapter, we summarize the main results and contributions of this PhD thesis with respect to each proposed objective, such that we are able to evaluate how and to what extent the objectives are met. Article I is a brief literature review that plays as a starting point of this PhD project without targeting any specific research objective. The correlations of objectives, research topics, and articles related to this thesis are summarized in Table 5.1. More detailed contributions to each objective are discussed in the following sections. The full versions of articles are included in Part II.

Table 5.1: Summary of contributions, objectives, and articles of this PhD thesis

Objectives	Main topic	Articles
New modeling approach	Evaluation models of continuous aging on time-dependent SISs degrading performance	Article III Article IV
	Models of hybrid effects of continuous aging and random demands on SIS deterioration	Article II Article VI
	New assessment method considering the effectiveness of collected information in tests	Article V
Novel decision-making	New decision-making method for scheduling SIS tests based on collected information in tests	Article II Article IV
	New method for balancing SIS performance and economic targets in operational decision-making	Article IV Article V

5.2 Contributions

5.2.1 Contributions to modeling approach for degradation

Developing suitable degradation models and methods for SIS performance quantification is the first focus of this PhD project, also the prerequisite of further studies. Contributions to the three proposed objectives on this topic are presented in this section.

Objective 1

Evaluation models of continuous aging on time-dependent SISs degrading performance

Article III: A degrading element of safety-instrumented systems with combined maintenance strategy
Article IV: Optimization of maintenances following proof tests for the final element of a safety-instrumented system

The objective is set based on the literature review that system performance is time-independent in most studies which neglecting the increasing vulnerability along with time. Consequently, system $\mathrm{PFD}_{\mathrm{avg}}$ with the foundation of exponential lifetime distribution keeps a constant value in periodic tests. The contributions from this PhD project to Objective 1 are found in Article III [25] and Article IV [26] with different scopes.

1. Article III demonstrates the estimation on unavailable duration in each test interval based on a stochastic model which bridges the time-dependent performance and system $\mathrm{PFD}_{\mathrm{avg}}$. Taking the advantage of describing common degradation phenomena in mechanical systems, e.g. corrosion, cracks, erosion and so on, a gamma process-based degrading mechanism is chosen to describe the time-dependent system performance. The system failure occurs when the degradation level exceeds a predefined threshold. A simulation procedure is proposed to validate the proposed assumptions.
2. Article IV extends the study of Article III with focus on the instantaneous system performance estimation. Article IV provides analytical formulas to calculate system availability with the collected degradation information from prior tests. With the known degradation level, the algorithm for calculating the conditional system $\mathrm{PFD}_{\mathrm{avg}}$ in the upcoming testing interval is proposed.

The relations among degradation process $X(t)$, instantaneous system availability $A(t)$ and $\mathrm{PFD}_{\mathrm{avg}}$ were explored, see Figure 5.1. These two papers quantify system $\mathrm{PFD}_{\mathrm{avg}}$ with the mean proportion of unavailable time in a test interval instead of failure rate.

The following main findings and contributions are as follows:

1. From the performance perspective, the as-good-as-new assumption after each proof

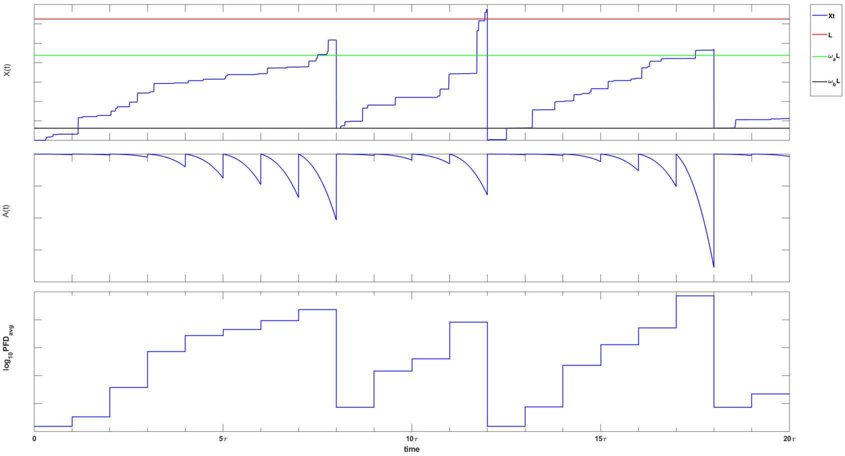


Figure 5.1: A possible degradation path $X(t)$ and the corresponding $A(t)$ and $\mathrm{PFD}_{\mathrm{avg}}$

test is far from practical even though the system is qualified. A stochastic process-based algorithm is developed to evaluate the single-unit instantaneous system degrading performance. The numerical results clearly show that the system $\mathrm{PFD}_{\mathrm{avg}}$ is changing with time, generally, increasing with time.

2. Given that the state of an SIS can be known only at test dates, the system can still experience downtime, which counts from the first arrival time of degradation level exceeding the predefined threshold before the next test, in cases of failures. The expected downtime provides an opportunity to estimate system performance.

3. The information collected in periodic tests demonstrates the system state. The quantified information in prior tests is the basis of calculating conditional $\mathrm{PFD}_{\mathrm{avg}}$ in stochastic process-based models.

These studies indicated the advantage of the stochastic process-based model in presenting time-dependent performance. In terms of stochastic process analysis, different thresholds are assumed to represent the related working conditions and tolerable performance requirements. Naturally, the tolerable performance/capacity of the system degrades with time as well. It means that the threshold should also change along with time, which is the limitation of these two papers. Article IV also discusses the maintenance strategies considering the collected information in proof tests, which in the scope of Objective 5 and will be explained later.

Objective 2

Models of hybrid effects of continuous aging and random demands on SIS deterioration

Article II: Performance analysis of redundant safety-instrumented systems subject to degradation and external demands

Article VI: Optimal activation strategies for heterogeneous channels of safety instrumented systems subject to aging and demands

The objective is set to quantify the demand-induced damage on the system into deterioration performance evaluation. The frequency of demands on SIS is equivalent to the activation history to some extent. The contributions from this PhD project to Objective 2 are founded in Article II [24] and Article VI [28] based on the consideration of random arrival of demands following homogeneous Poisson process with rate λ_{de}, along with Gamma-distributed damage size in the context of redundant configurations.

Each item is possibly subject to two degradation processes: (1) continuous aging process, and (2) random damages induced by demands. A failure occurs in case that the degradation level exceeds a predefined critical threshold.

The differences between the two papers are located in:

1. Article II describes a 1oo2 configuration with the two items suffering the external demands simultaneously with the same damage magnitude. The system will lose the predefined function when both of the items fail.
2. Article VI starts with a 1oo2 configuration following the assumption that external demands only exert on the activated item and negligible on the other to study system performance. Similar studies have been extended to 2oo3 and $K$oo$N$ redundant structures. The aim is to emphasize the random demands on system degradation performance and to seek the optimal activation strategy.

The motivation to quantify the random demands with non-negligible damage is to explore a conservative result given the role of SISs in the risk mitigation of EUC. A comparison study with assumed parameters is conducted in Article II, as Figure 5.2. It is obvious that when only the aging process is considered, the system performance will be overestimated to some extent.

Specifically, the main findings and contributions of Article II are as following:

1. Standing on the specific assumption of two dependent items due to the same demands, analytical formulas of $R(t)$ and $\mathrm{PFD}(t)$ for 1oo2 configuration are developed to take credits for the combined effects of continuous aging degradation and random demands in PFD calculation of a redundant SIS considering stochastic dependence.
2. Sensitivity analyses are conducted to address the effects of failure threshold, demand rate, and shape parameter of demands on $\mathrm{PFD}_{\mathrm{avg}}$. These parameters can be explained as the quantitative indicators to describe the required performance and working conditions.
3. In existing studies, the system is regarded as-good-as-new once working during proof tests. To release this assumption, Article II assumes that the system is working during proof tests without a known degradation level. The numerical example

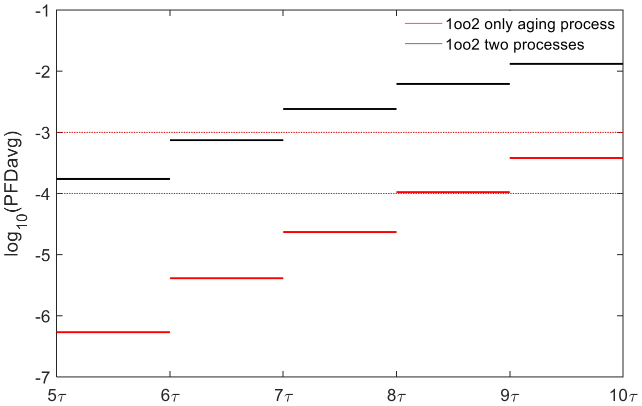


Figure 5.2: $\mathrm{PFD}_{\mathrm{avg}}$ of the 1oo2 configuration subject to aging degradation and random demands

demonstrates the system $\mathrm{PFD}_{\mathrm{avg}}$ increasing along time even though manifested as a working state in proof tests.

The main findings and contributions of Article VI are as following:

1. Analytical formulas of $R(t)$ and mean time to failure (MTTF) for redundant configuration are developed with the allocation of prior demand history exerting on the different items. Generally, MTTF of the 1oo2 system reaches the highest value with activation of the same item for all demands.

2. Opposite to the 1oo2 configuration, the 2oo3 system has the minimum MTTF while the same two items are activated for all demands. Therefore, when the three items are heterogeneous, they should be arranged to withstand the same amount of demands in operation.

3. To describe the ability of an SIS subsystem to continue to perform a required function in presence of hardware faults or errors, hardware fault tolerance (HFT) is suggested in IEC 61508 with $\mathrm{HFT} = N - K$ for $K\mathrm{oo}N$ architecture. it is concluded that if $K \leqslant \mathrm{HFT}$, it is acceptable to continue activating the same item for all demands. If $K > \mathrm{HFT}$, it is quite risky to activate the same items for all demands.

4. This model also develops the basis for adjusting the activation sequences for items to be competent with upcoming demands and meet the required SIL.

The contribution of this PhD thesis treats the operation history of items as quantitative random demands with nonnegligible damages into redundant structure system performance evaluation. More works need to be done to validate the applicability of these proposed models with practical cases.

Objective 3

New assessment method considering the effectiveness of collected information in tests

Article V: Study of testing and maintenance strategies for redundant final elements in SIS with imperfect detection of degraded state

The objective is set to divide system performance into finite states upon information collected in proof tests, e.g. working, degraded, and failed in article Article IV [26] and Article V [27]. In Article IV, system states are assumed to be perfectly revealed in tests. Actually, the actual system states are possibly distinguished as imperfect given some unintended errors in practice. The imperfect detection of the intermediate state which consequently weakens the real performance of follow-up actions is also worthy of a discussion on system performance evaluation. To release the perfect state revealing assumption, Article V introduces a coverage indicator α to quantify the imperfectness and to study the effect of imperfect detection of degraded state on redundant system performance.

The main findings and contributions are as follows:

1. For a single item, the coverage indicator α is introduced and defined as the conditional probability that a degraded state will be detected by the proof test, given that degradation has occurred when initiating the test. The predefined PM actions are available for the revealed degraded state with the unrevealed remaining until the next test. For a 1oo1 configuration, even though PM and CM are conducted on the degraded failed state, respectively, the system $\mathrm{PFD}(t)$ increases in the same test phase with $\alpha \neq 1$.
2. Thanks to the characteristics of the periodic proof test, the multi-phase Markov approach is adopted to conduct the dynamic analysis of the system in each test interval. Aiming at the 1oo2 configuration, two testing strategies, including simultaneous and staggered tests, and three maintenance strategies are proposed to investigate the effect of parameter α on system performance. An indicator k_{ji} is proposed to quantify the differences for $\mathrm{PFD}_{\mathrm{avg}}$ under proposed strategies.
$$k_{ji} = \frac{\mathrm{PFD}_{\mathrm{avg}} \text{ with strategy } j}{\mathrm{PFD}_{\mathrm{avg}} \text{ with strategy } i} \tag{5.1}$$
3. The proposed multi-phase Markov model is able to systematically address practical issues in system performance assessment which can be described in probability language, such as degraded state revealing coverage, maintenance effectiveness and so on.

The state-based reliability methods we adopted in the context of SISs can be regarded as a discretization of the proposed continuous degradation processes in the aforementioned papers. To be specific, state-based methods represents the continuous degrading process based on the judgment of external performance indicator.

Testing strategies and coverage is a conventional and much-studied topic for redundant structure in SISs in the context of failure-rate based reliability assessment. With the contribution of this PhD project, we can easily calculate the system reliability in these complicated situations and quantifiably illustrate the pros of each strategy. There is no denying that the increasing size and complexity of systems quickly invalidate the use of the proposed multi-phase Markov model for stochastic modeling of complex redundant structures.

5.2.2 Contributions to decision-making

From a practical perspective, it can be argued that engineers would like a procedure for reliability assessment to guide the ultimate decision-making [142]. The objective of this part is to explore how to make reasonable decisions under different scenarios of available information and estimated reliability. Contributions to the two objectives on this topic are presented in this section.

Objective 4

New decision-making method for scheduling SIS tests based on collected information in tests

Article II: Performance analysis of redundant safety-instrumented systems subject to degradation and external demands
Article IV: Optimization of maintenances following proof tests for the final element of a safety-instrumented system

The objective is set to schedule upcoming proof tests relied on the proposed system deterioration models incorporating previous performance information. For low-demand SISs, it might not be always worthwhile running proof tests periodically, especially if the shutdown and restart of the process are costly. In this case, the date of the next proof tests can be determined based on the degradation state observed in the current tests. Considering the role of SISs in the risk mitigation of EUC, the specific required SIL is undoubtedly the first priority when it comes to optimizing testing and maintenance strategies. The contributions from this PhD project to this objective are described in Article II and Article IV. Two articles with different scopes aim to achieve this objective:

1. Article IV describes how to arrange/ update testing interval for single-unit final element subject to aging degradation process with the information from tests.

2. Article II focus on a 1oo2 configuration, to explore how to model system degradation with dependent channels and update test intervals within the required SIL.

The main findings and contributions of Article IV are described as following:

1. The single item is subject to a homogeneous gamma degradation process, the initiation and result of PM are predefined. The arrival time of the first reach failure threshold is obtained based on simulation.

2. A simulation procedure is proposed to update test intervals with unknown exact degradation levels in tests. The diverse confidence intervals of simulated degradation levels are assumed as the starting point for the next testing interval.

3. In terms of the known degradation level, the actual testing interval can be inferred based on the conditional $\mathrm{PFD}_{\mathrm{avg}}$ complying to the assumed time-dependent degradation model.

The main findings and contributions of Article II are described as following:

1. An analytical model for conditional $\mathrm{PFD}_{\mathrm{avg}}$ for 1oo2 configuration is proposed. With the known degradation level in tests, the upcoming test interval to keep the system meeting the required SIL can be inferred based on the proposed formulas.

2. Without maintenance actions, the test interval is becoming shorter and shorter as the system degrades. Along with the elapsed time after installation, more tests are expected to keep the required SIL. It demonstrates the insufficiency of the existing as-good-as-new assumption with qualified as working in tests.

The contribution of this PhD thesis is providing a general framework to reckon upcoming testing intervals with the known knowledge of system state from prior tests. These algorithms only act as reference methods for updating test intervals, since several influencing factors in practice are neglected in these studies, such as test quality and partial tests, etc.

Objective 5

New method for balancing SIS performance and economic targets in operational decision-making

Article IV: Optimization of maintenances following proof tests for the final element of a safety-instrumented system
Article V: Study of testing and maintenance strategies for redundant final elements in SIS with imperfect detection of degraded state

Comparing to predefined periodic testing, the performance-based testing scheme is capable of adjusting/scheduling reasonably the testing frequencies upon SISs state, consequently, avoiding unnecessary interventions in EUC (e.g. shutdown and restart). However, everything has its own two sides. Without exception, the performance-based testing scheme on SISs contributing to inconstant $\mathrm{PFD}_{\mathrm{avg}}$ faces the challenge of meeting the required SIL.

Therefore, this objective is set to provide a direction for seeking an optimal testing and maintenance strategy which trades off between the cost and system performance.The contributions from this PhD project to this objective are described in Article IV [26] and Article V [27].

Article IV aims at seeking the optimal initiation and mitigation degree of PM in terms of a single-item system. The main finding and contribution are described as following:

1. A performance-based maintenance framework is proposed to guide the follow-ups with the observation in a proof test, including no action, PM, and CM actions to respond to the different manifested system state.
2. To fit the finite designed service time of SISs, a specialized cost method is proposed. To generalize the proposed cost rate method, cost ratios, instead of absolute costs are assumed and used in optimization analysis with taking the proof test cost as the unit cost.
3. The proposed maintenance framework assumes that PM actions can mitigate but not eliminate degradation. The initiation degree of PM has more influence on the system than the mitigation degree. PM cost is a contributor to the frequency determination of PM in practice.

Meanwhile, Article V discusses system performance with the imperfection of state detection under several strategies, with the following findings and contributions:

1. Similar as Article IV, the life cycle cost of SISs are estimated by the sum of expected cost after each proof test rather than steady-state criteria. The expected cost after each proof test is estimated by incorporating the system state probability and corresponding maintenance actions.
2. Estimation method for cumulative maintenance cost in a finite time regarding imperfect state revealing have been proposed. A quantitative comparison of three maintenance strategies is conducted.
3. The proposed model and algorithm provide clues in the selection of optimal testing and maintenance strategies for the 1oo2 final element.

The contributions of this PhD thesis represents a preliminary study of balancing life cycle cost and performance analysis of SISs. It investigates the effect on system life cycle cost and performance of introducing the PM actions to compensate for the degraded state rather than passive replacement after a system failure. Practitioners can get benefits from degradation modeling and have a better understanding and manage the system performance of SISs in the operational phase.

The preliminary study may not represent accurately the selection procedure for the testing strategy for redundant structure, it has the virtue of allowing practitioners and researchers to obtain an analytical relationship of a certain strategy in safety and economics aspects for the system.

Chapter 6

Conclusion and Future work

6.1 Conclusion

The primary objective of this PhD thesis is to explore new methods of performance assessment and decision-making, as the basis to shift the time-based testing and maintenance strategies in SIS operations to PHM. This objective is decomposed into five sub-objectives that are addressed through the six articles in Part II of the thesis, three among which aim at establishing modeling approaches for time-dependent performance analysis, and three aim at using the proposed modeling approach as a premise to explore the holistic decision-making methods coordinating system performance requirements and economics.

The contributions of individual objectives have been summarized in Chapter 5 aiming at specific research questions. Here, the main contributions are distilled from preceding chapters to emphasize the proposed primary objectives of this PhD project in Section 1.2 as follows:

1. Considering the vital role of SISs in risk control, there is a need to conduct activities to maintain system performance in the operational phase more efficiently aiming at lowering the intervention of the EUC and considering degrading phenomena. PHM procedures, covering data acquisition, data pre-processing, prognostics, and maintenance decision-making, are applicable to evolve time-based to performance-based SIS management in the operational phase. This contribution is a reminder to both researchers and practitioners interested in the integrity of SISs that actual performance information observed during proof tests also serves as an input to system performance estimation and scheduling of maintenance actions.

2. To describe the time-dependent performance of SISs, quantitative degradation models relying on the extracted health indicators are proposed for single-unit and redundant structure systems. Several factors resulting in the degradation performance are addressed in the outcomes of this PhD project, e.g. aging, operational history, complex configuration, and the state revealing coverage so on. This thesis offers SIS analysts with alternative modeling frameworks and procedures, especially in system degradation modeling. It also raises the discussion regarding performance criteria

chosen for SISs in terms of a specific requirement.

3. Based on the proposed degradation models, we develop maintenance models relying on the system state in tests. The contributions of this PhD thesis are thus twofold in terms of the maintenance of SISs. First, a performance-based multiple maintenance response framework is intentionally proposed to evolve the failure-based CM and time-based PM scheme. These proposed frameworks emphasize introducing PM in the SISs maintenance scheme and demonstrating the effect on system performance in a quantitative way. Second, factors involved in the proposed maintenance policy, e.g. initiation of PM, imperfect result of PM, and imperfect state revealing, have been emphasized from the practical perspective, which deserves more attention from practitioners in operational activities of SISs.

4. Decision-making regarding testing and maintenance upon time-dependent performance is a complex and far from easy task. SISs performance and intervention costs intertwine and call for contrary decisions. Algorithms are proposed to calculate the conditional $\mathrm{PFD_{avg}}$ and the responding maintenance cost in the life cycle based on the assumed degradation models, which provide the quantitative references in the decision-making step of PHM. The optimal decision should balance these two aspects that are keeping the SISs performance meet required and minimal intervention cost. The contribution of this PhD thesis is to provide the practitioners with methods in degradation modeling, conditional performance estimation, and life cycle cost estimation.

In conclusion, this PhD thesis contributes to recognizing the effects of aging and demands effects on SISs performance, promoting a more systematic method to estimate the conditional $\mathrm{PFD_{avg}}$ based on the collected information in tests, and a holistic understanding of the pros and cons of updating testing and maintenance strategy from safety and economics aspects for decision-making, further demonstrating the applicability of incorporating a PHM procedure on SISs management in the operational phase.

6.2 Future work

While the application of PHM in the context of SISs is a compound topic with many disciplines and perspectives involved. Even though this thesis presents some new ideas on SISs performance assessment, also arises some new questions that may be for further research on several topics. Among these topics are:

1. The time-dependent performance assessment method for entire SISs, including three subsystems. This thesis agrees implicitly with the exponentially distributed lifetime for sensor- and logic-solver subsystem. While software is subject to deterioration or out of date. This time-dependent performance could lead to serious consequences on SISs itself and EUC simultaneously, for instance, the testing coverage on SISs and the spurious activation on EUC. Even though the unavailability of the final element subsystem is the main contributor of the entire system $\mathrm{PFD_{avg}}$, but a more accurate result would get with three subsystems involved.

2. It has to be admitted that several factors are unresearched or assumed to be negligible, e.g. uncertainty and repair time, which is one of the limitations of this PhD thesis. In terms of the proposed models, uncertainties could come from several aspects that further contribute to the deviation of performance assessment, especially in the prediction process for the upcoming testing intervals. The predicted values rigidly rely on ideal assumptions. A possible solution is to allocate certain parameters with confidence intervals in each step to evaluate the propagation of uncertainties and their effects on prediction results. As for the assumption of negligible repair time, the idea was to simplify the proposed models. In practice, this assumption will contribute to a deviate result, e.g. offshore Blowout preventer (BOP) systems. In this case, there would be a twofold deviation in both system performance assessment and invention cost estimation.

3. As mentioned in the beginning, there are multiple safety barriers to prevent the undesired event in EUC. Therefore, a broad horizon should locate on the system of systems for safety barriers rather than single SIS management. Cascading failures and CCFs would be worthy of addressing. Meanwhile, the focus of maintenance will shift from a single SIS to the entire network of SISs.

Chapter 7

Acronyms and abbreviations

BOP	Blowout preventer
CBM	Condition based maintenance
CCF	common cause failure
CM	Corrective maintenance
DD	dangerous detected
DU	dangerous undetected
E/E/PE	Electrical, Electronic, Programmable Electronic
EUC	Equipment under control
HFT	hardware fault tolerance
HSE	Health, Safety and Environment
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LOPA	Layer of Protection Analysis
MTTF	mean time to failure
$\mathrm{PFD}_{\mathrm{avg}}$	Average Probability of failure on demand
PHM	Prognostics and health management
PM	Preventive maintenance
PST	partial stroke testing
PT	Pressure transmitter
SIF	Safety-instrumented function
SIL	Safety Integrity Level
SIS	Safety-instrumented system

Bibliography

[1] K. L. Tsui, N. Chen, Q. Zhou, Y. Hai and W. Wang, "Prognostics and health management: A review on data driven approaches," *Mathematical Problems in Engineering*, vol. 2015, 2015.

[2] M. Rausand, *Risk assessment: theory, methods, and applications*. John Wiley & Sons, 2013, vol. 115.

[3] ISO 31000, *Risk management—guidelines*, Geneva, Switerzeland: International Standard Organization, 2018.

[4] SN-ISO Guide 73, *Risk management - vocabulary*, International Standard Organization, 2009.

[5] S. Hauge and K. Øien, "Guidance for barrier management in the petroleum industry," SINTEF, Tech. Rep., 2016.

[6] S. Sklet, "Safety barriers: Definition, classification, and performance," *Journal of loss prevention in the process industries*, vol. 19, no. 5, pp. 494–506, 2006.

[7] Y. Liu, "Safety barriers: Research advances and new thoughts on theory, engineering and management," *Journal of Loss Prevention in the Process Industries*, p. 104 260, 2020.

[8] M. Rausand, *Reliability of safety-critical systems: theory and applications*. John Wiley & Sons, 2014.

[9] M. A. Lundteigen, "Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation," Ph.D. dissertation, Norwegian University of Science and Technology, 2009.

[10] NOG-070, "Application of IEC 61508 and IEC 61511 in the norwegian petroleum industry," The Norwegian Oil and Gas Association, Tech. Rep., 2004.

[11] Y. Zhang, "Condition-based maintenance models: Application to subsea safety systems," Ph.D. dissertation, Norwegian University of Science and Technology, 2018.

[12] HSE, "Principles for proof testing ofsafety instrumented systemsin the chemical industry," Health and Safety Executive (HSE), Norwich,UK, Tech. Rep. CRR 428/2002, 2002.

[13] Q. Wang, W. Liu, X. Zhong, J. Yang and Q. Yuan, "Development and application of equipment maintenance and safety integrity management system," *Journal of Loss Prevention in the Process Industries*, vol. 24, no. 4, pp. 321–332, 2011.

[14] B. H. Nystad, G. Gola, J. E. Hulsund and D. Roverso, "Technical condition assessment and remaining useful life estimation of choke valves subject to erosion," in *Annual conference of the prognostics and health management*, 2010, pp. 11–13.

[15] Y. Zhang, A. Barros and A. Rauzy, "Assessment of a condition-based maintenance policy for subsea systems: A preliminary study," in *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016 (Glasgow, Scotland, 25-29 September 2016)*, CRC Press, 2017.

[16] *What is phm?* [EB/OL], `https://carleton.ca/phm/what-is-phm/` Accessed October 21, 2020.

[17] N.-H. Kim, D. An and J.-H. Choi, *Prognostics and health management of engineering systems: An introduction*. springer, 2016.

[18] H. Meng and Y.-F. Li, "A review on prognostics and health management (phm) methods of lithium-ion batteries," *Renewable and Sustainable Energy Reviews*, vol. 116, p. 109 405, 2019.

[19] CALCE, *Phm newsletter*, [EB/OL], `http://https://www.prognostics.umd.edu/PHM_March_Newsletter_Final.pdf` Accessed October 21, 2020, Mar. 2012.

[20] G. Haddad, P. A. Sandborn and M. G. Pecht, "An options approach for decision support of systems with prognostic capabilities," *IEEE Transactions on reliability*, vol. 61, no. 4, pp. 872–883, 2012.

[21] T. Nakagawa, *Shock and damage models in reliability theory*. Springer Science & Business Media, 2007.

[22] G. Gola and B. H. Nystad, "From measurement collection to remaining useful life estimation: Defining a diagnostic-prognostic frame for optimal maintenance scheduling of choke valves undergoing erosion," in *Annual Conference of the Prognostics and Health Management Society*, vol. 2, 2011, p. 2011.

[23] A. Zhang, Y. Liu, A. Barros and Y. Wang, "Prognostic and health management for safety barriers in infrastructures: Opportunities and challenges," in *Safety and Reliability–Safe Societies in a Changing World. Proceedings of ESREL 2018*, Taylor & Francis, 2018.

[24] A. Zhang, A. Barros and Y. Liu, "Performance analysis of redundant safety instrumented systems subject to degradation and external demands," *Journal of Loss Prevention in the Process Industries*, vol. 62, p. 103 946, 2019.

[25] A. Zhang, Y. Liu, A. Barros and E. Kassa, "A degrading element of safety instrumented systems with combined maintenance strategy," in *Proceedings of the 29th European Safety and Reliability Conference (ESREL). 22–26 September 2019 Hannover, Germany*, Research Publishing Services, 2019.

[26] A. Zhang, T. Zhang, A. Barros and Y. Liu, "Optimization of maintenances following proof tests for the final element of a safety-instrumented system," *Reliability Engineering & System Safety*, vol. 196, p. 106 779, 2020.

[27] A. Zhang, H. Srivastav, A. Barros and Y. Liu, "Study of testing and maintenance strategies for redundant final elements in sis with imperfect detection of degraded state," *Reliability Engineering & System Safety*, p. 107 393, 2020.

[28] A. Zhang, R. Arismendi, A. Barros and Y. Liu, “Optimal activation strategies for heterogeneous channels of safety-instrumented systems subject to aging and demands,” *Submitted to Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 202x.

[29] E. Zio, “The future of risk assessment,” *Reliability Engineering & System Safety*, vol. 177, pp. 176–190, 2018.

[30] T. Aven and J.-E. Vinnem, *Risk Management: with Applications from the Offshore Petroleum Industry*. Springer, 2007.

[31] M. S. Dorfman, *Introduction to Risk Management and Insurance (9th Edition)*. Prentice Hall, 2007.

[32] U. Kjellén, “Safety in the design of offshore platforms: Integrated safety versus safety as an add-on characteristic,” *Safety science*, vol. 45, no. 1-2, pp. 107–127, 2007.

[33] C. Ramírez-Marengo, J. de Lira-Flores, A. López-Molina, R. Vázquez-Román, V. Carreto-Vázquez and M. S. Mannan, “A formulation to optimize the risk reduction process based on lopa,” *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 3, pp. 489–494, 2013.

[34] K. Øien, S. Hauge, F. Størseth and R. K. Tinmannsvik, “Towards a holistic approach for barrier management in the petroleum industry,” SINTEF, Tech. Rep., 2015.

[35] CCPS-Center of Chemical Process Safety, “Layer of protection analysis: Simplified process risk assessment,” *New York, NY: American Institute of Chemical Engineerings*, 2001b.

[36] D. Chastain-Knight, “Confirming the safety instrumented system layer of protection,” *Process safety progress*, vol. 39, no. 1, e12079, 2020.

[37] R. Pitblado, T. Potts, M. Fisher and S. Greenfield, “A method for barrier-based incident investigation,” *Process Safety Progress*, vol. 34, no. 4, pp. 328–334, 2015.

[38] S Basnyat, P Palanque, B. Schupp and P Wright, “Formal socio-technical barrier modelling for safety-critical interactive systems design,” *Safety Science*, vol. 45, no. 5, pp. 545–565, 2007.

[39] K. Miura, C. K. Morooka, J. R. P. Mendes and I. R. Guilherme, “Characterization of operational safety in offshore oil wells,” *Journal of Petroleum Science and Engineering*, vol. 51, no. 1-2, pp. 111–126, 2006.

[40] S. Sklet, “Safety barriers on oil and gas platforms. means to prevent hydrocarbon releases,” Ph.D. dissertation, Norges teknisk-naturvitenskaplige universitet, 2006.

[41] E. Hollnagel, “Risk+ barriers= safety?” *Safety science*, vol. 46, no. 2, pp. 221–229, 2008.

[42] DNV GL, “Barrier management in operation for the rig industry,” DNV GL, Tech. Rep., Mar. 2014.

[43] A. Groot, “Advanced process safety barrier management by applying proactive incident investigation to failed or impaired barriers,” in *SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility*, Society of Petroleum Engineers, 2016.

[44] V. Cozzani, A. Tugnoli and E. Salzano, “Prevention of domino effect: From active and passive strategies to inherently safer design,” *Journal of hazardous materials*, vol. 139, no. 2, pp. 209–219, 2007.

[45] V. De Dianous and C. Fievez, “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, no. 3, pp. 220–233, 2006.

[46] R Pitblado, M Fisher, B Nelson, H Fløtaker, K Molazemi and A Stokke, “Concepts for dynamic barrier management,” *Journal of Loss Prevention in the Process Industries*, vol. 43, pp. 741–746, 2016.

[47] M. Rausand and A. Høyland, *System reliability theory: models, statistical methods, and applications*. John Wiley & Sons, 2003, vol. 396.

[48] IEC 61508, “Functional safety of electrical/electronic/programmable electronic safety-related systems,” International Electrotechnical Commission, Geneva, Switzerland, standard, 2010.

[49] IEC 61511, “Safety instrumented systems for the process industry sector,” International Electrotechnical Commission, standard, 2016.

[50] A. Misuri, G. Landucci and V. Cozzani, “Assessment of safety barrier performance in natech scenarios,” *Reliability Engineering & System Safety*, vol. 193, p. 106 597, 2020.

[51] G. Landucci, F. Argenti, A. Tugnoli and V. Cozzani, “Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire,” *Reliability Engineering & System Safety*, vol. 143, pp. 30–43, 2015.

[52] V. M. Trbojevic, “Optimising hazard management by workforce engagement and supervision.,” Risk Support Limited, London, Tech. Rep., 2008.

[53] E. Hollnagel, *Barriers and accident prevention*. Aldershot, Hampshire, UK: Ashgate Publishing, 2004.

[54] I. Prashanth, G. J. Fernandez, R. G. Sunder and B. Boardman, “Factors influencing safety barrier performance for onshore gas drilling operations,” *Journal of Loss Prevention in the Process Industries*, vol. 49, pp. 291–298, 2017.

[55] S. Hauge, S. Håbrekke, T. Kråkenes, M. A. Lundteigen and M. Merz, “Barriers to prevent and limit acute releases to sea,” SINTEF, Tech. Rep., 2012.

[56] J. Sobral and C. G. Soares, “Assessment of the adequacy of safety barriers to hazards,” *Safety science*, vol. 114, pp. 40–48, 2019.

[57] H. Jin and M. Rausand, “Reliability of safety-instrumented systems subject to partial testing and common-cause failures,” *Reliability Engineering & System Safety*, vol. 121, pp. 146–151, 2014.

[58] S. Hauge, M. A. Lundteigen, P. Hokstad and S. Håbrekke, "Reliability prediction method for safety instrumented systems–pds method handbook," SINTEF, Tech. Rep., 2010.

[59] H. Azizpour and M. A. Lundteigen, "Analysis of simplification in markov-based models for performance assessment of safety instrumented system," *Reliability Engineering & System Safety*, vol. 183, pp. 252–260, 2019.

[60] D. Martynova and P. Zhang, "Optimization of maintenance schedule for safety instrumented systems," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 12 484–12 489, 2017.

[61] H. Srivastav, A. Barros and M. A. Lundteigen, "Modelling framework for performance analysis of sis subject to degradation due to proof tests," *Reliability Engineering & System Safety*, vol. 195, p. 106 702, 2020.

[62] T. Zhang, W. Long and Y. Sato, "Availability of systems with self-diagnostic components – applying markov model to IEC 61508-6," *Reliability Engineering & System Safety*, vol. 80, no. 2, pp. 133–141, 2003.

[63] Y. Liu and M. Rausand, "Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems," *Reliability Engineering & System Safety*, vol. 145, pp. 366–372, 2016.

[64] Y. Liu and M. Rausand, "Reliability assessment of safety instrumented systems subject to different demand modes," *Journal of Loss Prevention in the Process Industries*, vol. 24, no. 1, pp. 49–56, 2011.

[65] S. Wu, L. Zhang, M. A. Lundteigen, Y. Liu and W. Zheng, "Reliability assessment for final elements of siss with time dependent failures," *Journal of Loss Prevention in the Process Industries*, vol. 51, pp. 186–199, 2018.

[66] M. A. Lundteigen and M. Rausand, "Reliability of safety instrumented systems: Where to direct future research?" *Process safety progress*, vol. 29, no. 4, pp. 372–379, 2010.

[67] CCPS, *Guidelines for Safe and Reliable Instrumented Protective Systems*. Wiley&Sons, May 2007.

[68] H. Stein and M. A. Lundteigen, "Guidelines for follow-up of safety instrumented systems (siss) in the operating phase," SINTEF, Tech. Rep., 2008.

[69] M. Schönbeck, M. Rausand and J. Rouvroye, "Human and organisational factors in the operational phase of safety instrumented systems: A new approach," *Safety Science*, vol. 48, no. 3, pp. 310–318, 2010.

[70] R. Selega, "Safety instrumented system- requirements for successful operation and maintenance," *Chemical Engineering Transactions*, vol. 48, pp. 619–624, 2016. DOI: `DOI:10.3303/CET1648104`.

[71] R. Hernandez, R. Patel, T. Attaway, V. Shah and S. A. Granherne, "Implementation and challenges of a SIL 3 subsea HIPPS," in *Offshore Technology Conference*, Offshore Technology Conference, 2016.

[72] R. Phillips, "Delivering a hipps safety critical control system," in *Offshore Europe*, Society of Petroleum Engineers, 2005.

[73] H. Liu, X. Shi, X. Chen and Y. Liu, "Management of life extension for topsides process system of offshore platforms in chinese bohai bay," *Journal of Loss Prevention in the Process Industries*, vol. 35, pp. 357–365, 2015.

[74] P. A. P. Ramírez and I. B. Utne, "Use of dynamic bayesian networks for life extension assessment of ageing systems," *Reliability Engineering & System Safety*, vol. 133, pp. 119–136, 2015.

[75] L Oliveira, J Domingues, A Hafver, D Lindberg and F. Pedersen, "Evaluation of pfd of safety systems with time-dependent and test step-varying failure rates," in *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016 (Glasgow, Scotland, 25-29 September 2016)*, 2016.

[76] S. Hauge and M. A. Lundteigen, "A new approach for follow-up of safety instrumented systems in the oil and gas industry," in *Safety, Reliability and Risk Analysis: Theory, Methods and Applications*, Valencia, Spain, 2008, pp. 2921–2928.

[77] N. J. Edwin, L. Fornes and K. Øien, "Improved safety in the arctic through digitalization," in *Proceedings of the 29th European Safety and Reliability Conference*, ESREL, 2019.

[78] EXIDA, *Safety Equipment Reliability Handbook*, 3rd ed. EXIDA L.L.C., Fischbachau, 2010.

[79] OREDA, *Offshore Reliability Data Handbook*, 4th ed., OREDA Participants, Ed. Det Norske Veritas, Høvik, 2002.

[80] OREDA, *Offshore Reliability Data Handbook*, 5th ed., OREDA Participants, Ed. Det Norske Veritas, Høvik, 2010.

[81] SINTEF, *Reliability Data for Safety Instrumented Systems: PDS Data Handbook*, S. Hauge and T. Onshus, Eds. SINTEF, Trondheim, Norway, 2010.

[82] J. V. Bukowski, "Incorporating process demand into models for assessment of safety system performance," in *RAMS'06. Annual Reliability and Maintainability Symposium, 2006.*, IEEE, 2006, pp. 577–581.

[83] H. Jin, M. A. Lundteigen and M. Rausand, "Reliability performance of safety instrumented systems: A common approach for both low-and high-demand mode of operation," *Reliability Engineering & System Safety*, vol. 96, no. 3, pp. 365–373, 2011.

[84] S. Alizadeh and S. Sriramula, "Reliability modelling of redundant safety systems without automatic diagnostics incorporating common cause failures and process demand," *ISA transactions*, vol. 71, pp. 599–614, 2017.

[85] P. Hokstad, "Demand rate and risk reduction for safety instrumented systems," *Reliability Engineering & System Safety*, vol. 127, pp. 12–20, 2014.

[86] H. Jin, "A contribution to reliability assessment of safety-instrumented systems," Ph.D. dissertation, Norwegian University of Science and Technology, 2013.

[87] E. Rogova, G. Lodewijks and M. A. Lundteigen, "Analytical formulas of pfd and pfh calculation for systems with nonconstant failure rates," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 231, no. 4, pp. 373–382, 2017.

[88] S. Wu, L. Zhang, W. Zheng, Y. Liu and M. A. Lundteigen, “Reliability modeling of subsea siss partial testing subject to delayed restoration,” *Reliability Engineering & System Safety*, vol. 191, p. 106 546, 2019.

[89] H. Srivastav, G. de Azevedo Vale, A. Barros, M. A. Lundteigen, F. B. Pedersen, A. Hafver and L. F. Oliveira, “Optimization of periodic inspection time of sis subject to a regular proof testing,” *Safety and Reliability-Safe Societies in a Changing World*, 2018.

[90] P Martorell, I Martón, A. Sánchez and S. Martorell, “Unavailability model for demand-caused failures of safety components addressing degradation by demand-induced stress, maintenance effectiveness and test efficiency,” *Reliability Engineering & System Safety*, vol. 168, pp. 18–27, 2017.

[91] S. Martorell, P. Martorell, A. I. Sánchez, R. Mullor and I. Martón, “Parameter estimation of a reliability model of demand-caused and standby-related failures of safety components exposed to degradation by demand stress and ageing that undergo imperfect maintenance,” *Mathematical Problems in Engineering*, vol. 2017, 2017.

[92] H. Jahanian, “Generalizing PFD formulas of IEC 61508 for KooN configurations,” *ISA transactions*, vol. 55, pp. 168–174, 2015.

[93] L. Lu and G. Lewis, “Configuration determination for k-out-of-n partially redundant systems,” *Reliability Engineering & System Safety*, vol. 93, no. 11, pp. 1594–1604, 2008.

[94] L. F. Oliveira and R. N. Abramovitch, “Extension of ISA TR84. 00.02 PFD equations to koon architectures,” *Reliability Engineering & System Safety*, vol. 95, no. 7, pp. 707–715, 2010.

[95] J. K. Vaurio, “Unavailability equations for k-out-of-n systems,” *Reliability Engineering & System Safety*, vol. 96, no. 2, pp. 350–352, 2011.

[96] A. C. Torres-Echeverría, S. Martorell and H. Thompson, “Modelling and optimization of proof testing policies for safety instrumented systems,” *Reliability Engineering & System Safety*, vol. 94, no. 4, pp. 838–854, 2009.

[97] A. C. Torres-Echeverría, S. Martorell and H. Thompson, “Modeling safety instrumented systems with moon voting architectures addressing system reconfiguration for testing,” *Reliability Engineering & System Safety*, vol. 96, no. 5, pp. 545–563, 2011.

[98] A. C. Torres-Echeverría, S. Martorell and H. Thompson, “Multi-objective optimization of design and testing of safety instrumented systems with moon voting architectures using a genetic algorithm,” *Reliability Engineering & System Safety*, vol. 106, pp. 45–60, 2012.

[99] M. Chebila and F. Innal, “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.

[100] P.-J. Courtois and P. Delsarte, “On the optimal scheduling of periodic tests and maintenance for reliable redundant components,” *Reliability Engineering & System Safety*, vol. 91, no. 1, pp. 66–72, 2006.

[101] A. A. Mendes, D. W. Coit and J. L. D. Ribeiro, “Establishment of the optimal time interval between periodic inspections for redundant systems,” *Reliability Engineering & System Safety*, vol. 131, pp. 148–165, 2014.

[102] H. Yang and X. Yang, “Automatic generation of markov models in safety instrumented systems with non-identical channels,” in *2010 International Conference of Information Science and Management Engineering*, IEEE, vol. 1, 2010, pp. 287–290.

[103] J. Navarro and P. Fernández-Martínez, “Redundancy in systems with heterogeneous dependent components,” *European Journal of Operational Research*, 2020.

[104] H. Rolén, “Partial and imperfect testing of safety instrumented functions,” M.S. thesis, Norges teknisk-naturvitenskaplige universitet, 2007.

[105] G. Baradits Sr, J. Madár and J. Abonyi, “Novel failure model for the purpose of modeling the imperfect proof-testing,” *International Review of Chemical Engineering*, vol. 2, no. 2, pp. 210–218, 2010.

[106] W. Mechri, C. Simon and K. BenOthman, “Switching markov chains for a holistic modeling of sis unavailability,” *Reliability Engineering & System Safety*, vol. 133, pp. 212–222, 2015.

[107] S. Sachdeva, “Imperfect testing and its influence on availability of safety instrumented systems,” M.S. thesis, Norges teknisk-naturvitenskaplige universitet, 2015.

[108] M. A. Lundteigen and M. Rausand, “Partial stroke testing of process shutdown valves: How to determine the test coverage,” *Journal of Loss Prevention in the Process Industries*, vol. 21, no. 6, pp. 579–588, 2008.

[109] F. Brissaud, A. Barros and C. Bérenguer, “Probability of failure of safety-critical systems subject to partial tests,” in *2010 Proceedings-Annual Reliability and Maintainability Symposium (RAMS)*, IEEE, 2010, pp. 1–6.

[110] F. Brissaud, A. Barros and C. Bérenguer, “Probability of failure on demand of safety systems: Impact of partial test distribution,” *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 226, no. 4, pp. 426–436, 2012.

[111] F. Innal, M. A. Lundteigen, Y. Liu and A. Barros, “Pfdavg generalized formulas for sis subject to partial and full periodic tests based on multi-phase markov models,” *Reliability Engineering & System Safety*, vol. 150, pp. 160–170, 2016.

[112] S. Wu, L. Zhang, A. Barros, W. Zheng and Y. Liu, “Performance analysis for subsea blind shear ram preventers subject to testing strategies,” *Reliability Engineering & System Safety*, vol. 169, pp. 281–298, 2018.

[113] J. L. Rouvroye and J. A. Wiegerinck, “Minimizing costs while meeting safety requirements: Modeling deterministic (imperfect) staggered tests using standard markov models for sil calculations,” *ISA transactions*, vol. 45, no. 4, pp. 611–621, 2006.

[114] A. E. B. Longhi, A. A. Pessoa and P. A. de Almada Garcia, “Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees,” *Reliability Engineering & System Safety*, vol. 142, pp. 525–538, 2015.

[115] M Khalaquzzaman, H. G. Kang, M. C. Kim and P. H. Seong, "Optimization of periodic testing frequency of a reactor protection system based on a risk-cost model and public risk perception," *Nuclear Engineering and Design*, vol. 241, no. 5, pp. 1538–1547, 2011.

[116] Y. Redutskiy, "Optimization of safety instrumented system design and maintenance frequency for oil and gas industry processes," *Management and Production Engineering Review*, vol. 8, 2017.

[117] A. Hess, G. Calvello and T Dabney, "Phm a key enabler for the jsf autonomic logistics support concept," in *2004 ieee aerospace conference proceedings (ieee cat. no. 04th8720)*, IEEE, vol. 6, 2004, pp. 3543–3550.

[118] K. Javed, "A robust & reliable Data-driven prognostics approach based on extreme learning machine and fuzzy clustering.," Theses, Université de Franche-Comté, Apr. 2014. [Online]. Available: `https://tel.archives-ouvertes.fr/tel-01025295`.

[119] E. Zio, "Prognostics and health management of industrial equipment," in *Diagnostics and prognostics of engineering systems: methods and techniques*, IGI Global, 2013, pp. 333–356.

[120] S. Cheng, M. H. Azarian and M. G. Pecht, "Sensor systems for prognostics and health management," *Sensors*, vol. 10, no. 6, pp. 5774–5797, 2010.

[121] V. Atamuradov, K. Medjaher, P. Dersin, B. Lamoureux and N. Zerhouni, "Prognostics and health management for maintenance practitioners – review, implementation and tools evaluation," *International Journal of Prognostics and Health Management*, vol. 8, no. 060, pp. 1–31, 2017.

[122] S. Das, R. Hall, A. Patel, S. McNamara and J. Todd, "An open architecture for enabling cbm/phm capabilities in ground vehicles," in *2012 IEEE Conference on Prognostics and Health Management*, IEEE, 2012, pp. 1–8.

[123] J. Lee, F. Wu, W. Zhao, M. Ghaffari, L. Liao and D. Siegel, "Prognostics and health management design for rotary machinery systems – reviews, methodology and applications," *Mechanical systems and signal processing*, vol. 42, no. 1-2, pp. 314–334, 2014.

[124] R. Gouriveau and K. Medjaher, "Chapter 2 : Prognostics. Part : Industrial Prognostic - An Overview.," in *Maintenance Modelling and Applications.* Ser. ISBN : 978-82-515-0316-7, C. B. J. Andrews and L. Jackson, Eds., Det Norske Veritas (DNV), 2011, pp. 10–30. [Online]. Available: `https://hal.archives-ouvertes.fr/hal-00632043`.

[125] T. Tinga and R. Loendersloot, "Aligning phm, shm and cbm by understanding the physical system failure behaviour," in *European Conference on the Prognostics and Health Management Society*, 2014.

[126] J. Yan, *Machinery prognostics and prognosis oriented maintenance management.* John Wiley & Sons, 2014.

[127] A. K. Jardine, D. Lin and D. Banjevic, "A review on machinery diagnostics and prognostics implementing condition-based maintenance," *Mechanical systems and signal processing*, vol. 20, no. 7, pp. 1483–1510, 2006.

[128] ISO 13381-1, *Condition monitoring and diagnostics of machines – prognostics – part 1: General guidelines*, International Standard Organization, 2015.

[129] H. Sohn, C. R. Farrar, F. M. Hemez, G. Park, A. N. Robertson and T. O. Williams, "A coupled approach to developing damage prognosis solutions," in *Key Engineering Materials*, Trans Tech Publ, vol. 245, 2003, pp. 289–306.

[130] P. Hokstad, S. Håbrekke, R. Johnsen and S. Sangesland, "Ageing and life extension for offshore facilities in general and for specific systems," SINTEF, Tech. Rep., 2010.

[131] E. Taheri, I. Kolmanovsky and O. Gusikhin, *Survey of prognostics methods for condition-based maintenance in engineering systems*, 2019. arXiv: `1912.02708 [eess.SP]`.

[132] G. Gola and B. H. Nystad, "Prognostics and health management of choke valves subject to erosion: A diagnostic-prognostic frame for optimal maintenance scheduling," in *Diagnostics and Prognostics of Engineering Systems: Methods and Techniques*, IGI Global, 2013, pp. 313–331.

[133] B. H. Nystad, G. Gola and J. E. Hulsund, "Lifetime models for remaining useful life estimation with randomly distributed failure thresholds," in *First european conference of the prognostics and health management society*, vol. 3, 2012.

[134] B. Declerck, A. Deschoolmeester and Z. Brik, "Maintaining confidence dynamic risk management for enhanced safety," Reims, France, Oct. 2018.

[135] P Vaidya and M Rausand, "Remaining useful life, technical health, and life extension," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 225, no. 2, pp. 219–231, 2011.

[136] Y. Enomoto, "Steam turbine retrofitting for the life extension of power plants," in *Advances in Steam Turbines for Modern Power Plants*, Elsevier, 2017, pp. 397–436.

[137] K. Rafiee, Q. Feng and D. W. Coit, "Reliability modeling for dependent competing failure processes with changing degradation rate," *IIE transactions*, vol. 46, no. 5, pp. 483–496, 2014.

[138] TWI Report 17554/1/08, "Requirements for life extension of aging offshore production installations," TWI, Tech. Rep., Jan. 2008.

[139] N. Walliman, *Research methods: The basics*. Routledge, 2017.

[140] E. Phillips and D. Pugh, *How to get a PhD: A handbook for students and their supervisors*. McGraw-Hill Education (UK), 2010.

[141] R. B. Brown, *Doing your dissertation in business and management: the reality of researching and writing*. Sage, 2006.

[142] J. M. Aughenbaugh and J. W. Herrmann, "Reliability-based decision making: A comparison of statistical approaches," *Journal of Statistical Theory and Practice*, vol. 3, no. 1, pp. 289–303, 2009.

Part II

ARTICLES

Article I

Zhang, A., Liu, Y., Barros, A., & Wang, Y. (2018). Prognostic and health management for safety barriers in infrastructures: Opportunities and challenges. Safety and Reliability-Safe Societies in a Changing World. Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway. ESREL2018.

Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

Prognostic and health management for safety barriers in infrastructures: Opportunities and challenges

A. Zhang, Y. Liu & A. Barros
Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway

Y. Wang
School of Economics and Management, Tianjin Chengjian University, Tianjin, China
Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT: Different types of safety barriers are deployed in many infrastructures to reduce the occurrences of hazards, and protect people, environment and other assets in case the unexpected events have occurred and the capacity of these barriers against hazards can be weakened by degradations or the failures related to changes over time. It is natural to adapt the approaches of Prognostic and Health Management (PHM) to monitor the conditions and measurable parameters of safety barriers, and predict their future performance by assessing the extent of degradations. This study aims to identify the uniqueness and possible challenges when implementing PHM on safety barriers. Definitions and classifications of safety barriers will be discussed with considering their installation environment in infrastructures, in order to reveal what kind of characteristics of barriers can lead to higher demand on prognosis and heath monitoring. Another objective of this paper is to review the qualitative and quantitative measures for the capacity and performance of safety barriers, and to explore the possible methods and research gaps in the assessments for different PHM strategies, taking account their effects on safety barriers, and effects on the infrastructures being protected by the barriers.

1 INTRODUCTION

Maintenances can be defined as the activities to keep a system in a working order (Do et al. 2015). With the development of sensor technologies, the maintenances for many complex systems involve more and more condition-based and preventive activities to reduce maintenance costs on one hand, and improve their performance on the other hand (Sharma et al. 2017, Liu et al. 2017). Prognostics and Health Management (PHM), including fault detection, diagnostics, prognostics and health management, is a developing approach that enables real-time health assessment of a system and predicts of its future state based on up-to-date information. PHM has been conducted in many applications including manufacturing, aerospace systems, railway, energy, and military industry (Sun et al. 2012, Pecht and Rui 2010).

Safety barriers are installed in many critical systems and infrastructures to prevent hazardous events or mitigate their consequences, such as fire prevention systems and railway signaling systems. Technological safety barriers, such as shutdown valves in process, and airbags on cars, are also called as safety-critical system (Rausand 2014). But these safety barriers can also degrade and fail to accomplish their safety function under the evolving environment (Zio 2016). In case of failures of the barriers, serious accidents or disaster may occur. Many studies have been carried out on the operational and performance analysis of the safety barriers (Innal et al. 2015, Duijm and Goossens 2006, Innal et al. 2015, Rahimi et al. 2011, Cai et al. 2012), and most of them assume that the failures of components in the safety barriers follow the exponential distribution (Guo and Yang 2008, Jin and Rausand 2014, Catelani et al. 2011, Liu and Rausand 2011), meaning that their failure rate keep constant in any time.

According to IEC 61508 (2010) and IEC 61511 (2003), many technological safety barriers consist of three subsystems: sensor(s), logic solver(s) and actuating unit(s). The mechanical actuating units can degrade due to corrosion and wear-out etc, become more vulnerable along with time (Zio 2016), and so that the assumption of exponential distribution of failures is challenged. Based on this concern, a growing attention is given to the predict degradations of safety barriers and offer suitable maintenances in advance to ensure the barrier adequacy. PHM can be a helpful approach in performance prediction and decision-making for maintenances.

The purpose of this paper is to review the techniques of PHM and designing and operational characteristics of safety barriers, so as to explore the research issues when the PHM approach is planned to be implemented for improving the integrity of safety barriers.

The remained of this paper is organized as follows: In section 2, the development and advantages of PHM are introduced; Section 3, includes the review of safety barriers in infrastructure and introduces technological barriers; Section 4 introduces several unmet problems and challenges related to using PHM on safety barriers. A conclusion is given in Section 5.

2 PROGNOSTICS AND HEALTH MANAGEMENT

2.1 *Development of PHM*

PHM is developed based on the concept of Condition-based maintenance (CBM). CBM is an approach to carry out maintenance actions based on the information collected through condition monitoring on systems in contrast to breakdown or time-based preventive maintenance. In order to make a timely decision on maintenance, prognostics is the key technology for CBM (Jardine et al. 2006, Shin and Jun 2015, Bousdekis et al. 2015). From this point, PHM is developed from the concept of CBM. A CBM program consists of three key steps (see Figure 1) (Lee 2004):

1. Data acquisition step;
2. Data processing step;
3. Maintenance decision-making step

Diagnostics and prognostics are two aspects in CBM. Diagnostics deals with fault detection, isolation and identification when it occurs (Jardine et al. 2006). Prognostics, in ISO-13381 (2015), is to estimate the time to failure and risk for one or more existing and future failure modes. The relative placement of detection, diagnostic and prognostic can be explained in Figure 2 (Gouriveau and Medjaher 2011).

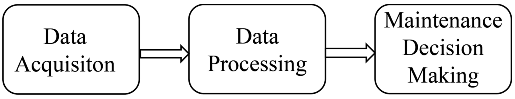


Figure 1. Three steps in CBM.

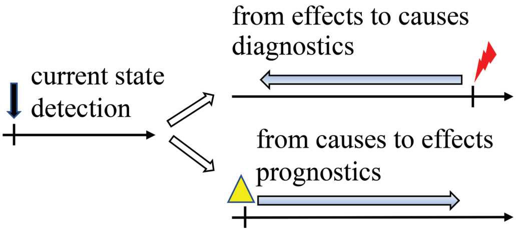


Figure 2. Complementarity of detection diagnostic and prognostic activities (Gouriveau, 2011).

In literature, prognostics is a process of health assessment and prediction, which includes incipient fault/failure detection, performance monitoring, life cracking and predicting residual useful lifetime (RUL) (Hess et al. 2005, Lee et al. 2014);

PHM is the extension of prognostics. According to CALCE (Center for Advanced Life Cycle Engineering) (2012), PHM is the means to predict and protect the integrity of equipment and complex systems, and avoid unanticipated operational problems leading to mission performance deficiencies, degradation, and adverse effects to mission safety.

Sun et al. (2010) regards PHM as a methodology to predict when and where failures will occur and to mitigate risks through evaluating the reliability of a system in its actual life cycle conditions. It is an enabling discipline of solving reliability problem in the process of design, manufacturing, operational and maintenance (Pecht and Jaai 2010). PHM is aiming to all information of an equipment in past, present and future while considering its environmental, operational and usage condition so as to detect its degradation, diagnose fault and predict and manage failures (Zio 2012).

Haddad (Haddad et al. 2012) regards PHM as a discipline that can used for: (i) evaluating the reliability of systems of their life cycle; (ii) determining the possible occurrence of failures and risk reduction; (iii) highlighting the Remanding Useful Lifetime (RUL) estimation. Actually, modern and comprehensive PHM systems take many issues into consideration, such as fault detection, fault isolation, useful life remaining, and performance degradation trending and then provides a broader set of maintenance benefits than any function by itself (Hess et al. 2005).

In this paper, we understand PHM as an approach to carry out dynamic management based on RUL which is predicted by status information collected through actual life cycle conditions, including environmental, operational and usage conditions.

2.2 *PHM architecture*

PHM means a complete process from capturing the data to decision-making (in maintenance,

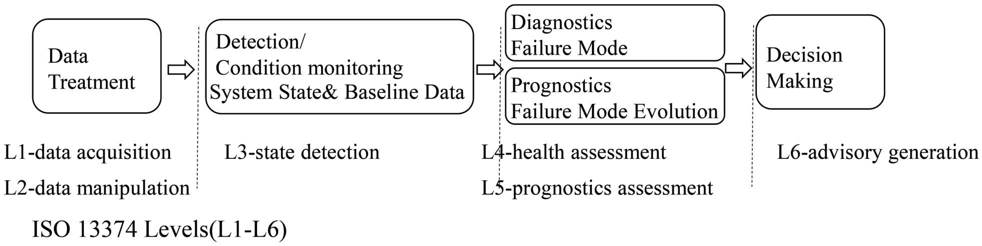


Figure 3. General process of PHM. Correlation with ISO 13374 (Guillén, 2016).

life time control, equipment design, etc.) (Guillén, Crespo, Macchi, & Gómez 2016), which is originally conceived by ISO 13374 and gradually becomes a standard in OSA-CBM (Open System Architecture for Condition Based Maintenance). As shown in Figure 3. The whole process of PHM is based on that of CBM, and can be divided into two parts. The first part (from Level 1/L1 to Level 5/L5) is related to health monitoring and prognostics, and the second part (Level 6/L6) is for health management.

In such a process, PHM attempts to answer several questions, e.g.:

- How is the status of system now? (Performance assessment).
- When will the system fail? (Remaining useful lifetime).
- What will the primary faults that cause system failure?
- Why does the incipient fault occur?

2.3 *PHM methodologies*

To answer the above questions, prognostics is currently carried out in different ways, namely with model-based, data-driven and hybrid prognostics (Brahimi et al. 2016).

The model-based approaches are based on a good knowledge of the physics of system and the available failure modes. Analysts can construct mathematical models with the above knowledge, and analyze those systems whose field operational and failure data is not enough (Lee et al. 2014, Luo et al. 2003). However, for many complex systems, one of limitations of the model-based approaches is the difficulty to create deliberate models representing the multiple physical processes (Pecht 2008). Moreover, it is very difficult to adopt the models built for some specific applications to the others, even though the systems are very similar.

The data-driven approaches are based on statistics and machine-learning techniques (Gu et al. 2007). In data-driven the remaining useful life would be predicted by fitting the monitoring data of developing fault to the degradation mechanism before it reaches the predetermined threshold level (e.g., see (Medjaher et al. 2012)). These methods are relatively simple to deploy due to the necessary of an analytical model of behavior and failure of the system.

The hybrid approaches are proposed in consideration of the pros and cons of the previous two groups (Lee 2004), in which prognostics results are claimed to be more reliable. The hybrid approaches have been used for the RUL prediction and maintenance of systems, such as (Kumar et al. 2008, García et al. 2010, Skima et al. 2015, Zhang et al. 2009).

PHM has been conducted in many areas, such as the infrastructures, aerospace industry, and in this paper we focus on the approach for safety barriers.

3 SAFETY BARRIERS

3.1 *Safety barriers and classification*

Safety barriers, or simply barriers are the equipment and features that are installed to protect people, the environment and other assets against harm should features or deviations occur in the most-designed system (Rausand 2013). Safety barriers are always related with a certain safety functions, which are defined by Sklet (2006) as the functions planned to prevent, control, or mitigate undesired events or accidents.

Figure 4 is a Bowtie diagram widely used in the field of risk analysis, where we can identify the two different roles of safety barriers. A hazardous event can occur due to some causes, so that some barriers can be located on the left side of the diagram (the causes side), to reduce the probability of the hazardous event. This kind of barriers are called as proactive barriers or prevention barriers, such as antilock braking system, electronic stability control system in automobiles. On the right side, some barriers are located on the right side (the consequences side), in case of the occurrence of a hazardous event, for reducing its effects or failure

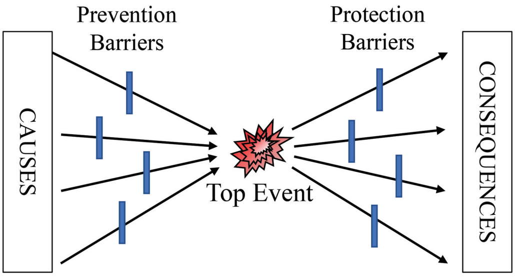


Figure 4. Bowtie diagram for a Top Event with prevention and protection barriers.

escalation, and they are regarded as reactive barriers, or protection barriers, e.g. seat belts, airbag systems (Hollnagel 2004, Rausand 2013, Groot 2016).

This classification is based on the objectives or functions of barriers. In addition, considering the operational modes of barriers, Rausand (2013) has distinguished safety barriers as passive and active barriers. An active barrier is dependent on some energy sources and a sequence of detection-diagnosis-action to perform its function, such as an airbag, Meanwhile, a passive system is not required to take an action and just by the presence of their elements to achieve its function (e.g. a seat belt).

Safety barriers also can be divided into on-line and off-line barriers. The on-line barriers operate continuously or so often, and on the contrary, the off-line ones are only used intermittently or infrequently. In practices, most protective barriers are off-line ones (Rausand & Arnljot 2004).

Sklet (2006), on the other hand, considers who are carrying out safety functions, and classifies barriers as the physical, technical, and human/operational barriers. Combining with the categorization based on the operational modes, we can obtain Figure 5. In the figure, technical barriers are always active. They are further divided into three groups: Safety Instrumented System (SIS), meaning that a technical barrier which involves the electric, electronic, and programmable electronic (E/E/PE) technologies, other technology safety-related systems and External risk reduction facilities. In the rest of this paper, we focus on technical barriers.

3.2 *Technological barriers*

A technological barrier, involving E/E/PE technologies and some mechanical items, generally consists of three subsystems: input element subsystem (e.g., sensors, transmitters), logic solver subsystem (e.g., programmable logic controllers [PLC]) and finial element subsystem (e.g., safety valves, circuit breakers). The main parts are illustrated in Figure 6.

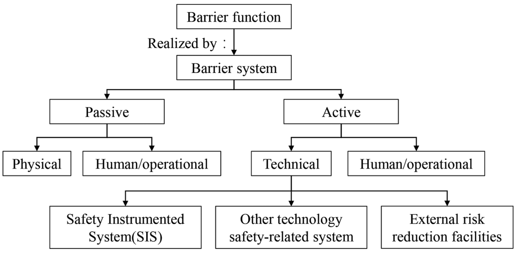


Figure 5. Classification of safety barriers (adopted from Sklet, 2006).

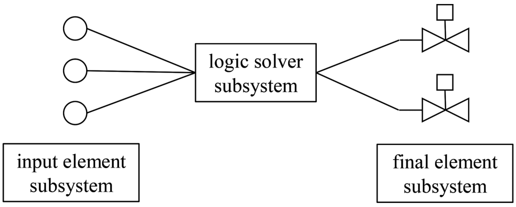


Figure 6. Main parts of a technological barrier.

The system protected by a technological barrier is called the Equipment Under Control (EUC). A safety-instrumented function (SIF) is a function that has been designed to protect the EUC against a specific demand. To enhance the reliability of a barrier, redundancy is often implemented in the system configuration.

4 DEVELOPMENT A PHM FOR SAFETY BARRIERS

We can introduce the PHM to safety barriers, with the purpose to assess the degree of deviation or degradation of barriers, and then plan maintenances in advances, so as to improve their availability and bring safety to EUC.

4.1 *Main functions of PHM on barriers*

Compared to the existing diagnostics of barriers, PHM is expected to predict failures from incipient failures or deviations in components. The main functions and potential benefits of the PHM on barriers can include:

- Advance warning of failures—Prognostics in PHM can evaluate the degradations of barriers, so as to detect incipient deviations. It is possible for maintenance staffs with prognostic results regarding the operational conditions to take actions on a barrier before a failure really occurs.

- Optimized maintenances—With prognostics, maintenance staffs also can estimate the remaining life of a component, especially a mechanical one, in a barrier, and then develop a maintenance, repair or replacement plan. Compared with scheduled maintenances, these condition-based and predictive maintenances eliminate unnecessary activities, and keep the barrier effective.
- Logistic support and cost reduction—Ideal prognostics tell the maintenance staffs when and where failures will occur, and thus they can identify and fix the failed components easily. PHM can reduce lead time and therefore increase the available time of safety barriers. Moreover, the "just-in-time" maintenances based on prognostics decrease the unnecessary costs of scheduled inspections and interruptions.

4.2 *Challenges of PHM on barriers*

Although PHM has been proved in many applications, we may meet challenges when we implement PHM on the technological safety barriers, due to the following design and operational characteristics of barriers:

4.2.1 *Operational modes of barriers*

Current PHM is always used for systems continuously running, while safety barriers have several operational modes in stead:

- Low-demand mode: where the safety function is only performed on demand, and where the frequency of demands is relatively low;
- High-demand mode: where the mechanism is same as low-demand, but the frequency of demands is relatively high;
- Continuous mode: where the safety function is a part of normal operation.

In the latest version of IEC 61508 (2010), the borderline between low-demand and high-demand is once per year in terms of demand frequency.

For those technologies barriers with demanding operational modes, they are usually in a dormant state and transit to an active state in case that demands come. The degradation mechanisms in different states are varied. Not many studies have been conducted so far on degradation prediction with state transitions. We need new approaches of parameters to predict the future performance of a barrier in response to demands during the durations of demands.

4.2.2 *Structures of barriers*

Redundancy structures are often used in barriers to improve availability and to enhance safety, e.g., two shutdown valves are installed in parallel to stop flow when the downstream pressure is too high. When one of them cannot activate, the process is still safe if the other works. Such kind of structures is called as 1-out-of-2 configuration. For a system with N channels, if at least K of the N channels need to be functional to ensure that the system is functional, the system has a K-out-of-N ($K$oo$N$) configuration.

Many barriers can be adaptive, meaning that they can change their configurations to perform safety functions when some expected occur. For example, a 2oo3 barrier can automatically transit to a 2oo2 configuration when one of the three channels fail. The challenge for PHM is to predict the effects of degradations in one channel on the entire barrier system with complex configuration and adaptivity, as well on the EUC.

4.2.3 *Failure modes and tests of barriers*

Failures of technological barriers can be classified as dangerous (D) failure and safe (S) failure. D failure refer to a failure that has the potential to put the barrier in a hazardous or fail-to-function state, while S failure does not leave the barrier in fail-to-function state (Rausand 2014), e.g. a valve shuts down unnecessarily.

The integrity of a technological barrier is highly related with tests, especially for those running in the low-demand mode. Regular proof tests are conducted on technological barriers (e.g. once per year), to reveal failures and then initiate maintenance activities if necessary. Many modern safety barriers have installed automatic self-testing modules, which has a diagnostic function and detects some failures. The D failures that can be found in diagnostic tests are called as dangerous detected (DD) failures, such as signal loss, signal out of range and final element in wrong position (Rausand 2014). The D failures that are not detected are called dangerous undetected (DU) failures. DU failures are only revealed in proof tests with regular intervals.

A research challenge of PHM is therefore to find suitable approaches to link the incipient failures or deviations with those D failures of interest in integrity of barriers. Most data-driven PHM approaches depend on the historical/training data to predict the trends of failure, but in those published data sources for technological barriers, such as Offshore Reliability Data (OREDA) and Process Equipment Reliability Data, we cannot find any clues. For model-based PHM approaches, no guidance is given to deal with those DU failures.

Another challenge is from the failure occurring in the redundancy structures. Common cause failures (CCFs) are the main contributor of the unavailability of redundant safety barriers (Hauge et al. 2015). CCFs are the failures of multiple components simultaneously or with a short time interval due to a shared root cause or a common cause. It is valuable to identify those deviations that can lead to CCFs and predict their potential influences in PHM.

4.2.4 *Measures of technological barriers*

IEC 61508 (2010) suggests the average probability of failure on demand (PFD) as a measure for technological barrier of low-demand, and the probability of failure per hour (PFH) as the measure for technological barrier of high-demand. And then, for different results of PFD and PFH, safety barriers can be located at different integrity levels (SILs), from the loose SIL 1 to the strictest SIL 4. These measures are widely used, and they are calculated always on the basis of some basic assumptions (Jin and Rausand 2014, Wang and Rausand 2014, Rausand 2014), including: (1) each failure is assumed to occur at a constant rate (i.e. exponential distributed failures); and (2) the channels in a redundant structures are identical and independent.

We release these assumptions when implementing PHM, and so weaken the theoretical foundations of measure calculations, since we have realized that deteriorations in mechanical components of a technological barrier is unavoidable. However, to evaluate the effectiveness of a PHM program, we still need to utilize the widely accepted measures, and build a relationship between SILs and effects of PHM.

4.2.5 *Cost-benefit analysis of PHM*

Safety and availability are dominator in the assessment of safety barriers. But for PHM, the return-on-investment (ROI) needs to be considered (Saxena et al. 2008, Wang and Pecht 2011), especially for the fact where other test and diagnostics are also employed on safety barriers.

The main work for ROI analysis or cost-benefit analysis is to quantify the costs and benefits of PHM (Scanff et al. 2007). The costs of a PHM program can includes: the cost of acquisition and installation for data, such as sensors and microprocessors, the cost of re-design of host product, which can be a big investment (Sun et al. 2012). The benefit is more complex including the decrease of proof tests and maintenances. It is challenging on how we choose the indicators to calculate the ROI of a PHM program. Moreover, we also need to determine the best PHM program for a specific technological barrier.

5 CONCLUSIONS

In this paper, a short review of PHM is presented. PHM enables estimating the RUL of the in-service equipment which can provide timely decision for maintenance. Due to the vital role of technological barriers and the advantages of PHM, an idea for developing a PHM system for SIS is presented. Compared with mechanical systems, technological barriers have their own characteristics which propose new challenges.

Therefore, we propose several research topics to be addressed in future, specifically in a PhD project:

- New approaches for predicting degradations of a component with state transitions;
- Mechanism of incorporating redundancy structures and varied configurations in degradation modeling and analysis;
- Models to link the effectiveness of PHM with the measures for safety barriers;
- Methods to optimize PHM and other maintenance activities under the constraints of SIL requirements by safety barriers.

REFERENCES

Bousdekis, A., B. Magoutas, D. Apostolou, & G. Mentzas (2015). A proactive decision making framework for condition-based maintenance. *Industrial Management & Data Systems 115*(7), 1225–1250.

Brahimi, M., K. Medjaher, M. Leouatni, & N. Zerhouni (2016). Development of a prognostics and health management system for the railway infrastructure review and methodology. In *Prognostics and System Health Management Conference (PHM-Chengdu), 2016*, pp. 1–8. IEEE.

Cai, B., Y. Liu, Z. Liu, X. Tian, H. Li, & C. Ren (2012). Reliability analysis of subsea blowout preventer control systems subjected to multiple error shocks. *Journal of Loss Prevention in the Process Industries 25*(6), 1044–1054.

CALCE (2012, March). http://www.prognostics.umd.edu/PHM_March_Newsletter_Final.pdf.

Catelani, M., L. Ciani, & V. Luongo (2011). A simplified procedure for the analysis of safety instrumented systems in the process industry application. *Microelectronics Reliability 51*(9), 1503–1507.

Do, P., A. Voisin, E. Levrat, & B. Iung (2015). A proactive condition-based maintenance strategy with both perfect and imperfect maintenance actions. *Reliability Engineering & System Safety 133*, 22–32.

Duijm, N.J. & L. Goossens (2006). Quantifying the influence of safety management on the reliability of safety barriers. *Journal of Hazardous Materials 130*(3), 284–292.

García, C.M., T. Escobet, & J. Quevedo (2010). Phm techniques for condition-based maintenance based on hybrid system model representation. In *Annual Conference of the Prognostics and Health Management Society*.

Gouriveau, R. & K. Medjaher (2011). Chapter 2: Prognostics. Part: Industrial Prognostic—An Overview. In C.B.J. Andrews and L. Jackson (Eds.), *Maintenance Modelling and Applications*. ISBN: 978-82-515-0316-7, pp. 10–30. Det Norske Veritas (DNV).

Groot, A. (2016, 01). Advanced process safety barrier management by applying proactive incident investigation to failed or impaired barriers.

Gu, J., N. Vichare, T. Tracy, & M. Pocht (2007, Jan). Prognostics implementation methods for electronics. In 2007 *Annual Reliability and Maintainability Symposium*, pp. 101–106.

Guillén, A., A. Crespo, M. Macchi, & J. Gómez (2016). On the role of prognostics and health management in advanced maintenance systems. *Production Planning & Control 27*(12), 991–1004.

Guo, H. & X. Yang (2008). Automatic creation of markov models for reliability assessment of safety instrumented systems. *Reliability Engineering & System Safety 93*(6), 829–837.

Haddad, G., P.A. Sandborn, & M.G. Pecht (2012). An options approach for decision support of systems with prognostic capabilities. *IEEE Transactions on Reliability 61*(4), 872–883.

Hauge, S., A. Hoem, P. Hokstad, S. Habrekke, & M.A. Lundteigen (2015). Common cause failures in safety instrumented systems.

Hess, A., G. Calvello, & P. Frith (2005, March). Challenges, issues, and lessons learned chasing the "big p". Real predictive prognostics. part 1. In *2005 IEEE Aerospace Conference*, pp. 3610–3619.

Hollnagel, E. (2004). *Barriers and accident prevention*. Aldershot, Hampshire, England.

IEC 61508 (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems. part 1–7.

IEC 61511 (2003). Functional safety—safety instrumented systems for the process industry sector.

Innal, F., Y. Dutuit, & M. Chebila (2015). Safety and operational integrity evaluation and design optimization of safety instrumented systems. *Reliability Engineering & System Safety 134*, 32–50.

ISO 13381-1:2015 (2015). Condition monitoring and diagnostics of machines—prognostics—part 1: General guidelines.

Jardine, A.K., D. Lin, & D. Banjevic (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical systems and signal processing 20*(7), 1483–1510.

Jin, H. & M. Rausand (2014). Reliability of safetyinstrumented systems subject to partial testing and common-cause failures. *Reliability Engineering & System Safety 121*, 146–151.

Kumar, S., M. Torres, Y.C. Chan, & M. Pecht (2008, June). A hybrid prognostics methodology for electronic products. In *2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, pp. 3479–3485.

Lee, J. (2004, 01). An integrated platform for diagnostics, prognostics and maintenance optimization.

Lee, J., F. Wu, W. Zhao, M. Ghaffari, L. Liao, & D. Siegel (2014). Prognostics and health management design for rotary machinery systems reviews, methodology and applications. *Mechanical systems and signal processing 42*(1), 314–334.

Liu, B., Z. Liang, A.K. Parlikad, M. Xie, & W. Kuo (2017). Condition-based maintenance for systems with aging and cumulative damage based on proportional hazards model. *Reliability Engineering & System Safety*.

Liu, Y. & 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.

Luo, J., M. Namburu, K. Pattipati, L. Qiao, M. Kawamoto, & S. Chigusa (2003, Sept). Model-based prognostic techniques [maintenance applications]. In *Proceedings AUTOTESTCON 2003. IEEE Systems Readiness Technology Conference*. pp. 330–340.

Medjaher, K., D.A. Tobon-Mejia, & N. Zerhouni (2012). Remaining useful life estimation of critical components with application to bearings. *IEEE Transactions on Reliability 61*(2), 292–302.

Pecht, M. (2008). *Prognostics and health management of electronics*. Wiley Online Library.

Pecht, M. & R. Jaai (2010). A prognostics and health management roadmap for information and electronics-rich systems. *Microelectronics Reliability 50*(3), 317–323.

Pecht, M. & K. Rui (2010). Diagnostics, prognostics and system's health management. *PHM Centre, City Unversity of Hong Kong*, 7–23.

Rahimi, M., M. Rausand, & M. Lundteigen (2011). Management factors that influence common-cause failures of safety-instrumented systems in the operational phase. *Advances in Safety, Reliability, and Risk Management, ESREL 2011*, 2036–2044.

Rausand, M. (2013). *Risk assessment: theory, methods, and applications*, Volume 115. John Wiley & Sons.

Rausand, M. (2014). *Reliability of safety-critical systems: theory and applications*. John Wiley & Sons.

Rausand, M. & H. Arnljot (2004). *System reliability theory: models, statistical methods, and applications*, Volume 396. John Wiley & Sons.

Saxena, A., J. Celaya, E. Balaban, K. Goebel, B. Saha, S. Saha, & M. Schwabacher (2008). Metrics for evaluating performance of prognostic techniques. In *Prognostics and health management, 2008. phm 2008. International conference on*, pp. 1–17. IEEE.

Scanff, E., K. Feldman, S. Ghelam, P. Sandborn, M. Glade, & B. Foucher (2007). Life cycle cost impact of using prognostic health management (phm) for helicopter avionics. *Microelectronics Reliability 47*(12), 1857–1864.

Sharma, P., M.S. Kulkarni, & V. Yadav (2017). A simulation based optimization approach for spare parts forecasting and selective maintenance. *Reliability Engineering & System Safety*.

Shin, J.-H. & H.-B. Jun (2015). On condition based maintenance policy. *Journal of Computational Design and Engineering 2*(2), 119–127.

Skima, H., K. Medjaher, C. Varnier, E. Dedu, & J. Bourgeois (2015, March). Hybrid prognostic approach for micro-electro-mechanical systems. In *2015 IEEE Aerospace Conference*, pp. 1–8.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of loss prevention in the process industries 19*(5), 494–506.

Sun, B., S. Zeng, R. Kang, & M. Pecht (2010). Benefits analysis of prognostics in systems. In *Prognostics and Health Management Conference, 2010. PHM'10*, pp. 1–8. IEEE.

Sun, B., S. Zeng, R. Kang, & M.G. Pecht (2012). Benefits and challenges of system prognostics. *IEEE Transactions on reliability 61*(2), 323–335.

Wang, W. & M. Pecht (2011). Economic analysis of canary-based prognostics and health management. *IEEE Transactions on Industrial Electronics 58*(7), 3077–3089.

Wang, Y. & M. Rausand (2014). Reliability analysis of safety-instrumented systems operated in high-demand mode. *Journal of Loss Prevention in the Process Industries 32*, 254–264.

Zhang, H., R. Kang, & M. Pecht (2009, Dec). A hybrid prognostics and health management approach for condition-based maintenance. In *2009 IEEE International Conference on Industrial Engineering and Engineering Management*, pp. 1165–1169.

Zio, E. (2012). Prognostics and health management of industrial equipment. *Diagnostics and prognostics of engineering systems: methods and techniques*, 333–356.

Zio, E. (2016). Some challenges and opportunities in reliability engineering. *IEEE Transactions on Reliability 65*(4), 1769–1782.

Article II

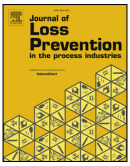
Zhang, A., Barros, A., & Liu, Y. (2019). Performance analysis of redundant safety-instrumented systems subject to degradation and external demands. Journal of Loss Prevention in the Process Industries, 62, 103946.

Journal of Loss Prevention in the Process Industries 62 (2019) 103946

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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



Performance analysis of redundant safety-instrumented systems subject to degradation and external demands

Aibo Zhang, Anne Barros, Yiliu Liu*

Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ARTICLE INFO

Keywords:
Safety-instrumented system
Degradation
Redundant structure
Probability failure on demand

ABSTRACT

Safety-instrumented systems (SISs) play a vital role in preventing hazardous events in the offshore facilities. Many of existing performance analysis of SISs are based on the constant failure rate assumption, which is however doubtful when it is applied to actuator sub-systems or mechanical final elements of a SIS. These mechanical SIS components can become vulnerable with time and with upcoming demands given the past exposures to shocks/demands. In this paper, we analyze SIS reliability and unavailability by considering that a failure occurs when total degradation of a SIS component, including continuous degradation and increments caused by random demands, exceeds to a predefined critical threshold. The dependency of two components in a redundant structure of mechanical actuators caused by random demands is also taken into account in the analysis. Approximation formulas for reliability and unavailability of the redundant SIS sub-system under a degradation process are developed. Finally, a numerical example is conducted to illustrate effects of degradation parameters on SIS performance.

1. Introduction

Safety instrumented systems (SISs), which generally consist of sensor-, logic solver- and actuator-subsystems, are widely used to prevent the occurrences of hazardous events or mitigate their consequences (Rausand, 2014). These systems are designed to perform some specific safety-instrumented functions (SIFs) to protect the equipment under control (EUC) in different industries (Rausand and Arnljot, 2004).

In terms of reliability assessment of SISs, a considerable amount of literature is available. Almost all reliability assessments of SISs are based on an assumption that the failure rates of the components within the systems are constant, such as (Guo and Yang, 2008; Liu and Rausand, 2011; Catelani et al., 2011; Jin and Rausand, 2014), even in (IEC 61511, 2010) and (IEC 61511, 2003). It means that all components or SIS channels are as-good-as-new when they are functioning, and their failures follow the exponential distribution. However, in practices many mechanical actuators of SISs become more vulnerable along with time (Zio, 2016), because they chronically expose to some failure mechanisms, such as corrosion, wear, fatigue (Rafiee et al., 2014, 2017). The actual lifetimes of actuators are determined not only by their reliability, but by the operating conditions (Nakagawa, 2007), and the assumption of constant failure rate is thus questionable. For such cases, researchers have identified that the failure rates of these items are non-constant, and they have chosen the Weibull distribution in reflecting the failure process (Rogova et al., 2017; Wu et al., 2018).

Redundant structures are often used in SISs to improve the system availability and so to enhance safety, e.g., two shutdown valves are installed in parallel to stop flow when the downstream pressure is too high. When one of them cannot be activated, the process, namely EUC, is still safe if the other valve works. Such kind of configuration is called as 1-out-of-2 (1oo2), where channels/units are also assumed identical with a same constant failure rate in most of the existing studies (Jin and Rausand, 2014; Chebila and Innal, 2015; Mechri et al., 2015; Innal et al., 2016). Actually, mechanical components in a 1oo2 configuration expose to the same environment and stand demands simultaneously, so that it is reasonable to suppose that their times-to-failure can be relevant and dependent.

In case the degradation in mechanical components is unavoidable, the performance information about system and evolving environment (Zhou et al., 2008) is helpful for the reliability assessment. Deterioration of the mechanical actuators in a SIS are not only due to chronic mechanisms, e.g. wear and material fatigue (Lai and Chen, 2016), but also from the external shocks, namely demands for SIS actuation (Nawaz, 2008). For example, in a high integrity pressure protection system (HIPPS), the required function of the actuator, valves, is to close

[*] Corresponding author.
E-mail address: yiliu.liu@ntnu.no (Y. Liu).

https://doi.org/10.1016/j.jlp.2019.103946
Received 12 July 2019; Received in revised form 1 August 2019; Accepted 21 August 2019
Available online 05 September 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/).

the flow in the pipeline when the pressure beyond the specialization. Occasional high pressures cause unprecedented stresses on the valve, and so the effects of such demands on degradation of the valves, especially on those with serious damages, may not be neglected.

Two degradation processes should be therefore considered in assessing the performance of mechanical SIS actuators: (1) continuous aging degradation, and (2) additional damages by the randomly occurring demands. It is also natural to assume that when the overall degradation of such components arrives at a predefined level, they can not be activated as expected when a new demand comes.

Degradation challenges the common assumption of as-good-as-new after each proof-test in SIS reliability assessment (see (IEC 61511, 2010) and (IEC 61511, 2003). In general, the reliability of a system decreases as the degradation processes develop (Zio, 2016). Once the degradation reaches a specific level, the component will fail. The so-called specific level for SIS actuators is referring to a certain performance requirement, such as closing time and maximum leakage rate in closed position (Hauge et al., 2016).

There has been considerable amount of published literature that analyzes the reliability of single component experiencing either degradation or random shocks (Kharoufeh and Cox, 2005; Tang et al., 2014; Rafiee et al., 2017; Liu et al., 2017; Zhang et al., 2017; Xu et al., 2018). Models used in these researches can be divided into several categories: statistical models of time to failure (e.g. (Gebraeel et al., 2009),), stochastic models (Ye and Xie, 2015; Ye et al., 2015; Chen et al., 2015) and multi-state models (Li and Pham, 2005a, 2005b; Lin et al., 2015; Song et al., 2018). Stochastic processes are very effective in modeling time dependent degradation with taking dynamic operating conditions included (Singpurwalla, 1995). Klutke and Yang (2002) have derived an availability model for an inspected system subject to shock and graceful degradation (Deloux et al., 2009). have considered both continuous degradations and shocks in the calculation of system reliability, and propose a predictive maintenance policy as a response (Bocchetti et al., 2009). have considered wear degradation and thermal cracking in their competing risk model for in a marine Diesel engine considering (Mercier et al., 2013). have used a Poisson process and a gamma process to model the cracks of passive components within electric power plant. The homogeneous gamma process has been in fact widely used to model gradual degradation phenomena, such as fatigue crack growth (Lawless and Crowder, 2004), thinning due to corrosion (Kallen and van Noortwijk, 2005), corroded steel gates (Frangopol et al., 2004), sealing performance of O-rings (Sun et al., 2018).

However, new research is motivated by the fact that the existing results in degradation analysis, even those for redundant systems, cannot be simply applied to a SIS due to its operational characteristics, e.g.

- For components in the redundant structure of a SIS, they are expose to same environment and same demands. The damage sizes of the two components caused by a random demand can be assumed be similar or same, and the degradation processes of two components are thus correlated.
- The components in a SIS are simultaneously tested and maintained in most cases, and such an operational approach weakens the assumption of independence of the two components.
- Failures and degradations are always hidden until periodical tests. For the valves in a HIPPS as an example, they are mainly in a dormant state in the normal operation, meaning that the performance can not be estimated by visual inspection or diagnostic tests (Rausand, 2014).
- SISs are evaluated with different measures when they are operated in different modes, and the frequency of demands to activate SISs is key to decide what measure can be used. Although more demands obviously can accelerate degradation, it is necessary to value the effects of demands in consideration of measure adaptability

The average probability of failures on demand ($\mathrm{PFD_{avg}}$) is a widely acknowledged measure to quantify the reliability of a low-demand SIF. In the current literature, all units are as-good-as-new as long as they are functioning at the proof-tests, so the $\mathrm{PFD_{avg}}$ is totally same in each test interval. It is not at all realistic for SISs with degradations. Given that no failure is revealed in a proof test, it only means that the unit is functioning, but not as-good-as-new. It is natural to suppose that the $\mathrm{PFD_{avg}}$ increases in step in different test intervals.

The objective of this paper is to deal with the challenges of a SIS to degradation analysis, and propose a degradation-based unavailability analysis model for a 1oo2 SIS. The specific objectives include:

- Investigating the combined effects of continuous degradation and random demands on the reliability and availability of a SIS with hidden failures;
- Developing new algorithms for calculating time-dependent $\mathrm{PFD_{avg}}$ in different test intervals.
- Providing guidance on decision-making for proof tests of SISs, to ensure compliance and cost-effective operation.

The remainder of this article is organized as follows. Section 2 describes the SIS operation as a stochastic degradation process, with random demand damages and demands arrivals. Section 3 discusses the reliability modeling and $\mathrm{PFD_{avg}}$ calculation of a 1oo2 SIS. In section 4, a numerical example is presented to demonstrate our models and sensitivity analysis is also included. Finally, Section 5 presents conclusions.

2. Definitions and assumptions

2.1. Notation

The notions used in formulating the reliability in this paper are now listed.

$N(t)$	number of demands arrived by time t
λ_{de}	arrival rate of random demands
L	performance threshold for failure in terms of a certain degradation
$X(t)$	aging degradation of a component
y_i	damage by the i-th random demand on a component
$Y(t)$	cumulative damage of demands on the component by t
τ	function test interval
$F_Z(z, t)$	the probability of total degradation less than z at time t
$G(X, t)$	cumulative density function of $X(t)$ at time t
$f_{y_i}^{k}$	probability density function of the sum of k independent and identically distributed (i.i.d.) y_i variables
$Z(t)$	overall degradation of the component

2.2. Redundancy and testing of SISs

SISs are designed to protect EUC given a specific safety integrity level (SIL). IEC 61508 specifies four levels for SIL, with SIL1 being the least reliable and SIL4 being the most reliable. To fulfill the performance requirements for a certain SIL, a SIS in the low-demand mode must have an average probability of failure on demand ($\mathrm{PFD_{avg}}$) in the corresponding interval, as illustrated in Table 1.

Table 1
SILs for low-demand SISs.

SIL	$\mathrm{PFD_{avg}}$
SIL 4	10^{-5} to 10^{-4}
SIL 3	10^{-4} to 10^{-3}
SIL 2	10^{-3} to 10^{-2}
SIL 1	10^{-2} to 10^{-1}

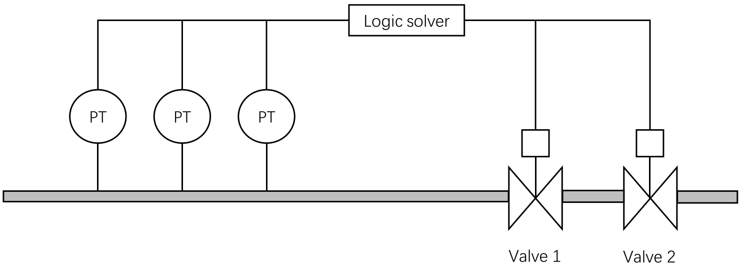


Fig. 1. Example of a HIPPS.

We can take HIPPS as an example of SISs, which architecture is shown in Fig. 1. As mentioned above, the two valves in this SIS are installed in series with a 1oo2 voting configuration to meet the requirement of (IEC 61511, 2010).

The fundamental tasks for the HIPPS is to control high pressure to keep the EUC under acceptable risk level. In general, mechanical systems are designed with safety margins to meet the specified performance requirement (Marszal and Mitchell, 2004). The performance criteria for the HIPPS, e.g. leakage rate and closing time, should be a target value with deviation (Rausand, 2014). In theory, the designed leakage rate should be 0 kg/s, but there is an acceptable deviation based on practical consideration, like 1 kg/s (Nawaz, 2008). Also the performance criteria is different under specific working scenarios. Like, in the offshore plants, acceptable leakage rates generally set higher than for an onshore installation, the main reason for this is due to lower human risk exposure in offshore plants (Nawaz, 2008).

If leakage rate is lower than this acceptable deviation, the performance of valve is acceptable, and it can be stated that the valve is functioning. Too much internal leakage also can weaken control, and even can cause a failure in control of pressure. If the actual leakage rate is higher than the acceptable, the valve is not effective any longer for risk control (Nawaz, 2008). The valve will be in a failed state. The failure mode is "Leakage (through the valve) in closed position (LCP)".

This failure mode is mainly caused by corrosion and erosion on the gate or the seat (Rausand, 2014). The failure mode is dangerous undetected failure and only can be revealed by proof tests or demands.

The possible failure causes could be:

- Normal wear due to corrosive medium. Since a valve is installed to control the pressure, the contact of its gate sealing area with erosive medium can not be avoided. The erosion of the gate sealing area is a progressive, which provides larger flow paths for leaking oil.
- Random demands beyond the specification. The intention of a shutdown valve is to shut-off the liquid flow in case an emergency that leads to a hazardous situation. Operating in higher pressure can result in the misalignment between the gate and the seat of the valve (Technical Note 101). The misalignment of a valve seat can accelerate the existing wear process.

Once high pressure occurs in a pipeline, the stresses on the 2 valves in Fig. 1 will be same or similar. The high pressure could cause a same damage on the two valves simultaneously. Considering the coupling factor, reliability analysis of 1oo2 configuration could not consider two valves separately.

2.3. Assumptions in modeling

In this paper, the aforementioned two processes of the 1oo2 actuator subsystem are regarded as stochastic processes.

For the LCP failure mode of valves, three factors are of interests: acceptable deviation, frequency of closing operations and the effects of high pressure, which will be quantified in the following analysis. First, the acceptable deviation will be the failure threshold L. The valve will be activated when a hazard or demand occurs, so the frequency of closing operation could be linked with a demand rate λ_{de} given that the occurrences of demands are modeled as a homogeneous Poisson process. Moreover, high pressure/demands can cause non-negative damage to valve and accelerate the degradation, and such side-effects are modeled by a gamma distribution since it is fairly flexible and positively-skewed distributed with the convenient mathematical properties.

The total degradation process of an actuator includes continuous deterioration and abrupt damages due to random demands as shown in Fig. 2. The occurrence times of random demands $t_1, t_2, \cdots$. are following Poisson process with parameter λ_{de}. Each demand could accelerate the degradation at some extent immediately, as $y_1, y_2, \cdots$. When the total degradation arrives at the failure threshold L, the valve will fail.

The following assumptions and considerations should be mentioned before the performance analysis of the actuators:

1. The actuator starts working at time $t = 0$ and it is subject to a continuous degradation process. In this paper, we assume that the degradation with aging $\{X(t);\ X(0) = 0,\ t\ \geq\ 0\}$ is a homogeneous Gamma process with the shape parameter $\alpha > 0$ and the scale parameters $\beta > 0$ (Van Noortwijk, 2009). For the period from s to t, $s < t$, the new degradation $X(t) - X(s)$ follows a Gamma density and probability density function (PDF)

$$X(t) - X(s) \sim \Gamma(\alpha(t-s), \beta) = f_{X(t)-X(s)}(x) = \frac{\beta^{\alpha(t-s)}}{\Gamma(\alpha(t-s), 0)} x^{\alpha(t-s)-1} e^{-\beta x},\ \alpha, \beta > 0 \tag{1}$$

The cumulative density function (CDF) of $X(t)$ for $T > 0$ (Wang et al., 2015) is

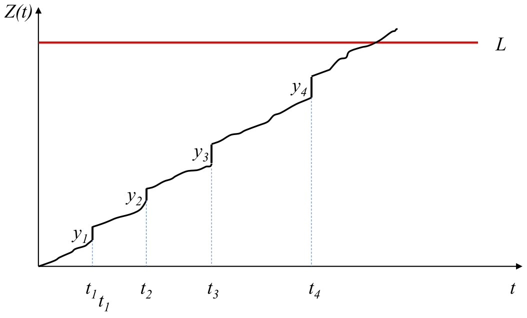


Fig. 2. The degradation behavior of one unit based on the two processes.

$$F_{X(t)}(x) = \Pr\{X(t) \le x\} = \int_0^x f_{X(t)}(z)dz = \frac{\gamma(\alpha t, x\beta)}{\Gamma(\alpha t)} \tag{2}$$

where Γ denotes the upper incomplete Gamma function defined as

$$\Gamma(\alpha) = \int_0^\infty z^{\alpha-1}e^{-z}dz,\ \alpha > 0 \tag{3}$$

γ denotes the lower incomplete Gamma function defined as

$$\gamma(\alpha, x) = \int_0^x z^{\alpha-1}e^{-z}dz,\ x \ge 0,\ \alpha > 0 \tag{4}$$

Then, the mean and variance of $X(t)$ are $\alpha t/\beta$ and $\alpha t/\beta^2$, respectively.

2. The actuator mainly stays in a dormant state. Demands occur following a homogeneous Poisson process with rate λ_{de}. Let $N(t)$ denote the number of all demands that arrived by time t. The probability of exactly n demands occurring in the time interval $[0, t)$ is

$$\Pr(N(t) = n) = \frac{e^{-\lambda_{de}t}(\lambda_{de}t)^n}{n!},\ n = 0,1,\cdots, \tag{5}$$

3. It is assumed that the damage y_i, for $i = 1,2,\ \cdots,N(t)$, on the actuator caused by the i-th demand is non-negative, independent and gamma distributed with parameters (ξ_i, ρ). The cumulative damage due to demands by time t, $Y(t)$, can be given as

$$Y(t) = \begin{cases} \sum_{i=1}^{N(t)} y_i, & \text{if } N(t) > 0 \\ 0, & \text{if } N(t) = 0 \end{cases} \tag{6}$$

Meanwhile, all demands y_i are assumed to have the same scale parameter ρ, then

$$\textstyle\sum_{i=1}^{N(t)} y_i \sim Gamma\left(\sum_{i=1}^{N(t)} \xi_i, \rho\right) \tag{7}$$

4. All demands will cause the same damage size on two valves simultaneously.
5. A failure occurs when the total degradation reaches a certain critical threshold L. The failure to work of the system means that both of the two components have degraded to the failure threshold L.
6. The system is regularly proof-tested after a certain period τ ($\tau > 0$). Proof-tests are non-destructive and non-damage to the actuators. During a proof-test, the only information we can collect about the system status is whether it is functioning or not.
7. Common cause failures (CCFs) in such a 1oo2 configuration are excluded, with the purpose to illustrate the effects of degradation on a redundant architecture apparently.

As mentioned before, $\mathrm{PFD}_{\mathrm{avg}}$ is a widely used unavailability measure of a SIF. To describe the system performance clearly, algorithms and approximation formulas for the reliability of one unit and that of a 1oo2 configuration will be derived at first, and then such formulas will be the basis of $\mathrm{PFD}_{\mathrm{avg}}$ calculation.

3. Reliability and unavailability analysis

3.1. Unit reliability analysis

According to assumptions in 2.3, the total degradation of one unit, $Z(t)$, is the sum of degradation due to aging process and the instantaneous damages due to random demands. The overall degradation of unit is expressed as $Z(t) = X(t) + Y(t)$.

Considering the demands following a Poisson process, the probability that total degradation at time t is less than z, $F_Z(z, t)$, can be derived as

$$\begin{gathered} F_Z(z, t)(t) = \Pr(Z(t) < z) \\ = \textstyle\sum_{i=0}^\infty \Pr(X(t) + Y(t) < z|N(t) = i)\Pr(N(t) = i) \end{gathered} \tag{8}$$

Furthermore, a convolution integral can be used in (8). We set $G(X, t)$ as the cumulative density function of $X(t)$ at t, $f_{y_i}^k$ as the probability density function of the sum of k independent and identically distributed (i.i.d.) Y_i variables, then $F_Z(z, t)$ can be derived as:

$$F_Z(z, t)(t) = \sum_{i=0}^\infty \left(\int_0^z G(z-u, t)f_{y_i}^k(u)du\right)\frac{e^{-\lambda_{de}t}(\lambda_{de}t)^i}{i!} \tag{9}$$

3.2. System reliability analysis

The actuator subsystem is still functioning even when one of the two units has failed, so that the reliability of such a 1oo2 configuration by time t is the probability that total degradation of at least one component is less than the threshold level $(Z(t) < L)$. The survivor function of the 1oo2 configuration is,

$$R(t) = P\{[Z_1(t) < L] \cup [Z_2(t) < L]\} \tag{10}$$

Given that one demand can result in same damage of the two units, the times-to-failure of two components are dependent (Song et al., 2014). Most existing papers only considered the dependence due to same number of demands $N(t)$. Since the two components are exposing to same damage each time. It is reasonable to consider the dependency due to impact of each demand. We need to compute it by finding the marginal distribution, $f_Y(y)$. Based on the law of total probability, we then integrate the marginal distribution to derive the system reliability, as shown in 11.

As assumed, demands are independent from the aging degradation process, then the reliability of a 1oo2 configuration is given

$$\begin{aligned} R(t) &= P\{[Z_1(t) < L] \cup [Z_2(t) < L]\} \\ &= \textstyle\int_0^L [1 - \prod_{i=1}^2 (1 - P(Z_i(t) < L|Y = y, N(t))]f_Y(y)dy \\ &= \textstyle\sum_{k=0}^\infty \int_0^L [1 - \prod_{i=1}^2 (1 - P(X_i(t) + Y_i(t) < L|S = y, N(t) = k)]f_Y(y) \\ &\quad dy \cdot P[N(t) = k] \\ &= \textstyle\sum_{k=0}^\infty \int_0^L [1 - \prod_{i=1}^2 (1 - P(X_i(t) < L - y)]f_Y(y)dy \cdot P[N(t) = k] \\ &= \textstyle\sum_{k=0}^\infty \int_0^L \left[1 - \prod_{i=1}^2 \left(1 - \frac{\gamma(\alpha t, (L-y)\beta)}{\Gamma(\alpha t)}\right)\right] \frac{\rho^{k\xi} \cdot y^{k\xi-1} \cdot e^{-\rho y}}{\Gamma(k\xi)}dy \cdot \frac{e^{-\lambda_{de}t}(\lambda_{de}t)^k}{k!} \\ &= \textstyle\sum_{k=0}^\infty \int_0^L \left[1 - \left(1 - \frac{\gamma(\alpha t, (L-y)\beta)}{\Gamma(\alpha t)}\right)^2\right] \frac{\rho^{k\xi} \cdot y^{k\xi-1} \cdot e^{-\rho y}}{\Gamma(k\xi)}dy \cdot \frac{e^{-\lambda_{de}t}(\lambda_{de}t)^k}{k!} \\ &= \left[1 - \left(1 - \frac{\gamma(\alpha t, L\beta)}{\Gamma(\alpha t)}\right)^2\right] \cdot e^{-\lambda_{de}t} + \\ &\quad \textstyle\sum_{k=1}^\infty \int_0^L \left[1 - \left(1 - \frac{\gamma(\alpha t, (L-y)\beta)}{\Gamma(\alpha t)}\right)^2\right] \frac{\rho^{k\xi} \cdot y^{k\xi-1} \cdot e^{-\rho y}}{\Gamma(k\xi)}dy \cdot \frac{e^{-\lambda_{de}t}(\lambda_{de}t)^k}{k!} \end{aligned} \tag{11}$$

The process for general *KooN* architecture is same as 1oo2 in this paper. The only consideration is to replace the survivor function in Eq. (10). Here, we take 1oo2 as a typical configuration to illustrate the tendency of $R(t)$ and $\mathrm{PFD}_{\mathrm{avg}}$.

3.3. Calculating PFD

In the existing studies, components in SISs are as-good-as-new after each proof-test, and therefore $\mathrm{PFD}_{\mathrm{avg}}$ within each proof-test interval is completely same. When degradation is in consideration, the situation becomes different, namely $\mathrm{PFD}_{\mathrm{avg}}$ in a proof-test interval is dependent on that in the previous one.

Consider a 1oo2 configuration and let T denote the time to failure of the actuator subsystem. The failure probability by t is $F(t) = Pr\{[Z_1(t) > L] \cap [Z_2(t) > L] | T \le t\}$, and the instantaneous unavailability of the SIS subsystem within the first proof test interval, $\mathrm{PFD}_1(t)$, is

$$\mathrm{PFD}_1(t) = \Pr([Z_1(t) > L] \cap [Z_2(t) > L] \text{ by } t)$$
$$= F(t) = 1 - \Pr([Z_1(t) < L] \cup [Z_2(t) < L]) = 1 - R(t) \tag{12}$$

The average value of $\mathrm{PFD}_1(t)$ in the first proof test interval$(0,\tau)$ can be obtained then

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{1}{\tau}\int_0^\tau \mathrm{PFD}_1(\mathrm{t})dt = 1 - \frac{1}{\tau}\int_0^\tau R(t)dt \tag{13}$$

Using the survivor function of the system $\mathrm{R}(t)$ in (11), we can get

$$\mathrm{PFD}_{\mathrm{avg}} = 1 - \tfrac{1}{\tau}\int_0^\tau R(t)dt$$
$$= 1 - \tfrac{1}{\tau}\int_0^\tau \left\{\left[1 - \left(1 - \tfrac{\gamma(\alpha t, L\beta)}{\Gamma(\alpha t)}\right)^2\right] \cdot e^{-\lambda_{de}t} + \right.$$
$$\left.\sum_{k=1}^\infty \int_0^L \left[1 - \left(1 - \tfrac{\gamma(\alpha t,(L-y)\beta)}{\Gamma(\alpha t)}\right)^2\right] \frac{\rho^{k\xi} \cdot y^{k\xi-1} \cdot e^{-\rho y}}{\Gamma(k\xi)}dy \cdot \frac{e^{-\lambda_{de}t}(\lambda_{de}t)^k}{k!}\right\}dt \tag{14}$$

A proof-test will be executed at time τ. If the subsystem is functioning at τ with unknown degradation level, $\mathrm{PFD}_2(t)$ becomes the conditional probability of failure with $t > \tau$ given functioning by τ

$$\mathrm{PFD}_2(t) = \Pr[T < t|T > \tau, t > \tau] = 1 - \Pr[T < t|T > \tau, t > \tau]$$
$$= 1 - \frac{\Pr[T > t \cap T > \tau, t > \tau]}{\Pr[T > \tau]} = 1 - \frac{R(t)}{R(\tau)} \tag{15}$$

The $\mathrm{PFD}_{\mathrm{avg}}$ in the second test interval$(\tau,2\tau)$ is then:

$$\mathrm{PFD}_{\mathrm{avg}} = \tfrac{1}{\tau}\int_\tau^{2\tau} PFD_2(t)dt$$
$$= \tfrac{1}{\tau}\int_\tau^{2\tau}\left[1 - \tfrac{R(t)}{R(\tau)}\right]dt$$
$$= 1 - \tfrac{1}{\tau}\int_\tau^{2\tau} \tfrac{R(t)}{R(\tau)}dt \tag{16}$$

Similarly, if the subsystem is functioning in the i-th proof-test interval of $((i-1)\tau, i\tau)$, the $\mathrm{PFD}_i(t)$ can be calculated as:

$$\mathrm{PFD}_i(t) = \Pr[T < t|T > (i-1)\tau, t > (i-1)\tau]$$
$$= 1 - \Pr[T > t|T > (i-1)\tau, t > (i-1)\tau]$$
$$= 1 - \frac{\Pr[T > t \cap T > (i-1)\tau, t > (i-1)\tau]}{\Pr[T > (i-1)\tau]}$$
$$= 1 - \frac{R(t)}{R((i-1)\tau)} \tag{17}$$

In the i-th proof-test interval $((i-1)\tau, i\tau)$, $\mathrm{PFD}_{\mathrm{avg}}$ can be calculated as:

$$\mathrm{PFD}_{\mathrm{avg}} = \tfrac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \mathrm{PFD}_i(t)dt$$
$$= 1 - \tfrac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \tfrac{R(t)}{R((i-1)\tau)}dt \tag{18}$$

Based on the results above, it is still difficult to generate a straightforward expression of PFD(t) and $\mathrm{PFD}_{\mathrm{avg}}$. Therefore, in the rest of this paper, a numerical example is chosen to manifest differences between the proposed method and the existing ones.

4. Case studies

In this section, an example is given to illustrate the function of the proposed algorithm. We will compare the results based on the method in this paper and those from the widely used formulas for $\mathrm{PFD}_{\mathrm{avg}}$. We will also perform sensitivity analysis for the effects of parameters on $R(t)$ and $\mathrm{PFD}_{\mathrm{avg}}$. The three following variables will be evaluated: failure threshold L, demand rate λ_{de}, shape parameter ξ of demand damage.

4.1. Reference values from simplified formulas

In the simplified formulas in (Rausand and Arnljot, 2004), the subsystem is assumed as-good-as-new after each proof test. The units in a 1oo2 configuration have the same failure rate λ, and they are tested at the same time with an interval τ. The approximation formulas for the $\mathrm{PFD}_{\mathrm{avg}}$ of this 1oo2 configuration is

$$\mathrm{PFD}_{\mathrm{avg}}^{(1oo2)} \approx \tfrac{(\lambda\tau)^2}{3} \tag{19}$$

Table 2
Parameter values.

Parameter	Value
L	0.00125 (Tanner and Dugger, 2003)
λ_{de}	$2.5 \times 10^{-5}h^{-1}$
A	1.02×10^{-4}
B	1.2×10^4
Ξ	4.0
P	4×10^4
T	$8760h$

*h means hour.

The SIL requirement for a 1oo2 valve actuator subsystem in the IEC standard is SIL3 (IEC 61511, 2010). Following the corresponding values of $\mathrm{PFD}_{\mathrm{avg}}$ listed in Table 1, the upper and lower limits of $\mathrm{PFD}_{\mathrm{avg}}$ for SIL3 is 10^{-4} and 10^{-3}. Using Eq. (19), we can get the constant failure rate λ with $\tau = 8760$ is 2×10^{-6} and 6.25×10^{-6}, the maximum and minimum mean time to failure (MTTF) is 5×10^5 and 1.6×10^5, respectively. In other words, if the design of actuator can follow the requirement of SIL3, the maximum acceptable failure rate of each unit in the 1oo2 configuration is 6.25×10^{-6}.

The failure rate of LCP for valve is obtained from (Rausand, 2013) as 2.7×10^{-6}. These three failure rates will be used as reference values to validate the proposed degradation model.

The parameters of aging degradation and random demands are provided in Table 2, and then the two processes are simulated in Matlab R2018a.

To investigate the effect of damage caused by random demands on system, we compare two degradation modes: degradation only with the aging process, and degradation as the combination the aging and random demands.

Based on Eq. (11), under the combined effects of aging and demands, reliability of the 1oo2 configuration decreases along with time as plotted in Fig. 3.

In Fig. 3, it is easy to notice that $R(t)$ of the 1oo2 configuration only with the continuous process is overlapping with that subject to two processes by around 0.5×10^5. When the time in consideration is longer, random demands gradually have more obvious effects on degradation, with the reflection in Fig. 3 that $R(t)$ only with the continuous process is higher. The difference between two curves reflects the accumulating effect caused by random demands. With time going on, the effect of random demands is more obvious. If only the aging process is considered, reliability of the SIS will be overestimated and risk of EUC will be underestimated.

$\mathrm{PFD}_{\mathrm{avg}}$ values of the SIS in the two degradation modes are shown in Fig. 4.

It is easily noticed that there are much difference on $\mathrm{PFD}_{\mathrm{avg}}$ for the two degradation modes. For the degradation mode with two processes, the $\mathrm{PFD}_{\mathrm{avg}}$ of this 1oo2 configuration is not in the range of SIL3 anymore after 7τ. But if only considering the aging processes, this system can still meet the required SIL3 in the test interval $[9\tau,10\tau)$. Considering the safety requirement of EUC, the combined degradation processes could make the reliability and $\mathrm{PFD}_{\mathrm{avg}}$ more stricter than only aging process.

After the valves installation, their reliability and availability should be assessed through periodic and diagnostic tests. In order to meet the required SIL, it is necessary to maintain an accurate record not only operating time and proof test results but also the previous operation history. Considering the harsh operating environment, valves that report only on installation time may not be sufficient for assessing the status.

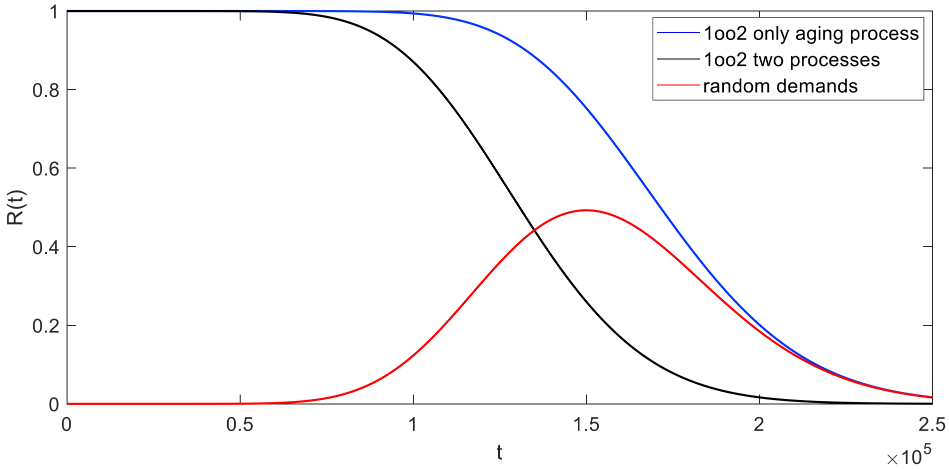


Fig. 3. Reliability of the 1oo2 configuration subject to aging degradation and random demands.

4.2. Sensitivity analysis of parameters

To investigate the effect of degradation process on the PFD$_{avg}$, several parameters will be discussed: i.e. threshold L, demand rate λ_{de}, and shape parameter ξ. Here, these three parameters are used to describe the working conditions of the 1oo2 configuration.

4.2.1. Effects of thresholds

Taking the LCP failure mode as an example, the maximum allowable leakage rate of a valve can act as a threshold for determining whether a failure occurs. The reflection of leakage rate on the valve is the depth of erosion and corrosion.

In practices, the maximum allowable depth is determined by several aspects. First of all, during the design stage, it is the property of material. Designers should choose more stable material for valves installed harsh working condition. Secondly, it is related with the leakage rate requirement. Therefore, the working condition should be considered during the selection and installation of the valve.

In this paper, the maximum value of depth under each specific scenario is assumed as the failure threshold L. Different threshold values are given under a constant demand rate $\lambda_{de} = 2.5 \times 10^{-5}$ per hour, and their effects on the reliability are shown in Fig. 5.

It can be found that $R(t)$ is not sensitive to L until t reaches a certain value around 0.5×10^5, meaning that the maximum depth values have slight effect on the system reliability at the beginning. The system stays with high reliability by this time, with no consideration about manufacturing error or failures, because the 1oo2 configuration has just experienced slight aging degradation and seldom demands have come. Along with longer time, the reliability decreases dramatically. By increasing thresholds L shifts from 0.00115 to 0.00155, namely releasing the requirement for acceptable leakage rate, $R(t)$ shifts to the right. Such a shift is from the loosing definition on the system functioning.

As seen in Fig. 5, the reliability profiles (solid lines) based on the proposed degradation model are totally different with those having constant failure rates (dashed lines). The hypothesis of a constant failure rate provides easier mathematical models to assess the performance of actuators. At the early stage, the method based on the constant failure rate (the dashed solid line) underestimates the reliability of system. The underestimation can bring unnecessary costs in SIS design and over protection in some degree. While more focus should be put on

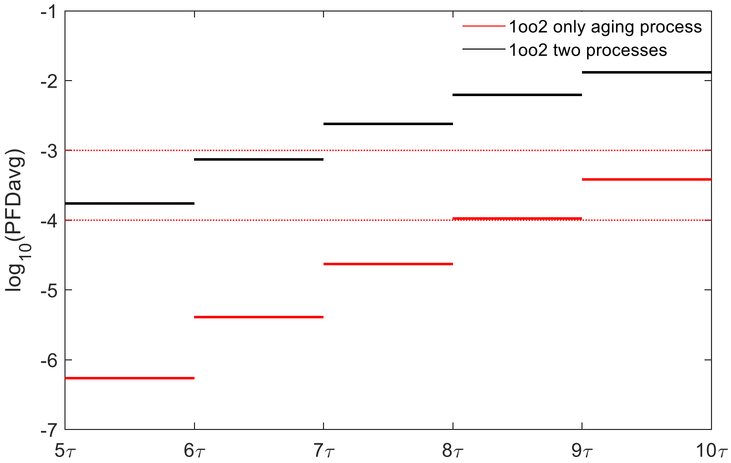


Fig. 4. PFD$_{avg}$ of the 1oo2 configuration subject to aging degradation and random demands.

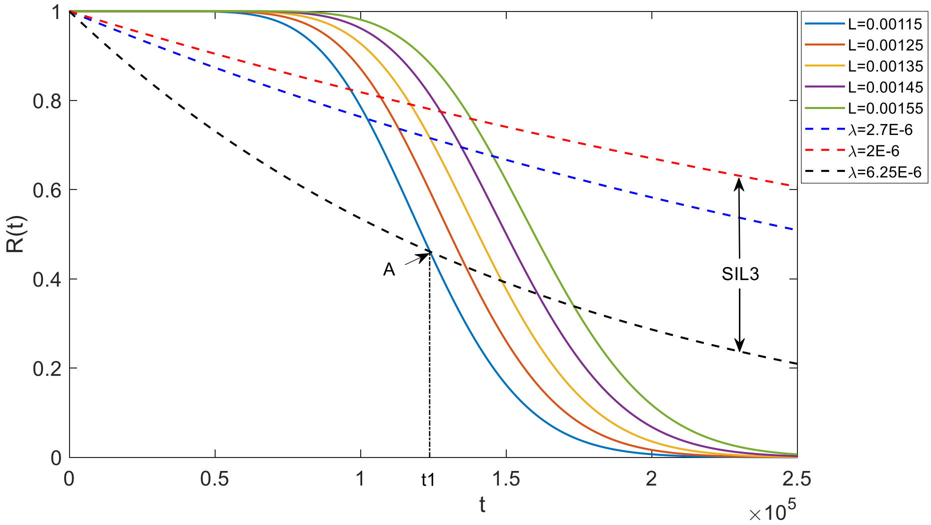


Fig. 5. Sensitivities of $R(t)$ on threshold L.

the period after a specific time point, e.g. the intersections of the dashed blue lines with the solid ones in Fig. 5, where the constant rate-based method overestimates the system reliability. In such contexts, even the SIS can be degraded at a high SIL, it actually cannot provide sufficient protection on EUC.

We can use MTTF to denote the system reliability and compare the results with different values of L and the constant failure rate.

$$\mathrm{MTTF} = E(T) = \int_0^\infty tf(t)dt \approx \int_0^\infty R(t)dt \tag{20}$$

Based on the configuration, we can firstly determine the minimum MTTF of a subsystem for SIL3 is 1.60×10^5. Then, it can be found in the table that when $L = 0.00155$, MTTF is within the range of SIL3. For the other settings of L, the subsystem only can comply with SIL2. Meanwhile, the higher threshold also means a higher tolerance for SIS which has a longer MTTF. From Table. 3, we can see that the integrity of SIS is partly dependent on how much the EUC can tolerate the rate of leakage. If the EUC is sensitive to leakage, we need to be more conservative in grading its SIS.

Meanwhile, the degradation analysis provide an opportunity to estimate the overhaul time for the SIS. Normally, if after testing we discovered an anomaly, we can schedule intervention, such as lubrication; On the contrary, if the valves is functional after each proof test, theoretically, we will not act on the valves. But when the reliability of valves has decreased considerably so it is risky to meet the safety requirement for possible demands. That is, the valves should be arranged with an overhaul time even if it has not given any symptoms of having a problem. When the calculated reliability under degradation cannot satisfy the requirement of SIL3, shown as point A. The overhaul time can be settled as time t_1 in Fig. 5. Similarly, considering different acceptable threshold, the overhaul time can be adjusted.

To illustrate the effects of threshold values on $\mathrm{PFD_{avg}}$, $\log_{10}$-scale on the y-axis is then adopted since it can present more details when the value of $\mathrm{PFD_{avg}}$ is rather small. $\mathrm{PFD_{avg}}$ is calculated for every interval $[(i-1)\tau, i\tau)$ based on the proposed formula (18). A numerical comparison of $\mathrm{PFD_{avg}}$ under different thresholds is shown in Fig. 6.

The system reliability $R(t)$ of different thresholds before $0.5 \times 10^5$is overlapping, that is, the $\mathrm{PFD_{avg}}$ is easily affected by the calculation accuracy given the property of gamma function. Hereby, $\mathrm{PFD_{avg}}$ during the test intervals $[5\tau,6\tau)$, $[6\tau,7\tau)$, $[7\tau,8\tau)$,$[8\tau,9\tau)$,$[9\tau,10\tau)$ are analyzed respectively. To compare with the results of reference value, $\mathrm{PFD_{avg}}$ calculated based on assumptions of constant failure rate ($\lambda = 2.7 \times 10^{-6}$) and as-good-as-new after proof-tests ($\tau = 8760$), is drawn in red dashed line in Fig. 6.

Generally speaking, the $\mathrm{PFD_{avg}}$ is decreasing with the threshold in the same test interval, e.g. SIL4 for $L = 0.00155$ in interval $[6\tau,7\tau)$, but SIL2 for $L = 0.00115$, with the same assumption that the valve is functioning at 6τ during the proof test. The $\mathrm{PFD_{avg}}$ for $L = 0.00115$ is almost 100 times higher for $L = 0.00155$. It means that the EUC with lower threshold of leakage is more risky. Meanwhile, in these test intervals, the increment of $\mathrm{PFD_{avg}}$ between two consecutive thresholds keeps more or less the same value in each test interval. It means that under the same operating environment (demand rate), the $\mathrm{PFD_{avg}}$ increments of the two consecutive thresholds are proportional to the difference between the thresholds, which is proved by the constant difference of MTTF between two consecutive thresholds in Table 3.

During these test intervals, for the same threshold L, $\mathrm{PFD_{avg}}$ is also increasing with time, e.g. SIL of L= 0.00155 from qualifying SIL4 in $[5\tau,6\tau)$ is released to SIL2 in $[9\tau,10\tau)$. Such a change manifests that the probability of the system failing to demand is increasing even it is functioning at each proof test. Namely, the assumption of as-good-as-new after each proof test is too optimistic for $\mathrm{PFD_{avg}}$. The valves are activated during the proof test, it only means that valves are functioning but unnecessary to be a total new state. Consequently, the periodic test policy is questionable and becoming insufficient to meet SIL requirement with time going by. This finding could be used as a rough guideline for proof test plans. For example, the $\mathrm{PFD_{avg}}$ when $L = 0.00125$ in interval $[6\tau,7\tau)$ is within SIL3, but for the latter interval $[7\tau,8\tau)$, the $\mathrm{PFD_{avg}}$ jumps to SIL2. In practical applications, the test intervals should be updated and shortened after 7τ rather than to keep $\tau = 8760$.

4.2.2. *Effects of demand rates*

Given the characteristics of low demand systems, they are required to be activated when a hazardous event occur. λ_{de} could be an indicator to describe the working condition of HIPPS.

In this subsection, we fix the failure threshold $L = 0.00125$, and observe $\mathrm{PFD_{avg}}$ of the 1oo2 configuration when the demand rate λ_{de} is set as different values as shown in Fig. 7.

$\mathrm{PFD_{avg}}$ acts as an effective measure for the low-demand system. The

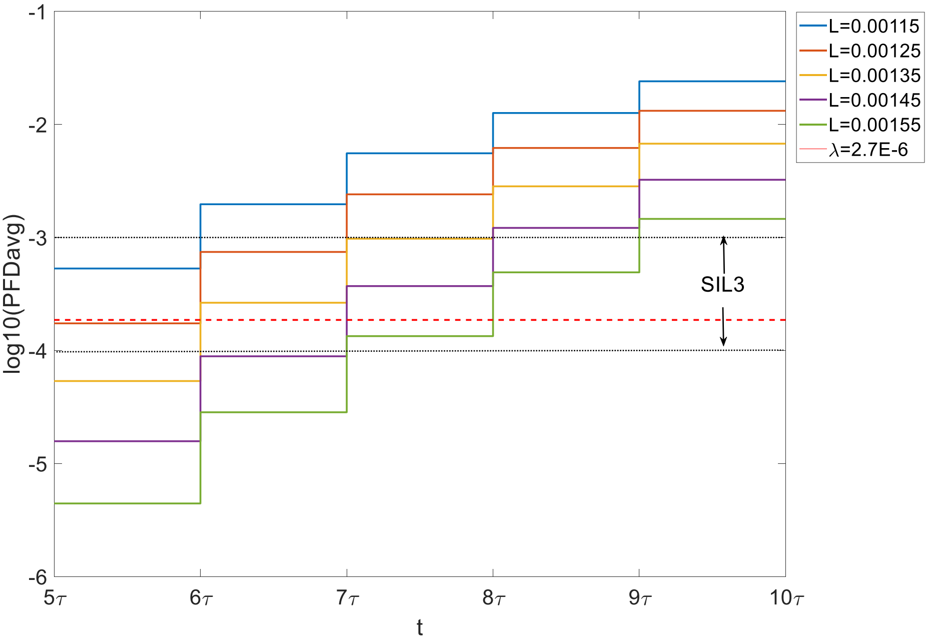


Fig. 6. Effects of threshold L on.PFD$_{\text{avg}}$.

Table 3
Estimated MTTF under different L.

Parameter	MTTF
$L = 0.00115$	1.23×10^5
$L = 0.00125$	1.32×10^5
$L = 0.00135$	1.42×10^5
$L = 0.00145$	1.52×10^5
$L = 0.00155$	1.61×10^5
Maximum MTTF for SIL3	1.60×10^5

boundary of high-and low-demands can be approximated as once per year when the proof test frequency is also once per year (Liu, 2014), so the maximum $\lambda_{de} = 1 \times 10^{-4}$ is chosen in this paper.

It is not so hard to imagine that the system reliability decreases when it is operating with higher arrival rates of random demands. The overall tendency is similar as in Fig. 5. No further discussion about system reliability here.

The effects of demand rate λ_{de} on PFD$_{\text{avg}}$ are shown in Fig. 7. Similarly to threshold L, in each test interval, the PFD$_{\text{avg}}$ is increasing with the demand rate λ_{de}. When the demand rate increase 10 times from $\lambda_{de} = 2.5 \times 10^{-6}$ to $\lambda_{de} = 2.5 \times 10^{-5}$, the PFD$_{\text{avg}}$ increases almost 100 times in [5τ,6τ). It is more than SIL4 under $\lambda_{de} = 2.5 \times 10^{-6}$, while, up to SIL1 under $\lambda_{de} = 1 \times 10^{-4}$ which is far from the required SIL3. It means the valves are less reliable when they are installed in higher demand rate circumstance. In a higher demand rate working condition, the 1oo2 configuration is easier to get the damage from random demands. The accumulated damage increase the overall degradation which make the valves are more fragile for the upcoming demands.

Under the same λ_{de}, the PFD$_{\text{avg}}$ of 1oo2 configuration is increasing with time. In order to meet SIL3, the test interval $\tau = 8760$ is enough until 7τ under the demand rate $\lambda_{de} = 2.5 \times 10^{-5}$. From [7$\tau$,8$\tau$) on, it is out of the range of SIL3 but in SIL2 or higher instead. To meet the performance requirement, the proof test interval should be shorter than $\tau = 8760$ after 7τ in this example.

Compared to the threshold L, the demand rate has a more obvious effect on PFD$_{\text{avg}}$. When the valves are installed in a higher demand context, the SIL could beyond the safety requirement even in the early stage. These effects should attract the attentions of maintenance crews. More stricter proof tests and maintenance should be arranged for higher demand rate operating environment. After each demand, therefore, the basic visual check or simple maintenance should be followed to ensure safety. Similar to threshold L, λ_{de} is worth being taken into account when determining the overhaul time of the SIS. When demand rate is higher, it suffers more damages from demands, which requires earlier services.

4.2.3. *Effects of the shape parameter of demands*

As another key parameter of the working condition, the demand damage size on system should be discussed in this section. This parameter could be linked with the pressure in EUC. As assumed in 2.3, the size of damage by each random demand follows a gamma distribution with parameters (ξ_i, ρ), while the shape parameter ξ is the contributor for damage size under the same scale parameter ρ. Since the sum of k damages also follows gamma distribution with parameters ($\sum_{i=1}^{k} \xi_i$, ρ), the shape parameter can be estimated as $k\xi$when assume these demands have same shape parameter ξ. In the sensitivity analysis, different shape parameter values are given under a constant demand rate $\lambda_{de} = 2.5 \times 10^{-5}$ per hour and threshold $L = 0.00125$.

The effects of shape parameter ξ on PFD$_{\text{avg}}$ is shown in Fig. 8. For each of ξ, PFD$_{\text{avg}}$ increases with time. Meanwhile, PFD$_{\text{avg}}$ has a positive relationship with shape parameter ξ of demand. With the higher value of shape parameter of demand ξ, PFD$_{\text{avg}}$ increases in same test interval, e.g. it is following SIL4 for $\xi = 2$, and only following SIL3 for $\xi = 4$ in [5τ,6τ). This phenomena means that the average unavailability increases with higher average damage size under same demand rate. If the HIPPS is installed in the severe pressure condition, it is becoming more risky for the upcoming demands. The possible solution is to choose the higher tolerance equipment for more severe working

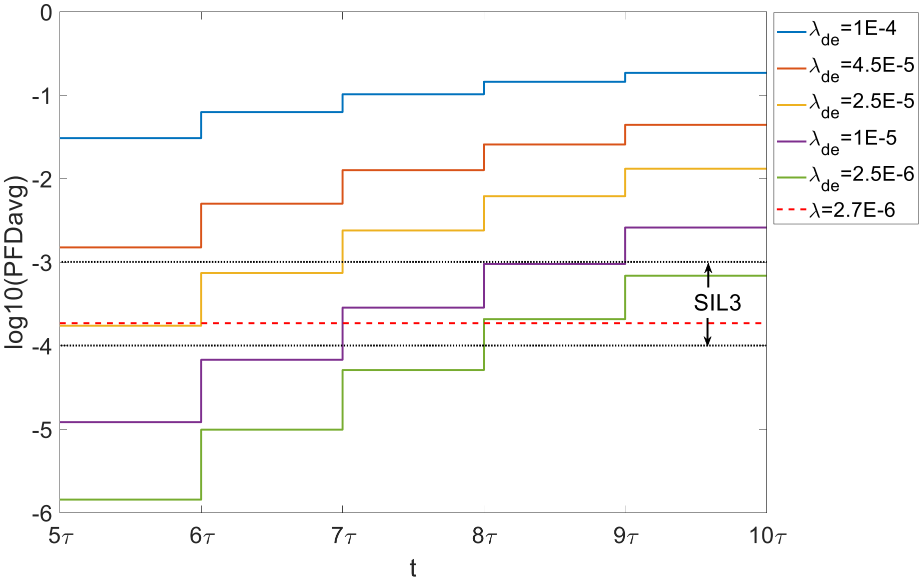


Fig. 7. Effects of demand rates λ_{de} on $\mathrm{PFD}_{\mathrm{avg}}$.

condition. Another way is to execute preventive maintenance after demands.

4.3. Updating the test intervals

Having considered the degradation, it is interesting to consider the length of test intervals. Given that degradation has been found influential on the decision-making for testing strategies, the most constraint is the SIL level to be followed. Normally, the EUC system will shutdown for the proof test of SISs. The shutdown and re-operation of EUC will cause an economic loss. In order to avoid unnecessary loss, the minimum proof test frequency should be settled. Here, we are going to discuss the first 6 test interval under different threshold L to get the different time dates.

In this example, such a 1oo2 SIS needs to meet SIL3. Here, we take different thresholds L in Fig. 9 as an example. Values of the two variables are at first set as $\lambda_{\mathrm{de}} = 2.5 \times 10^{-5}$, and $\xi = 4$ respectively. Similar to Eq. (18), we can connect reliability and average PFD in a test interval

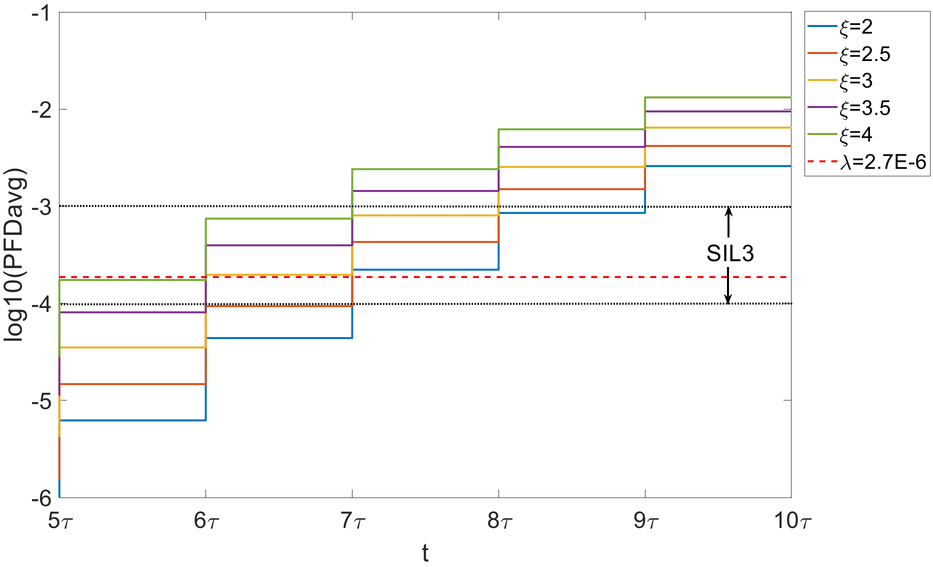


Fig. 8. Sensitivities of PFD_{avg} on shape parameter ξ of demands.

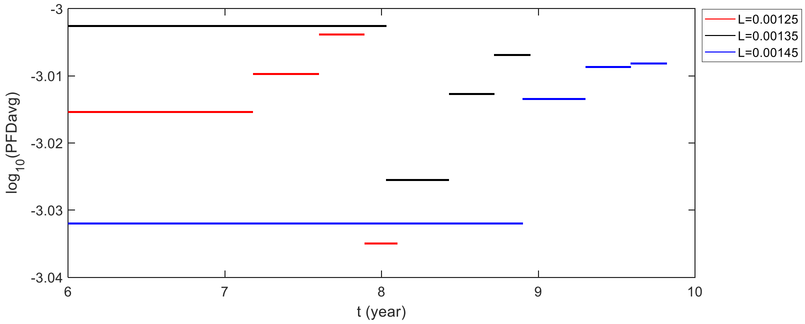


Fig. 9. Updated test interval under SIL3.

$$\text{PFD}_{\text{avg}} = 1 - \frac{1}{t - t_0}\int_{t_0}^{t} \frac{R(u)}{R(t_0)}du \qquad (21)$$

The idea is to calculate time t when PFD_{avg} is in the range of $[10^{-4}, 10^{-3})$ given functional at time t_0, where $R(u)$ is changing with time as in Eq. (11).

Here, we take the $\tau = 8760h$ (1 year) as time unit. In order to keep safety, 3 years is set as the maximum length of the proof-test interval (Hauge and Lundteigen, 2008). For the first test interval $[0,3\tau)$, the SIL is much higher than SIL4. As for the second interval $[3\tau, 6\tau)$, the values of $\log_{10}\text{PFD}_{\text{avg}}$ under thresholds are -3.99, -4.53 and -5.09, respectively, which satisfying SIL3. It means, for first two test intervals, 3-year interval is sufficient to keep the 1oo2 configuration to meet SIL3.

Considering the proposed degradation process, Eq. (21) is used to calculate the proof test time. Results of the updated test dates after the first two intervals are shown in Fig. 9. The exact values of the each test time point are shown in Table 4.

It can be found that the length of test interval is becoming shorter and shorter, decreasing from 3 to 0.2 years. The test interval is longer under the higher threshold L. For example, the 3rd test interval for $L = 0.00145$ is almost 3 years, while only around 1 year for $L = 0.00125$. Different test interval should be adopted for SISs under different working conditions.

But, it is worth mentioning that the values in Table 4 are calculated only based on the assumption of functioning at the previous proof test without considering any other factors.

In practices, the following factors should be considered in updating proof test intervals for a certain SIL requirement:

- Test quality: In order to estimate the performance accurately, the potential leakage rate should be detected perfectly in proof tests. Considering the errors of tests, the calculated PFD_{avg} with a confidence interval should be used to estimate the test interval.
- Maintenance: Since no maintenance work is considered in this example, we regard the system same no matter 0 leakage is existing or the leakage rate is close to the threshold. In practices, when the leakage rate is approaching threshold, preventive maintenance can be conducted to stop or at least slow down the degradation. After preventive maintenance, the reliability of system can be supposed to improved, the test interval should be lengthened.
- Partial tests: The length of test interval refers to the full proof test, but partial proof tests can be introduced between two full proof tests. The efficient partial test can collect the performance information which will reduce possible damages on the actuators. According to the result of partial tests, the full proof test interval could be adjusted.

Table 4
Updated test interval under different L based on SIL3.

Parameter	3rd	4th	5th	6th
$L = 0.00125$	6τ, 7.18τ	7.18τ, 7.6τ	7.6τ, 7.89τ	7.89τ, 8.1τ
$L = 0.00135$	6τ, 8.03τ	8.03τ, 8.43τ	8.43τ, 8.72τ	8.72τ, 8.95τ
$L = 0.00145$	6τ, 8.9τ	8.9τ, 9.3τ	9.5τ, 9.59τ	9.59τ, 9.82τ

*$\tau = 8760$ h = 1 year.

5. Conclusions

In order to evaluate the effects of aging and demands effects on SISs, this paper has presented a degradation-based approach for performance analysis of 1oo2 actuators of SISs. The model is developed taking account a continuous aging process and random demands on individual units. Considering the dependency of two units due to same demands, reliability algorithm for the 1oo2 subsystem has been proposed, and the approximation formulas for $R(t)$ and PFD_{avg} of the subsystem have been developed.

A numerical example is given to illustrate usefulness of the proposed models. Sensitivity analyses are conducted to examine the effects of failure threshold, demand rate and shape parameter PFD_{avg}. Based on the operational assumption at each test date, we found that the conditional PFD_{avg} is increasing with time under the assumption of functional in proof tests. PFD_{avg} is negatively related with the value of failure thresholds L and positively with demand rate λ_{de} and shape parameter ξ.

According to the results of sensitivity analysis, we propose to adjust proof test intervals based on the testing results. Flexible proof test intervals could be settled rather than keep them fixed. At the early stage of the system, the reliability of SIS is high, and so the proof test interval could be settled longer based on the unavailability acceptable criteria, to reduce operational costs. With time goes by, the length of proof test interval should be shorter to ensure safety.

This paper focuses on the calculation of $R(t)$ and PFD_{avg} of a 1oo2 SIS without considering maintenance work. One extension of the current work is to take maintenance work for restoration into consideration, since system resilience has been regarded as significant measure (Cai et al., 2018; Feng et al., 2019; Ren et al., 2019). Another extension is to study the general $KooN$ architecture in SIS. Dependency of a common number of shocks, $N(t)$ and dependency due to impact of each demand on all among components will be studied separately and reported later.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.jlp.2019.103946.

References

Bocchetti, D., Giorgio, M., Guida, M., Pulcini, G., 2009. A competing risk model for the reliability of cylinder liners in marine diesel engines. Reliab. Eng. Syst. Saf. 94, 1299–1307.

Cai, B., Xie, M., Liu, Y., Liu, Y., Feng, Q., 2018. Availability-based engineering resilience metric and its corresponding evaluation methodology. Reliab. Eng. Syst. Saf. 172, 216–224.

Catelani, M., Ciani, L., Luongo, V., 2011. A simplified procedure for the analysis of safety instrumented systems in the process industry application. Microelectron. Reliab. 51, 1503–1507.

Chebila, M., Innal, F., 2015. Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH. J. Loss Prev. Process. Ind. 34, 167–176.

Chen, N., Ye, Z.-S., Xiang, Y., Zhang, L., 2015. Condition-based maintenance using the inverse Gaussian degradation model. Eur. J. Oper. Res. 243, 190–199.

Deloux, E., Castanier, B., Bérenguer, C., 2009. Predictive maintenance policy for a gradually deteriorating system subject to stress. Reliab. Eng. Syst. Saf. 94, 418–431.

Feng, Q., Fan, D., Cai, B., Liu, Y., Ren, Y., et al., 2019. Resilience design method based on meta-structure: a case study of offshore wind farm. Reliab. Eng. Syst. Saf. 186, 232–244.

Frangopol, D.M., Kallen, M.-J., Van Noortwijk, J.M., 2004. Probabilistic models for life-cycle performance of deteriorating structures: review and future directions. Prog. Struct. Eng. Mater. 6, 197–212.

Gebraeel, N., Elwany, A., Pan, J., 2009. Residual life predictions in the absence of prior degradation knowledge. IEEE Trans. Reliab. 58, 106–117.

Guo, H., Yang, X., 2008. Automatic creation of markov models for reliability assessment of safety instrumented systems. Reliab. Eng. Syst. Saf. 93, 829–837.

Hauge, S., Lundteigen, M.A., 2008. Guidelines for Follow-Up of Safety Instrumented Systems (SIS) in the Operating Phase. Technical Report SINTEF A8788 SINTEF NO-7465, Trondheim, NORWAY.

Hauge, S., Hokstad, P., Håbrekke, S., Lundteigen, M.A., 2016. Common cause failures in safety-instrumented systems: using field experience from the petroleum industry. Reliab. Eng. Syst. Saf. 151, 34–45.

IEC 61508, 2010. Functional Safety of Electrical/electronic/programmable Electronic Safety-Related Systems. pp. 1–7 part.

IEC 61511, 2003. Functional Safety-Safety Instrumented Systems for the Process Industry Sector.

Innal, F., Lundteigen, M.A., Liu, Y., Barros, A., 2016. PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase markov models. Reliab. Eng. Syst. Saf. 150, 160–170.

Jin, H., Rausand, M., 2014. Reliability of safety-instrumented systems subject to partial testing and common-cause failures. Reliab. Eng. Syst. Saf. 121, 146–151.

Kallen, M., van Noortwijk, J., 2005. Optimal maintenance decisions under imperfect inspection. Reliab. Eng. Syst. Saf. 90, 177–185.

Kharoufeh, J.P., Cox, S.M., 2005. Stochastic models for degradation-based reliability. IIE Trans. 37, 533–542.

Klutke, G., Yang, Y., 2002. The availability of inspected systems subject to shocks and graceful degradation. IEEE Trans. Reliab. 51, 371–374.

Lai, M., Chen, S., 2016. A bivariate optimal replacement policy with cumulative repair cost limit under cumulative damage model. Sādhanā 41, 497–505.

Lawless, J., Crowder, M., 2004. Covariates and random effects in a gamma process model with application to degradation and failure. Lifetime Data Anal. 10, 213–227.

Li, W., Pham, H., 2005a. An inspection-maintenance model for systems with multiple competing processes. IEEE Trans. Reliab. 54, 318–327.

Li, W., Pham, H., 2005b. Reliability modeling of multi-state degraded systems with multi-competing failures and random shocks. IEEE Trans. Reliab. 54, 297–303.

Lin, Y., Li, Y., Zio, E., 2015. Integrating random shocks into multi-state physics models of degradation processes for component reliability assessment. IEEE Trans. Reliab. 64, 154–166.

Liu, Y., 2014. Discrimination of low-and high-demand modes of safety-instrumented systems based on probability of failure on demand adaptability. Proc. Inst. Mech. Eng. O J. Risk Reliab. 228, 409–418.

Liu, Y., Rausand, M., 2011. Reliability assessment of safety instrumented systems subject to different demand modes. J. Loss Prev. Process. Ind. 24, 49–56.

Liu, H., Yeh, R., Cai, B., 2017. Reliability modeling for dependent competing failure processes of damage self-healing systems. Comput. Ind. Eng. 105, 55–62.

Marszal, E.M., Mitchell, K.J., 2004. Justifying the use of high integrity pressure protection systems (HIPPS). In: ASME/JSME 2004 Pressure Vessels and Piping Conference. American Society of Mechanical Engineers, pp. 207–212.

Mechri, W., Simon, C., BenOthman, K., 2015. Switching Markov chains for a holistic modeling of sis unavailability. Reliab. Eng. Syst. Saf. 133, 212–222.

Mercier, S., Bordes, L., Remy, E., Dautrême, E., 2013. A stochastic model for competing degradations. In: Proceedings of the 22nd ESREL Conference.

Nakagawa, T., 2007. Shock and Damage Models in Reliability Theory. Springer Science & Business Media.

Nawaz, C.M.Z., 2008. What Are the Effects of Changing the Test Interval of Land Based Safety Critical Valves in Hydrocarbon Transport Systems. Master's thesis. University of Stavanger, Norway.

Rafiee, K., Feng, Q., Coit, D.W., 2014. Reliability modeling for dependent competing failure processes with changing degradation rate. IIE Trans. 46, 483–496.

Rafiee, K., Feng, Q., Coit, D.W., 2017. Reliability assessment of competing risks with generalized mixed shock models. Reliab. Eng. Syst. Saf. 159, 1–11.

Rausand, M., 2013. Risk Assessment: Theory, Methods, and Applications. John Wiley & Sons.

Rausand, M., 2014. Reliability of Safety-Critical Systems: Theory and Applications. John Wiley & Sons.

Rausand, M., Arnljot, H., 2004. System Reliability Theory: Models, Statistical Methods, and Applications, vol. 396 John Wiley & Sons.

Ren, Y., Fan, D., Feng, Q., Wang, Z., Sun, B., Yang, D., 2019. Agent-based restoration approach for reliability with load balancing on smart grids. Appl. Energy 249, 46–57.

Rogova, E., Lodewijks, G., Lundteigen, M.A., 2017. Analytical formulas of PFD and PFH calculation for systems with nonconstant failure rates. Proc. Inst. Mech. Eng. O J. Risk Reliab. 231, 373–382.

Singpurwalla, N.D., 1995. Survival in dynamic environments. Stat. Sci. 86–103.

Song, S., Coit, D.W., Feng, Q., 2014. Reliability for systems of degrading components with distinct component shock sets. Reliab. Eng. Syst. Saf. 132, 115–124.

Song, X., Zhai, Z., Liu, Y., Han, J., 2018. A stochastic approach for the reliability evaluation of multi-state systems with dependent components. Reliab. Eng. Syst. Saf. 170, 257–266.

Sun, B., Yan, M., Feng, Q., Li, Y., Ren, Y., Zhou, K., Zhang, W., 2018. Gamma degradation process and accelerated model combined reliability analysis method for rubber o-rings. IEEE Access 6, 10581–10590.

Tang, S., Guo, X., Yu, C., Xue, H., Zhou, Z., 2014. Accelerated degradation tests modeling based on the nonlinear wiener process with random effects. Math. Probl. Eng. *2014*.

Tanner, D.M., Dugger, M.T., 2003. Wear mechanisms in a reliability methodology. In: Reliability, Testing, and Characterization of MEMS/MOEMS II, vol. 4980. International Society for Optics and Photonics, pp. 22–41.

Technical Note 101 ( ). Valve Alignment Troubleshooting. Valco Instruments Co. Inc.

Van Noortwijk, J., 2009. A survey of the application of gamma processes in maintenance. Reliab. Eng. Syst. Saf. 94, 2–21.

Wang, H., Xu, T., Mi, Q., 2015. Lifetime prediction based on gamma processes from accelerated degradation data. Chin. J. Aeronaut. 28, 172–179.

Wu, S., Zhang, L., Lundteigen, M.A., Liu, Y., Zheng, W., 2018. Reliability assessment for final elements of SISs with time dependent failures. J. Loss Prev. Process. Ind. 51, 186–199.

Xu, A., Shen, L., Wang, B., Tang, Y., 2018. On modeling bivariate wiener degradation process. IEEE Trans. Reliab. 67, 897–906.

Ye, Z., Xie, M., 2015. Stochastic modelling and analysis of degradation for highly reliable products. Appl. Stoch Model Bus. Ind. 31, 16–32.

Ye, Z., Chen, N., Shen, Y., 2015. A new class of wiener process models for degradation analysis. Reliab. Eng. Syst. Saf. 139, 58–67.

Zhang, Z., Hu, C., Si, X., Zhang, J., Shi, Q., 2017. A prognostic approach for systems subject to wiener degradation process with cumulative-type random shocks. In: Data Driven Control and Learning Systems (DDCLS), 2017 6th. IEEE, pp. 694–698.

Zhou, Y., Ma, L., Mathew, J., 2008. A Non-gaussian Continuous State Space Model for Asset Degradation. Springer.

Zio, E., 2016. Some challenges and opportunities in reliability engineering. IEEE Trans. Reliab. 65, 1769–1782.

Article III

Zhang, A., Liu, Y., Barros, A., & Kassa, E. (2019). A degrading element of safety-instrumented systems with combined maintenance strategy. In Proceedings of the 29th European Safety and Reliability Conference (ESREL). September 22-26, 2019, Hannover, Germany. Research Publishing Services.

A degrading element of safety-instrumented systems with combined maintenance strategy

Aibo Zhang, Yiliu Liu, Anne Barros, Elias Kassa

Norwegian University of science and technology, Trondheim, Norway. E-mail: aibo.zhang@ntnu.no, yiliu.liu@ntnu.no, anne.barros@ntnu.no, elias kassa@ntnu.no

Safety-instrumented systems (SISs) are widely used to prevent hazardous events. The mechanical actuator subsystem in a SIS can become more vulnerable with time due to progressive degradation mechanisms, such as erosion, corrosion and wear-out etc. Such kind of phenomenon challenges the assumption of constant failure rates or exponentially distributed lifetime that the existing reliability analysis depends on. This study aims to assess the performance of the actuator of a SIS subject to a continuous degradation, which will be modeled by homogeneous gamma process. Periodic tests with the interval τ are executed to check the subsystem state. A combining maintenance strategy including corrective maintenances (CMs) and imperfect preventive maintenances (PMs) will be adapted according to the state, which can be evaluated by actual degradation level. Given that maintenances are triggered only at inspection dates, the actuator can experience downtime in cases of failures. The expected downtime in each test interval will be used to estimate the average unavailability of the SIS. A numerical example is shown that the average unavailability of such a SIS sub-system is changing with time rather than keeping as a constant value.

Keywords: Safety-instrumented system, degrading actuating element, gamma process, imperfect preventive maintenance, $\mathrm{PFD_{avg}}$, Monte Carlo simulation.

1. Introduction

Safety instrumented systems (SISs), which generally consist of sensor-, logic solver- and actuator-subsystems, are widely used in different industries to prevent the occurrences of hazardous events or mitigate their consequences (Rausand (2014)). The examples of SISs include fire prevention systems and railway signaling systems. These systems are designed to perform some specific safety-instrumented functions (SIFs) to protect the equipment under control (EUC) (Rausand and Høyland (2004)).

For the SISs in the low-demand operational mode, they are normally in a dormant state and are only activated when a demand/hazardous event in EUC occurs (with a frequency lower than once per year). Faults of these SISs may therefore remain hidden until proof tests or real demands (Rausand (2014)).

Reliability assessment of SISs has drawn many attentions recently. The average probability of failure on demand ($\mathrm{PFD_{avg}}$) is the common-used measure for the reliability of SISs in the low-demand (IEC 61508 (2010)). Most of the existing studies is based on the assumption that SISs and their sub-systems have constant failure rates (Guo and Yang (2008); Liu and Rausand (2011); Catelani et al. (2011); Jin and Rausand (2014)), but it is doubtful when it is applied on those mechanical items.

In fact, many actuator sub-systems of SISs, such as emergency shutdown (ESD) valves, are rather vulnerable to degradation processes(Wu et al. (2018)). Many mechanisms, including erosion, corrosion, and cracks etc, can lead the reliability and performance of mechanical units to degrade with time (Zio (2016)). Once the degradation reaches a predefined level, the actuator subsystem will be in a failed state. One example is the failure mode "Leakage (through the valve) in closed position (LCP)" in process industries. A likely cause of this failure mode is a progressive failure mechanism — erosion in the gate sealing area (Rausand (2014)). After a failure, the valve "Cannot prevent leakage (through the valve) in closed position. Such a failure is dangerous undetected (DU), meaning that it cannot be revealed by autumatic disgnostis, and it can be a main contributor to the loss of the functionality of a SIS.

Unavoidable progressive failure mechanisms challenge the assumption for constant failure rate. The aging process is also challenging the assumption of as-good-as-new after each proof test. Actually, if no failure is revealed in a proof test, it only means that the SIS in a functioning state, but not necessarily as-good-as-new.

To keep the performance of SIS in accordance with the required, associated maintenance work is also executed with proof tests. Preventive maintenance, such as lubrication and calibration, can not make an element work to perfectly as a new one. Given the limitations of cost or production,

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio
Copyright © 2019 European Safety and Reliability Association.
Published by Research Publishing, Singapore.
ISBN: 978-981-11-2724-3; doi:10.3850/978-981-11-2724-3_0490-cd

it is unrealistic to execute corrective maintenance after each proof test. Considering aforementioned factors, $\mathrm{PFD_{avg}}$ should be different in different testing interval, rather than keep as a constant value.

With the development of sensor technologies, more practice performance information considering operating condition could be collected in periodic proof tests. An efficient way for reliability modeling of SISs is to utilize the degradation information to estimate the health condition of the system (Ye and Xie (2015)). Based on these concerns, a growing attention is given to predict degradation of SISs and offer suitable maintenance in advance to ensure the barrier adequacy.

Given that maintenance actions are conducted only at test dates, a mechanical SIS sub-system can still experience downtime. This paper will consider the combined maintenance strategy of a SIS subject to a continuous-time random deterioration, simulate its operations and calculate $\mathrm{PFD_{avg}}$, and monitor the subsystem through perfect periodic proof tests.

The remainder of this article is arranged as follows. Section 2 describes problem statement in terms of definitions and model assumptions. Section 3 states the basic knowledge of Monte Carlo Simulation and flow chart of simulation process. In section 4, analytical formulas of downtime and $\mathrm{PFD_{avg}}$ in each test interval are derived. Finally, section 5 presents conclusions.

2. System description and assumptions

2.1. *Performance assessment*

ESD valves, are used to perform one or more safety functions, such as closing or opening to provide over-pressure protection. The functionality of ESD valves plays a basis of risk level of EUC. The main failure modes of ESD valves includes:

- Valve fails to close on demand
- Valve fails to close with the specified time
- It leaks in a closed position

The required performance assessment of ESD is performed into three steps (Nawaz (2008)):

- To identify and illustrate the function of valve
- To explain the effects on safety of the above failure modes
- To classify acceptable/unacceptable level of specific performance indicator, like leakage rate or closing time

The performance criteria for the ESD, e.g. internal leakage rate and closing time, should be a target value with deviation (Rausand (2014)). Ideally leakage rate of the valve should be 0 kg/s, but there is an acceptable and unacceptable deviation based on practical consideration , like 0.05 kg/s and 0.1kg/s, respectively (Nawaz (2008)). Meanwhile, these performance indicators should be related with the working condition, like acceptable leakage rates for the onshore and offshore plants could be different. The main reason for this is due to the difference of human risk exposure.

From the view of safety, acceptable and unacceptable level of performance indicator could be employed as guidelines for maintenance. Corrective maintenance should be executed when the performance indicator exceeds the unacceptable level. When the indicator is higher than acceptable level, preventive maintenance, like lubrication, should be done.

2.2. *Definitions of states and maintenance policy*

Consider a single valve that subject to aging degradation process. When the erosion in the gate sealing area exceeds a predefined threshold, the external performance during proof test is the leakage rate through higher than the unacceptable level. It means that the valve will not implement its function when emergency occurs. If the leakage rate is higher than acceptable level but lower than unacceptable level, then the valve could still satisfy safety function but with degraded performance. From this viewpoint, the valve has three states, shown in Table 1.

Table 1. States and description of one unit

State	Status	State description
0	working	The unit is functioning as specified
1	degraded	The unit has a degraded performance
2	failed	The unit has a failed fault

Given the limitations of maintenance cost and production loss, combined maintenance strategy are taken to keep the performance of the unit. The state of the system is perfectly known at test point $\tau, 2\tau \cdots$. The failed state will remain hidden between two proof test. If the indicator is lower than acceptable level, no maintenance is required. Once the performance indicator is beyond acceptable level, preventive maintenance is executed. Due to continuous aging degradation, preventive maintenance could not make the unit ‘as-good-as-new’. Once the performance indicator is beyond unacceptable level, corrective maintenance is executed. The failed unit will be replaced by a new one. The time spent in test and maintenance is assumed to be negligible. The proof test is perfect to get information.

Therefore, three value are of interests in this analysis: unacceptable level, acceptable level and the value of degradation level after preventive maintenance. In this paper, we use the following values:

- L: unacceptable level (failure threshold)
- $\omega_a \times L$: acceptable level (preventive maintenance threshold)
- $\omega_b \times L$: the result of imperfect preventive maintenance
  ($\omega_b < \omega_a < 1$, both ω_a and ω_b are constant values.)

Given that maintenance actions are triggered only at test dates, the unit can still experience downtime.

The combined maintenance strategy and degradation process is shown in Fig. 1. Where there are two imperfect preventive maintenance at times 2τ and 3τ and one corrective maintenance at time 5τ. Meanwhile, there is a hidden unavailability period between 4τ and 5τ.

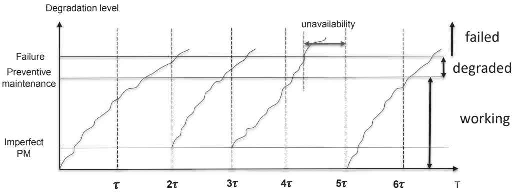


Fig. 1. The combined maintenance strategy

For low-demand system, PFD_{avg} is the average probability of the item in SIS is not able to perform its specified safety function if a demand occur (IEC 61508 (2010); Rausand (2014)). It means that with test interval τ and the expected downtime $E[D(\tau)]$, PFD_{avg} can be expressed as:

$$\text{PFD}_{\text{avg}} = \frac{E[D(\tau)]}{\tau} \tag{1}$$

SISs are designed to protect EUC given a specific safety integrity level (SIL). To fulfill the performance requirement for a certain SIL, a SIS in the low-demand mode must have an PFD_{avg} in the corresponding interval, as illustrated in

Table 2. SILs for low-demand SISs

SIL	PFD_{avg}
SIL 4	$10^{-5}$to 10^{-4}
SIL 3	$10^{-4}$to 10^{-3}
SIL 2	$10^{-3}$to 10^{-2}
SIL 1	$10^{-2}$to 10^{-1}

The objective of this paper is to estimate the downtime in each test interval based on the proposed model and use the expected downtime to estimate PFD_{avg}. The main purpose is to check the value of PFD_{avg} with time.

2.3. *Assumptions*

In the following analysis, common assumptions have been made:

- The final element starts working at time $t = 0$, and it is subject to a continuous degradation process. In this paper, we assume that the degradation process follows a homogeneous Gamma process with shape parameter $\alpha > 0$ and scale parameter β.
- The failure mode is a hidden failure and only could be detected by proof tests or demands. The downtime should be calculated from the arrival time of failed state to next proof test.
- The unit is tested periodically with interval τ to check its state. Tests are assumed to be instantaneous, perfect and non-destructive.
- If the unit is in failed state at a test, corrective maintenance will be executed to replace the failed unit with a new one and the degradation level equals to 0.
- If the unit is in a degraded state at a test, which means degradation level is over than preventive threshold $\omega_a \times L$ but less than failure threshold L, imperfect preventive maintenance will be executed on the same unit and degradation level equals to $\omega_b \times L$.
- If the unit is in working state which degradation level is less than $\omega_a \times L$, no maintenance work will be executed.
- The time spent in repair is negligible.

3. Monte Carlo Simulation

A number of papers are available regarding the use of Monte Carlo methods to solve reliability, availability, maintainability and safety (RAMS) problems Barata et al. (2002); Malefaki et al. (2016); Wang et al. (2017); Nadjafi et al. (2017); Lin et al. (2018).

Monte Carlo Simulation is based on generation of random events to obtain the probability distributions for the variables of the problem, thus estimating the future performance of systems (Santos et al. (2018)).

Monte Carlo Simulation will be employed to simulate the continuous aging process and estimate the PFD_{avg} in each test interval under combined maintenance strategy.

3.1. *Simulation process*

Let $S(t) = 0, 1, 2$ represent the state set of unit at time t, where state $0, 1$ and 2 represent working, degraded and failed state, respectively. The quantities χ_i^s for $s = 1, 2$, which can be interpreted as the arrival time to state s in i-th test interval $((i-1)\tau, i\tau)$. Considering the arrival time of state 2 and test time points, $U(i) = i\tau - \chi_i^2$ is the downtime in i-th test interval for this unit. So, the $\overline{\mathrm{PFD}^{\mathrm{i}}_{\mathrm{avg}}}$ in i-th test interval can be estimated by the average value of $\widetilde{\mathrm{PFD}^{\mathrm{i}}_{\mathrm{avg}}}$

$$\overline{\mathrm{PFD}^{\mathrm{i}}_{\mathrm{avg}}} = \frac{1}{N}\sum_{i=1}^{N}(\frac{U(i)}{\tau})_j = \frac{1}{N}\sum_{i=1}^{N}(\frac{i\tau - \chi_i^2}{\tau})_j \tag{2}$$

where $(U(i)/\tau)_j$ stands $\mathrm{PFD}_{\mathrm{avg}}$ of j-th degradation path in i-th test interval.

The followings are simulation procedures of degradation process.

(i) Define the initial parameters of degradation model;
(ii) According to PDF of gamma process, direct sampling method is used to generate the degradation increment of time step Δt. Sum of increment of Δt will be regarded as total degradation of this unit. If total degradation exceeds failure threshold L, arrival time of state 2 will be recorded.
(iii) Periodic tests are executed. According to total degradation at tests time, in simulation, the values will be updated based on assumptions in Section 2.3. After test and associated maintenance work, the simulation process will restart from step (ii).
(iv) Save $U(i) = i\tau - \chi_i^2$ in i-th test interval.
(v) Repeat the whole process for N times and calculate average value $\overline{\mathrm{PFD}^{\mathrm{i}}_{\mathrm{avg}}}$.

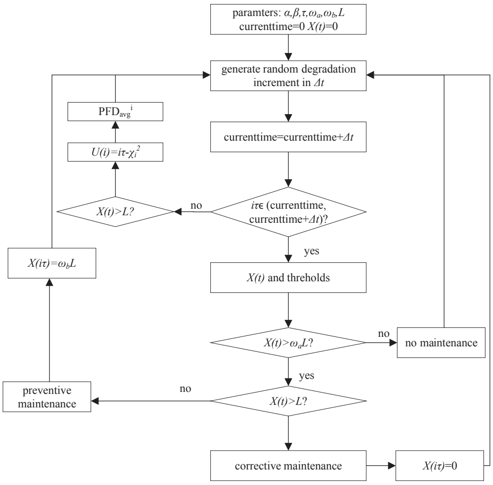


Fig. 2. Flow chart of Monte Carlo Simulation

3.2. *Numerical example*

The parameters of aging degradation and maintenance thresholds are provided in Table 3. The process is simulated in Matlab R2018a.

Table 3. Parameter value

parameter	value
L	0.00125
α	1.12×10^{-4}
β	8×10^{-5}
τ	$8760h$
ω_a	0.8
ω_b	0.1

*: h means hour

The simulation result of $\mathrm{PFD}_{\mathrm{avg}}$ is shown in Table 4.

Table 4. Simulation result of $\mathrm{PFD}_{\mathrm{avg}}$

test interval	PFDavg	PFDavg	PFDavg	PFDavg
	(N=50000)	(N=100000)	(N=200000)	(N=300000)
1	0	0	0	0
2	0	0	0	0
3	0	0	9.08E-06	4.16E-06
4	7.48E-06	1.32E-05	3.02E-06	1.43E-05
5	1.99E-05	5.19E-05	5.37E-05	5.55E-05
6	1.64E-04	8.98E-05	1.00E-04	1.09E-04
7	2.53E-04	2.82E-04	2.90E-04	2.61E-04
8	4.01E-04	4.64E-04	4.44E-04	4.64E-04
9	6.64E-04	6.68E-04	6.80E-04	7.04E-04
10	9.77E-04	1.08E-03	9.40E-04	9.64E-04
11	1.46E-03	1.24E-03	1.28E-03	1.29E-03
12	1.54E-03	1.56E-03	1.54E-03	1.37E-03
13	1.58E-03	1.65E-03	1.71E-03	1.53E-03
14	1.39E-03	1.64E-03	1.59E-03	1.57E-03
15	1.31E-03	1.57E-03	1.54E-03	1.60E-03
16	1.23E-03	1.29E-03	1.37E-03	1.32E-03
17	1.34E-03	1.19E-03	1.20E-03	1.16E-03
18	1.08E-03	1.07E-03	1.10E-03	1.03E-03
19	9.77E-04	9.30E-04	8.83E-04	9.81E-04
20	1.097E-03	1.01E-03	1.01E-03	9.01E-04

The estimated $\overline{\mathrm{PFD}^{\mathrm{i}}_{\mathrm{avg}}}$ is 0 for early several test intervals. This is because of low occurrence of failure in those test intervals. It means that neglecting incipient production failures, the final is high reliable at the beginning.

During simulation test intervals, it is obvious that $\mathrm{PFD}_{\mathrm{avg}}$ is changing, generally, increasing with time. Such a change that the probability of the final element failing to demand is increasing.

For the first 10 intervals, the SIL of this unit can at least satisfy SIL3. From the 11-th interval, the $\mathrm{PFD}_{\mathrm{avg}}$ is in the range of SIL3.

Based on this simulation result, if only considering SIS unavailability acceptable (e.g. SIL3), a possible solution is to extend the proof test intervals at the beginning according to the change of $\mathrm{PFD}_{\mathrm{avg}}$.

To investigate the effects of degradation parameters on $\mathrm{PFD}_{\mathrm{avg}}$, parameter ω_a is simulated following a set of value $\omega_a = [0.6, 0.8, 1]$ with $\omega_b = 0.1$. The simulation result is shown in Table 5.

Table 5. Simulation result of $\mathrm{PFD}_{\mathrm{avg}}$ under different parameter ω_a(N=50000)

test interval	PFDavg (ω_a=0.6)	PFDavg (ω_a=0.8)	PFDavg (ω_a=1)
1	0	0	0
2	0	0	0
3	0	0	8.88E-06
4	2.96E-05	7.48E-06	2.15E-05
5	2.92E-06	1.99E-05	1.11E-04
6	7.80E-06	1.64E-04	5.06E-04
7	4.51E-05	2.53E-04	1.25E-03
8	8.23E-05	4.01E-04	3.04E-03
9	5.11E-05	6.64E-04	5.34E-03
10	3.56E-05	9.77E-04	9.54E-03
11	5.62E-05	1.46E-03	1.56E-02
12	6.78E-05	1.54E-03	2.37E-02
13	4.77E-05	1.58E-03	3.07E-02
14	2.12E-05	1.39E-03	3.95E-02
15	8.53E-05	1.31E-03	4.44E-02
16	6.08E-05	1.23E-03	4.86E-02
17	4.13E-05	1.34E-03	4.83E-02
18	4.66E-05	1.08E-03	4.56E-02
19	5.38E-05	9.77E-04	4.26E-02
20	7.88E-05	1.097E-03	3.66E-02

The effects of ω_a on $\mathrm{PFD}_{\mathrm{avg}}$ is shown in Fig. 3 From Table 5 and Fig. 3, it is obvious that the $\mathrm{PFD}_{\mathrm{avg}}$ has a direct relationship with parameter ω_a.

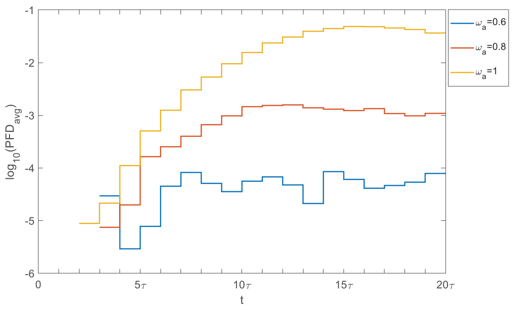


Fig. 3. Effects of ω_a on $\mathrm{PFD}_{\mathrm{avg}}$

If $\omega_a = 0.6$, it means that the acceptance criterion is more strict. $\mathrm{PFD}_{\mathrm{avg}}$ is more than SIL4 in each test interval, it means the unit is high reliable. Meanwhile, the proof tests and maintenance normally require shutdown the EUC (Rausand (2014)). The significant consequences include increased EUC risks during shutdown and restart operations, and the associated economic loss.

If $\omega_a = 1$, it means that there is no preventive maintenance, the unit will only be replaced once failed. The values of $\mathrm{PFD}_{\mathrm{avg}}$ in each test interval are increasing with time and exceed the required SIL3 at some time point.

It is a trade-off between SIL and the preventive maintenance parameter ω_a. The best solution is to reduce the unnecessary preventive maintenance and periodic tests but keep $\mathrm{PFD}_{\mathrm{avg}}$ in the required range of SIL.

Another vital parameter of maintenance decision is the parameter ω_b. A set value of parameter ω_b is $\omega_b = [0, 0.1, 0.4]$ with $\omega_a = 0.8$. The effect of parameter ω_b on $\mathrm{PFD}_{\mathrm{avg}}$ is shown in Table 6 and Fig. 4.

Table 6. Simulation result of $\mathrm{PFD}_{\mathrm{avg}}$ under different parameter ω_b(N=50000)

test interval	PFDavg (ω_b=0)	PFDavg (ω_b=0.1)	PFDavg (ω_b=0.4)
1	0	0	0
2	0	0	0
3	0	0	0
4	3.08E-06	7.48E-06	9.16E-06
5	7.88E-05	1.99E-05	4.66E-05
6	8.12E-05	1.64E-04	1.12E-04
7	2.95E-04	2.53E-04	2.22E-04
8	5.17E-04	4.01E-04	5.29E-04
9	7.95E-04	6.64E-04	8.27E-04
10	8.82E-04	9.77E-04	9.71E-04
11	1.38E-03	1.46E-03	1.41E-03
12	1.58E-03	1.54E-03	1.49E-03
13	1.40E-03	1.58E-03	1.57E-03
14	1.57E-03	1.39E-03	2.03E-03
15	1.52E-03	1.31E-03	1.99E-03
16	1.44E-03	1.23E-03	1.81E-03
17	9.55E-04	1.34E-03	1.97E-03
18	8.47E-04	1.08E-03	2.03E-03
19	9.46E-04	9.77E-04	2.11E-03
20	8.88E-04	1.097E-03	1.62E-03

For $\omega_b = 0$, it means that the preventive maintenance policy is also prefect and as-good-as-new. The tendency of $\mathrm{PFD}_{\mathrm{avg}}$ is increasing first and decreasing later with time. The main possible reason is the action of preventive maintenance. For some degradation paths, it reaches the preventive maintenance threshold $\omega_a \times L$ at certain test interval and start a new cycle.

For $\omega_b = 0.4$, it means that degradation level

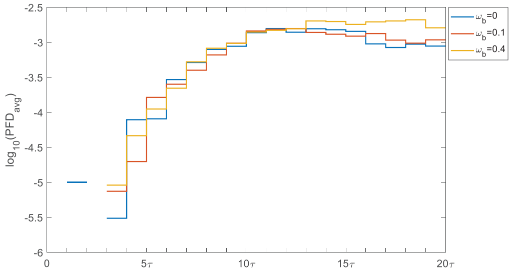


Fig. 4. Effects of ω_b on $\mathrm{PFD}_{\mathrm{avg}}$

of this unit decrease to 40% of failure threshold. Using the preventive maintenance policy, we can keep $\mathrm{PFD}_{\mathrm{avg}}$ with the SIL range more possibly. In contrast to the parameters ω_a, the frequency of preventive maintenance is going up with higher value of ω_b. But the effect on $\mathrm{PFD}_{\mathrm{avg}}$ is not so obvious compared to $\omega_b = 0.1$.

Since both maintenance policy parameter ω_a and ω_b have the direct relationship with the $\mathrm{PFD}_{\mathrm{avg}}$, the further work is to find the optimal solution of (ω_a, ω_b) given specific SIL. But no further discussion for this topic in this paper.

4. Analytical formulas

There are lots of similar preventive and corrective threshold-based maintenance policy for continuous/periodic monitored with gamma degradation process (Castanier et al. (2005); Deloux et al. (2009); Fouladirad and Grall (2011); Mercier and Pham (2012, 2014); Zhu et al. (2015); Zhao et al. (2018); Huynh et al. (2018)). In most of existing preventive maintenance policies, the result of preventive maintenance is as-good-as-new. However,imperfect preventive maintenance for deteriorating systems has not received much attention.

The main objective of analytical formulas is to validate the $\mathrm{PFD}_{\mathrm{avg}}$ result from Monte Carlo simulation in Section 3.

Let $X(t)$ be the stochastic process of the maintained unit. $X(t)$ is a homogeneous Gamma process with the following characteristics:

- $X_0 = 0$;
- $X(t)$ has independent increments;
- For the period from s to t,$s < t$, the new degradation $X(t) - X(s)$ follows a Gamma density with shape parameter $\alpha(t-s)$ and scale parameter β.

$$f_{\alpha(t-s),\beta}(x) = \frac{\beta^{\alpha(t-s)} x^{\alpha(t-s)-1} e^{-\beta x}}{\Gamma(\alpha(t-s))} \tag{3}$$

- The mean and variance of $X(t)$ are $\alpha t/\beta$ and $\alpha t/\beta^2$, respectively.

As is shown in Dieulle et al. (2001, 2003); Mercier and Pham (2014), $X(t)$ describing the evolution of the system is a semi-regenerative process with semi-regeneration times being the proof test time $i\tau$.

After inspection $i\tau$, the future evolution of unit depends only on its state at time $i\tau$. Based on the maintenance rule, the unit state is necessarily below the preventive maintenance threshold $\omega_a \times L$ after PM or CM.So, the sequence $X_{i\tau}$ is a Markov chain with continuous state $[0, \omega_a \times L]$.

According to assumptions, there are two possible scenarios for unit at inspection time τ:

- The unit is in degraded state and repaired imperfectly with deterioration level $\omega_b \times L$;
- The unit is left as it is.

Assume that the initial degradation state of a component is equal to x, the first scenario happens with the probability

$$Pr(X_{\tau^-} > \omega_a \times L \mid x) = \overline{F_\tau}(\omega_a \times L - x) \tag{4}$$

As for the second scenario, it means that degradation level of the unit at time τ is $x + X_\tau$, with $x + X_\tau < \omega_a \times L$.

It is also proved in Dieulle et al. (2001, 2003); Mercier and Pham (2014), the transition probability density function of the Markov chain X_τ is given by

$$\begin{aligned} Pr(dy \mid x) = {} & \overline{F_\tau}(\omega_a \times L - x)\delta_0(dy) \\ & + f_\tau(y - x)\mathbf{1}_{x \leqslant y < \omega_a \times L} dy \end{aligned} \tag{5}$$

where δ_0 is a Dirac mass function.

Considering that the unit starts from $X_0 = 0$, for the first test interval, the probability of total degradation $X(t)$ at time t is higher than L, $\overline{F_t}(L)$, can be derived as:

$$\begin{aligned} \overline{F_t}(L) &= Pr\{X(t) > L\} \\ &= \int_L^{+\infty} f_{X(t)}(z) dz = \frac{\Gamma(\alpha t, L\beta)}{\Gamma(\alpha t)} \end{aligned} \tag{6}$$

Where Γ denotes the complete Gamma function defined as

$$\Gamma(\alpha, x) = \int_x^{+\infty} z^{\alpha-1} e^{-z} dz, \alpha > 0 \tag{7}$$

So, the expected downtime in first interval with $x = 0$ is

$$\begin{aligned} U(0, (0, t)) &= E(\int_0^t Pr(X_u \geqslant L) du) \\ &= \int_0^t \frac{\Gamma(\alpha u, L\beta)}{\Gamma(\alpha u)} du \end{aligned} \tag{8}$$

The $\mathrm{PFD}^1_{\mathrm{avg}}$ in the first test interval can be calculated by

$$\mathrm{PFD}^1_{\mathrm{avg}} = \frac{U(0, (0, \tau))}{\tau} \tag{9}$$

From the property of independent increments of gamma process, for second test interval $(\tau, 2\tau)$, the calculation of expected downtime is conditioning on degradation level y at time τ.

$$
\begin{aligned}
&U(0,(\tau,t)) = E(\int_{\tau}^{t} Pr(X_u \geqslant L \mid X_\tau)du) \\
&= \int_{0}^{t-\tau} Pr(X_u \geqslant L \mid y)duP(dy \mid x) \\
&= \int U(y,(0,t-\tau))Pr(dy \mid x) \\
&= \int U(\omega_b L,(0,t-\tau))\overline{F_\tau}(\omega_a \times L)\delta_0(dy) \\
&+ \int U(y,(0,t-\tau))f_\tau(y)\mathbf{1}_{x \leqslant y < \omega_a \times L}dy
\end{aligned}
\tag{10}
$$

The $\mathrm{PFD}^2_{\mathrm{avg}}$ in second test interval can be calculated by

$$\mathrm{PFD}^2_{\mathrm{avg}} = \frac{U(0,(\tau,2\tau))}{\tau} \tag{11}$$

Similarly, the expected downtime in i-th test interval $((i-1)\tau, i\tau)$ is

$$
\begin{aligned}
&U(0,((i-1)\tau,t)) = E(\int_{(i-1)\tau}^{t} P_0(X_u \geqslant L)du) \\
&= E(\int_{(i-1)\tau}^{t} P_r(X_u \geqslant L \mid X_{(i-1)\tau})du)
\end{aligned}
\tag{12}
$$

Then, we can get the PFD^i_{avg} is

$$\mathrm{PFD}^{\mathrm{i}}_{\mathrm{avg}} = \frac{U(0,((i-1)\tau,i\tau))}{\tau} \tag{13}$$

The calculation results based on formulas are shown in Table 7. The results are also assumed increment in each test interval. All results in each test interval are very close.

Table 7. Simulation result of $\mathrm{PFD}_{\mathrm{avg}}$

test interval	formulas	PFDavg (N=300000)
1	3.98E-08	0
2	3.02E-07	0
3	4.13E-06	4.16E-06
4	1.42E-05	1.43E-05
5	5.53E-05	5.55E-05
6	1.07E-04	1.09E-04
7	2.59E-04	2.61E-04
8	4.62E-04	4.64E-04
9	7.06E-04	7.04E-04
10	9.63E-04	9.64E-04
11	1.31E-03	1.29E-03
12	1.38E-03	1.37E-03
13	1.52E-03	1.53E-03
14	1.55E-03	1.57E-03
15	1.51E-03	1.60E-03
16	1.30E-03	1.32E-03
17	1.22E-03	1.16E-03
18	1.07E-03	1.03E-03
19	9.43E-04	9.81E-04
20	1.00E-03	9.01E-04

5. Conclusion

We here consider a degrading final element with combined corrective maintenance and imperfect preventive maintenance strategy. We propose the model to link $\mathrm{PFD}_{\mathrm{avg}}$ with stochastic degradation process. These findings challenge the existing assumption of as-good-as-new and constant value of $\mathrm{PFD}_{\mathrm{avg}}$ in each test interval.

The $\mathrm{PFD}_{\mathrm{avg}}$ is calculated by the expected downtime, rather than failure rate. The results clearly show that the $\mathrm{PFD}_{\mathrm{avg}}$ could be linked with degradation parameters and is changing with time, generally, increasing with time. Given the maintenance work, from 11th test interval, $\mathrm{PFD}_{\mathrm{avg}}$ is becoming stable and mostly in a specific SIL3. For $\mathrm{PFD}_{\mathrm{avg}}$ in the range of SIL4, we can adjust the test interval to reduce the necessary tests. Both degradation threshold parameter ω_a and the result parameter ω_b have the direct relationship with the $\mathrm{PFD}_{\mathrm{avg}}$.

As mentioned before, the choice of the test interval and of the coefficient ω_a and ω_b value will obviously influence the cost of maintenance. Studies on the maintenance optimization will be reported in the future.

References

Barata, J., C. G. Soares, M. Marseguerra, and E. Zio (2002). Simulation modelling of repairable multi-component deteriorating systems for on conditionmaintenance optimisation. *Reliability Engineering & System Safety 76*(3), 255–264.

Castanier, B., A. Grall, and C. Bérenguer (2005). A condition-based maintenance policy with non-periodic inspections for a two-unit series system. *Reliability Engineering & System Safety 87*(1), 109–120.

Catelani, M., L. Ciani, and V. Luongo (2011). A simplified procedure for the analysis of safety instrumented systems in the process industry application. *Microelectronics Reliability 51*(9-11), 1503–1507.

Deloux, E., B. Castanier, and C. Bérenguer (2009). Predictive maintenance policy for a gradually deteriorating system subject to stress. *Reliability Engineering & System Safety 94*(2), 418–431.

Dieulle, L., C. Berenguer, A. Grall, and M. Roussignol (2001). Continuous time predictive maintenance scheduling for a deteriorating system. In *Annual Reliability and Maintainability Symposium. 2001 Proceedings. International Symposium on Product Quality and Integrity (Cat. No. 01CH37179)*, pp. 150–155. IEEE.

Dieulle, L., C. Bérenguer, A. Grall, and M. Roussignol (2003). Sequential condition-based maintenance scheduling for a deteriorating system. *European Journal of operational research 150*(2), 451–461.

Fouladirad, M. and A. Grall (2011). Condition-based maintenance for a system subject to a non-homogeneous wear process with a wear rate transition. *Reliability Engineering & System Safety 96*(6), 611–618.

Guo, H. and X. Yang (2008). Automatic creation of markov models for reliability assessment of safety instrumented systems. *Reliability Engineering & System Safety 93*(6), 829–837.

Huynh, K. T., I. T. Castro, A. Barros, and C. Bérenguer (2012). Modeling age-based maintenance strategies with minimal repairs for systems subject to competing failure modes due to degradation and shocks. *European journal of operational research 218*(1), 140–151.

Huynh, K. T., A. Grall, and C. Bérenguer (2018). A parametric predictive maintenance decision-making framework considering improved system health prognosis precision. *IEEE Transactions on Reliability* (99), 1–22.

IEC 61508 (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems. part 1-7.

Jin, H. and M. Rausand (2014). Reliability of safety-instrumented systems subject to partial testing and common-cause failures. *Reliability Engineering & System Safety 121*, 146–151.

Lin, Y.-H., Y.-F. Li, and E. Zio (2018). A comparison between monte carlo simulation and finite-volume scheme for reliability assessment of multi-state physics systems. *Reliability Engineering & System Safety 174*, 1–11.

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.

Malefaki, S., V. P. Koutras, and A. N. Platis (2016). Multi-state deteriorating system dependability with maintenance using monte carlo simulation. In *2016 Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (SMRLO)*, pp. 61–70. IEEE.

Mercier, S. and H. H. Pham (2012). A preventive maintenance policy for a continuously monitored system with correlated wear indicators. *European Journal of Operational Research 222*(2), 263–272.

Mercier, S. and H. H. Pham (2014). A condition-based imperfect replacement policy for a periodically inspected system with two dependent wear indicators. *Applied Stochastic Models in Business and Industry 30*(6), 766–782.

Nadjafi, M., M. A. Farsi, and H. Jabbari (2017). Reliability analysis of multi-state emergency detection system using simulation approach based on fuzzy failure rate. *International Journal of System Assurance Engineering and Management 8*(3), 532–541.

Nawaz, C. M. Z. (2008). What are the effects of changing the test interval of land based safety critical valves in hydrocarbon transport systems. Master's thesis, University of Stavanger, Norway.

Rausand, M. (2014). *Reliability of safety-critical systems: theory and applications*. John Wiley & Sons.

Rausand, M. and A. Høyland (2004). *System reliability theory: models, statistical methods, and applications*, Volume 396. John Wiley & Sons.

Santos, F., J. Villanueva, R. Gouveia, and J. Silva (2018). Method of monte carlo simulation for the analysis of uncertainty for ultrasonic time-of-flight. In *Journal of Physics: Conference Series*, Volume 1044, pp. 012045. IOP Publishing.

Wang, W., F. Di Maio, and E. Zio (2017). Three-loop monte carlo simulation approach to multi-state physics modeling for system reliability assessment. *Reliability Engineering & System Safety 167*, 276–289.

Wu, S., L. Zhang, M. A. Lundteigen, Y. Liu, and W. Zheng (2018). Reliability assessment for final elements of siss with time dependent failures. *Journal of Loss Prevention in the Process Industries 51*, 186–199.

Ye, Z.-S. and M. Xie (2015). Stochastic modelling and analysis of degradation for highly reliable products. *Applied Stochastic Models in Business and Industry 31*(1), 16–32.

Zhao, X., S. He, Z. He, and M. Xie (2018). Optimal condition-based maintenance policy with delay for systems subject to competing failures under continuous monitoring. *Computers & Industrial Engineering 124*, 535–544.

Zhu, W., M. Fouladirad, and C. Bérenguer (2015). Condition-based maintenance policies for a combined wear and shock deterioration model with covariates. *Computers & Industrial Engineering 85*, 268–283.

Zio, E. (2016). Some challenges and opportunities in reliability engineering. *IEEE Transactions on Reliability 65*(4), 1769–1782.

Article IV

Zhang, A., Zhang, T., Barros, A., & Liu, Y. (2020). Optimization of maintenances following proof tests for the final element of a safety-instrumented system. Reliability Engineering & System Safety, 196, 106779.

Reliability Engineering and System Safety 196 (2020) 106779

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Optimization of maintenances following proof tests for the final element of a safety-instrumented system

Aibo Zhang[a], Tieling Zhang[b], Anne Barros[a,c], Yiliu Liu[a,*]

[a] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway
[b] School of Mechanical, Materials, Mechatronic and Biomedical Engineering, University of Wollongong, Wollongong, NSW 2522, Australia
[c] CentraleSupelec, Paris Saclay University, France

ARTICLE INFO

Keywords:
Safety-instrumented system
Final element
Degradation
Preventive maintenance
Maintenance strategy
PFD_{avg}

ABSTRACT

Safety-instrumented systems (SISs) have been widely installed to prevent accidental events and mitigate their consequences. Mechanical final elements of SISs often become vulnerable with time due to degradations, but the particulars in SIS operations and assessment impede the adaption of state-of-art research results on maintenances into this domain. This paper models the degradation of SIS final element as a stochastic process. Based on the observed information during a proof test, it is essential to determine an optimal maintenance strategy by choosing a preventive maintenance (PM) or corrective maintenance (CM), as well deciding what degree of mitigation of degradation is enough in case of a PM. When the reasonable initiation situation of a PM and the optimal maintenance degree are identified, lifetime cost of the final element can be minimized while keeping satisfying the integrity level requirement for the SIS. A numerical example is introduced to illustrate how the presenting methods are used to examine the effects of maintenance strategies on cost and the average probability of failure on demands (PFD_{avg}) of a SIS. Intervals of the upcoming tests thus can be updated to provide maintenance crews with more clues on cost-effective tests without weakening safety.

1. Introduction

Considering production safety and environment protection, many safety-instrumented systems (SISs) have been employed in different industries. For example, on an offshore oil and gas production platform, emergency shutdown (ESD) systems are installed to protect the facility in case of an undesired event. Normally, a SIS, like the ESD system, consists of sensor(s) (e.g. pressure transmitters), logic solver(s) and final element(s) (shutdown valves) [1]. The final element performs one or more safety-instrumented functions (SIFs), by closing itself down to stop the gas flow in a pipeline if an emergency occurs in production. The facility protected by the ESD system is called equipment under control (EUC) in this context.

An ESD system is a typical SIS operating in a low demand mode, where the activation frequency is less than once per year in general. The final elements of such a SIS are mainly in a dormant state unless there is a proof test or a real shock on the equipment being protected by the SIS, or equipment under control (EUC) [1]. Therefore, some failure modes of final elements will stay hidden until the time to be activated. These hidden failures are called dangerous undetected (DU) if they can result in serious accidents. The average probability of failures on demands (PFD_{avg}) is a common-used measure in the evaluation of unavailability of SISs in the low demand mode [2], and DU failures are the main contributors for PFD_{avg}. In IEC standards, the value of PFD_{avg} will be used to determine the safety integrity level (SIL) of a SIS.

Many researches have paid attention to the calculation of PFD_{avg}, using: simplified formulas [1,3], Markov methods [4–7] and Petri Nets [8–10]. Common for most of these methods is the assumption of constant failure rates of all elements in a SIS. In practices, such an assumption is always valid for electronic components, but its validity for mechanical components is in question.

Mechanical components, such as many final elements of SISs, including shutdown valves, are operated in harsh conditions, and they are rather vulnerable to creeping or other degradation processes [11]. Thus, their failure rates, namely the conditional probability of failure in the next short time period, always increase with time. Several authors have assessed unavailability of SISs in consideration of non-constant failure rate [11,12]. Meanwhile, several dynamic reliability method, e.g. multiphase Markov process, have been applied to SISs for reliability assessment [5,13–16]. Their findings show that PFD_{avg} is changing with time and becomes different from one proof test interval to the next. The changing PFD_{avg} makes the updating of proof test interval necessary

[*] Corresponding author.
E-mail address: yiliu.liu@ntnu.no (Y. Liu).

https://doi.org/10.1016/j.ress.2019.106779
Received 2 August 2019; Received in revised form 29 October 2019; Accepted 22 December 2019
Available online 23 December 2019
0951-8320/ © 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/).

based on the requirement from SILs.

With the development of sensor technologies, more data about operation conditions and system degradation status can be collected in periodic proof tests. Information about degradation is helpful for the assessment of system performance [17]. Numerous parameters, such as lubricant ingredient, corrosion extent and so on, can be measured and utilized for failure prediction and diagnosis [18]. When any deviation from the normal, or early-phase signal of failure is identified, the upcoming tests and following maintenance actions need to be re-scheduled.

In terms of the final elements of an ESD, they can suffer several failure mechanisms, including erosion, corrosion, cracks etc., which can lead the capacity of performing safety functions to degrade with time [19]. For example, closing time on demand is an indicator of the performance of a shutdown valve. Once degradation of the valve reaches a certain level, the final element will be in a faulty/failed state. Such a DU failure will be hidden until a proof test identifies that closure of the valve needs too much time.

However, even though the shutdown valve is qualified in a proof test, the final element may be not as-good-as-new. Namely, the closing time is under the acceptable maximum value, but it is still longer than that when the SIS is just put into operation. As-good-as-new after each proof test is the extension of the constant failure rate assumption, meaning that $\mathrm{PFD}_{\mathrm{avg}}$ remains a fixed value in each test interval [20]. Since, the unavoidable gradual degradation of mechanical components challenges the constant failure rate assumption, the unavailability of final element should be supposed to increase by time.

In the simple calculation of $\mathrm{PFD}_{\mathrm{avg}}$, more frequent proof tests are regarded to lower risks, but some practical issues can weaken such a conclusion. If a proof test of SISs fully stops the process, or complete a whole trip of shutdown, stoppage and restart of the process will cause production loss, especially in offshore engineering and facilities [1]. In addition, such a whole shutdown trip may damage the valve (e.g. wear of the valve seat area) in some degree due to high stress level [11,21]. Hence, it is reasonable to consider how to utilize given proof test information to schedule future tests more effectively (e.g. to avoid unnecessary tests), while keeping the SIS availability meeting in the required level.

With the observation in a proof test of a shutdown valve, three options of follow-ups are possible: (1) No action if the valve in test is working well; (2) preventive maintenance (PM) if a certain degradation has been identified; (3) repair or replacement of the valve if it is failed. Repair/replacement can be regarded as perfect, leading the SIS to work as-good-as-new. For a PM, degradation of the valve can be mitigated but not be eliminated, so that the probability of failure by the next test is reduced. The mitigation degree can be naturally assumed positively correlated with the resources and time spent in the PM, namely the cost of PM. However, it is challenging to decide what is the optimal degree of PM that can balance the cost and the SIS availability. In addition, questions exist in the level of degradation initiating a PM. In other words, when closing time of a valve is a bit longer than the design value, a decision needs to be made whether the degradation can be ignorable, or some actions should be taken immediately. Ignoring means to take more risks to EUC, but actions are costly especially when they are not needed.

It should be noticed that even though many studies on maintenance optimization with degradation have been conducted, they are not naturally suitable for SIS final elements. As aforementioned, failures and degradations of SISs are hidden and only can be observed periodically. Decision-making on maintenances is not based on instantaneous availability but should be based on the estimation of system performance in the next test interval. In addition, to comply with international standards, the effects of maintenances should be connected with the average unavailability of a SIS in a period ($\mathrm{PFD}_{\mathrm{avg}}$) and should always be a strict constraint when making any testing and maintenance strategies. Considering those maintenance models for renewal systems having some similarities with SISs, they assume perfect PM or CM [22–26] and focus on the average long-run cost rate [27–29]. However, for SISs, the total cost in the designed service time (e.g. 20 years) is more of interest, and perfect PMs are often not practical or necessary.

Therefore, the main objective of this paper is to deal with both the challenges by degradation to SIS assessment and the challenges by SISs to maintenance optimization, to identify the optimal PM strategies of a SIS. Specifically, the optimal combination of the two threshold values of a SIS final element is in search: the degree of degradation initiating a PM (ω_a), and the degree of degradation where completing of this PM (ω_b) can be acceptable.

The remainder of this paper is organized as follows: Section 2 explains how a SIS final element operates and what are the assumptions in the analysis; Section 3 investigates the calculation of instantaneous unavailability of SIS, $\mathrm{PFD}_{\mathrm{avg}}$ and expected cumulative maintenance cost; Section 4 discusses the optimal values of two thresholds PMs based on the minimum expected cost and the SIL requirement respectively; Section 5 illustrates a method to update the test interval and conclusions are in Section 6.

2. Descriptions of safety-instrumented systems

2.1. System states and performance requirements

Without losing generality, we use an ESD system to study behaviors and operations of SISs. The ESD system is designed to maintain or achieve the EUC in a safe state, e.g. a normal pressure in process. One of main SIFs of an ESD valve is to cut off the flow when the high pressure occurs. To keep the risk of EUC within acceptable level, the valve is designed with a specific closing time, for example, 12 s. The actual performance requirement for this valve is, normally, the designed target value with acceptable deviations, e.g. 3 s. It means that the valve is considered to be functioning (with respect to this particular function) as long as the closing time is within the interval (9, 15) seconds.

If the valve closes too slowly, e.g. 18 s, it, as a safety barrier, will not meet the performance requirements for risk mitigating of EUC. A failure occurs on this valve since the required function is terminated. The corresponding failure mode is called ‘closing too slowly’, which is one of dangerous failure modes of ESD valve [1]. Degradation like corrosion or erosion due to the harsh environment is the reason of such a failure. Meanwhile, even the closing time is still within the acceptable interval, the criticality of the failure will obviously increase with the deviation from the target value (12 s) [20]. In most cases, it is not possible to observe such kind of failure without activating the valve, and so the failure mode ‘closing too slowly’ is a DU failure. Therefore, closing time checked in proof tests can be collected and reflect the valve status/degradation [30].

It is obvious that when the closing time is beyond 15 s, the valve is in a failed state. When the closing time is shorter than a certain value, e.g.14 s, we can regard the valve in a good condition. While if the closing time is between 14 and 15 s, we can consider the valve with a degraded performance but still functioning. Therefore, we can consider the valve with three different states: working, degraded and failed, as shown in Table 1. It should be noted that degradation still can exist in state 0, but it can be accepted without any maintenance action.

Because maintenance or replacement after each proof test is often

Table 1
System state definition.

state	status	State description
0	Working	The system is functioning as specified
1	Degraded	The system has a degraded performance but functioning
2	Failed	The system has a fault

expensive, no action is welcomed when the estimation based on the observed situation has shown that failure probability of the SIS by the next test is rather low. Specifically, when the valve is at the working state (state 0), no maintenance will be executed. When the valve in a degraded state, even it is still functioning, a PM with reasonable costs will be employed. The degradation is mitigated but is not eliminated considering a perfect maintenance is too costly. When the valve in a failed state, replacement is needed.

2.2. System operation and test

Possible causes of ‘closing too slowly’ failure mode may be because of the loss of stiffness of a spring [1,31,32]. According to [33,34], such kind of degradation could be described by stochastic process. Gamma process has been justified by practical applications for modeling degradations [35,36] due to its strongly monotone increasing property [37–39].

The final element of such a SIS is assumed to be subject to a homogeneous gamma degradation process, and a hidden failure occurs when the degradation level exceeds a predefined threshold L. The SIS is periodically tested at τ, 2τ, ..., where τ is the test time interval, e.g. one year. In a proof test, degradation level is checked. As shown in Fig. 1, at 4τ, the degradation level is found beyond the failure threshold, L, then the failed system is replaced by a new one. When the degradation level is found beyond $\omega_a L$ in a proof test, PM is needed. For example, at 6τ or 8τ in Fig. 1, PM is executed and the degradation level goes back to a specific level ($\omega_b L$) rather than 0.

Consider a one-unit system that is subject to a continuous aging degradation process. The degradation process is modeled by a Gamma process with the initial state $X_0 = 0$. Then, the degradation $X(t)$ follows a gamma probability density function (PDF).

$$X(t) \sim \Gamma(\alpha t, \beta) = f_{X(t)}(x) = \frac{\beta^{\alpha t}}{\Gamma(\alpha t)} x^{\alpha t - 1} e^{-\beta x},\ \alpha, \beta > 0 \tag{1}$$

The cumulative density function (CDF) of $X(t)$ for $t > 0$ is

$$F_{X(t)}(x) = \Pr\{X(t) \le x\} = \int_0^x f_{X(t)}(z) dz \tag{2}$$

Then, the mean and variance of $X(t)$ are $\alpha t/\beta$ and $\alpha t/\beta^2$, respectively.

Periodic proof tests are executed. Proof tests are assumed perfect in this study and have no direct influence on the degradation process. In addition, we assume that the time spent in repair and test is negligible compared with the much longer test intervals.

3. Maintenance modeling and unavailability estimation

3.1. Maintenance modeling of a final element

The SIS is periodically tested with an interval τ and with cost C_{PT}. During each proof test, if the observed the degradation level $X(t)$ of the final element is less than the predefined $\omega_a L$, no action is carried out and total cost is only C_{PT}. If the degradation level is higher than $\omega_a L$ but less than L, a PM is performed with cost C_{PM} and $C_{PM} > C_{PT}$. However, if the system is found failed, it will be replaced by a new one with C_{CM}, where $C_{CM} > C_{PM}$. In addition, the cost (C_D) related with risks of EUC needs to be considered in the downtime of SIS, C_D is calculated by the product of demand rate λ_{de} and the possible loss in an EUC accident.

The long-run cost rate could be calculated with the renewal theorem [29].

$$C^{\infty} = \lim_{t \to \infty} \frac{C(t)}{t} = \frac{E[C(S_1)]}{E(S_1)} \tag{3}$$

where $C(t)$ is the cumulated maintenance cost by time t, and S_1 is the length of the first renewal cycle.

The designed service time of most SISs is not infinite, and thus the steady-state assumption may not be accepted. We estimate the cost rate over a SIS lifetime as

$$C_t^{(\omega_a,\omega_b)} = C_T N_i(t) + C_{CM} N_{CM}(t) + C_{PM} N_{PM}(t) + C_D T_d(t) \tag{4}$$

where N_i (t), N_{CM} (t), N_{PM} (t) and T_d (t) are, respectively, number of proof tests, number of CMs, PMs and the expected downtime in $[0, t]$.

It is not hard to understand that the $C_t^{(\omega_a,\omega_b)}$ is a function of maintenance parameters, including the degradation level L, PM coefficient (ω_a, ω_b) and test interval τ.

Here, minimization of cost over the designed life (e.g. 20τ) is the criterion of selecting a suitable maintenance strategy.

3.2. Unavailability calculation

We start from estimation availability ($A(t)$) of the maintained final element at time t, namely the conditional probability that the component is working at time t given $X_0 = x$, with $x \in [0, \omega_a L]$. $A(t)$ is the probability that the system performs its required function at time t, when the degradation level is less than the predefined failure threshold L.

$$A(x, t) = \Pr(X_t < L) \tag{5}$$

In the case $t \le \tau$, there is no maintenance action on $[0, t)$. So,

$$A(x, t) = F_{X(t)}(L - x),\ \ \text{for } t \le \tau \tag{6}$$

From the second interval, the prior test result acts as the condition

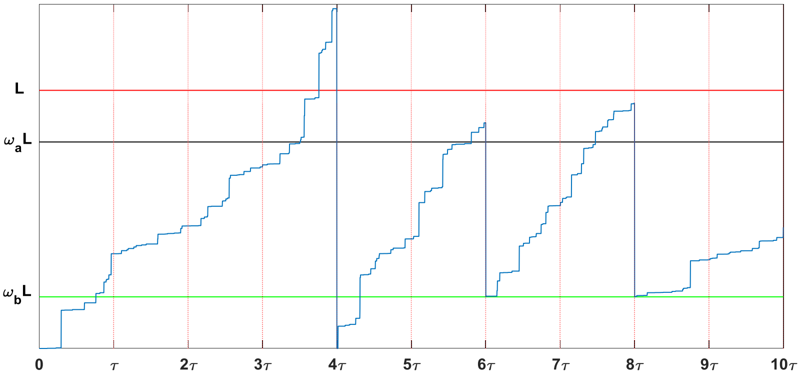


Fig. 1. Possible degradation path.

to estimate the instantaneous availability. For $i \geq 2$, we have the conditional knowledge given the degradation level μ at time τ, for $\tau < t \leq 2\tau$:

$$A(x, t) = \Pr(X(t) < L | X_\tau = \mu < L) = F_{X(t-\tau)}(L - x - \mu) \tag{7}$$

Similarly, we can get $A(x,t)$, for $(i\text{-}1)\tau < t \leq i\tau$ as,

$$A(x, t) = \Pr(X(t) < L | X_{(i-1)\tau}) = F_{X(t-(i-1)\tau)}(L - x - X_{(i-1)\tau}) \tag{8}$$

The valve will fail to function when the degradation level reaches or overpasses a predefined critical threshold L. PFD$_{\text{avg}}$, the widely measure of a low demand SIS, is not the long-term approximation here, but the average proportion of time where the system is not able to perform the required safety function within one test interval [1]. PFD$_{\text{avg}}$ in the first test interval is

$$\text{PFD}_{\text{avg}}^{1} = \frac{\int_0^\tau \bar{A}(x, t)dt}{\tau} = \frac{\int_0^\tau 1 - A(x, t)dt}{\tau} = 1 - \frac{\int_0^\tau F_{X(t)}(L - x)dt}{\tau} \tag{9}$$

While PFD$_{\text{avg}}$ in the second interval $(\tau, 2\tau)$ with known degradation level μ at time τ can be calculated as

$$\text{PFD}_{\text{avg}}^{2} = \frac{\int_\tau^{2\tau} \bar{A}(x, t)dt}{\tau} = 1 - \frac{\int_\tau^{2\tau} F_{X(t-\tau)}(L - x - \mu)dt}{\tau} \tag{10}$$

Similarly, PFD$_{\text{avg}}$ in the i th interval can be calculated using Eq. (8).

$$\text{PFD}_{avg}^{i} = \frac{\int_{(i-1)\tau}^{i\tau} \bar{A}(x, t)dt}{\tau} = 1 - \frac{\int_{(i-1)\tau}^{i\tau} F_{X(t-(i-1)\tau)}(L - x - X_{(i-1)\tau})dt}{\tau} \tag{11}$$

Each SIF should comply with the specific SIL. IEC 61,508 [2] specifies four SILs, with SIL4 most strict in terms of safety. SILs and their associated values of PFD$_{\text{avg}}$ are shown in Table 2.

To estimate degradation of the SIS element in each test interval, Monte Carlo simulation is implemented here by generating random events to obtain the probability distributions for the variables of the problem. A number of papers can be found using Monte Carlo methods in the domains of reliability, availability, maintainability and safety (RAMS) [40–43].

The main idea here is to randomly generate M degradation paths to simulate M possible components and use the average value in each test interval to estimate the performance.

4. Evaluation and optimization of maintenance strategies

4.1. Optimization criteria

As mentioned in Eq. (4), the cost is a function of several parameters, including failure threshold, L, test interval, τ, PM coefficient factors (ω_a, ω_b). It is difficult to obtain exact values of cost parameters [44], especially those related with production loss of shutdown process and the potential effects of hazardous event due to the failure of a SIS. Therefore, cost ratios, instead of absolute costs, are used here in optimization. Taking C_{PT} as the unit cost, C_D, C_{CM}, C_{PM}, can be expressed as k_1C_{PT}, k_2C_{PT}, and k_3C_{PT} respectively, where $k_1 > k_2 > k_3 \geq 1$.

For a SIS, the optimal (ω_a, ω_b) should find a trade-off between the minimum lifetime cost and the required SIL. For an ESD valve as an example, its required SIL is SIL3 (see Table 2), meaning that PFD$_{\text{avg}}$ should be in the range of $(10^{-4},10^{-3})$.

Table 2
SILs for low demand SISs, from [2].

IL	PFD$_{\text{avg}}$
SIL4	10^{-5}~10^{-4}
SIL3	10^{-4}~10^{-3}
SIL2	10^{-3}~10^{-2}
SIL1	10^{-2}~10^{-1}

Table 3
Parameter values for system analysis.

Parameter	Value
L	1.25×10^{-3}
α	1.02×10^{-4}
β	1.2×10^{4}
τ	8760
λ_{de}	2.5×10^{-5}
N_i	20
C_T	1
k_1	1×10^{5}
k_2	10
k_3	5

4.2. Numerical example

To illustrate the proposed method for optimizing maintenance strategy, a numerical example is employed with the degradation and operation parameters listed in Table 3.

4.2.1. Instantaneous availability

The degradation level $X(t)$, availability $A(t)$ and PFD$_{\text{avg}}$ of such an element can be plotted based on Eq. (1), Eqs. (6)–(8) and Eqs. (9)–(11) respectively, as depicted in Fig. 2.

At the starting point, $X_0 = 0$, and $A(0) = 1$. With time elapsing, the degradation level $X(t)$ is accumulating, meanwhile, $A(t)$ is decreasing and PFD$_{\text{avg}}$ is increasing. Given the periodic proof tests, the system status will be updated after each proof test. $A(t)$ curve has a certain periodicity but $A(t)$ reduces faster due to the accumulation of degradation. PFD$_{\text{avg}}$ curve indicates that even the valve is functioning at each proof test, PFD$_{\text{avg}}$ is increasing with time. It implies that the final element is becoming more fragile compared to that at the beginning. Given that the accumulated degradation level, $X(t)$, exceeds PM threshold, ω_aL, at 8τ, a PM is applied. After that, the degradation level is set back to ω_bL, the correspondingly instantaneous availability is improved. In other words, the SIS goes back to a situation performing its SIF well. But due to the existing degradation, PFD$_{\text{avg}}$ is still higher than that in the first test interval. At 12τ, the degradation level $X(t)$ goes beyond failure threshold L, and then replacement is executed. The system availability, $A(t)$, is improved while PFD$_{\text{avg}}$ decreases as low as the first test interval. Another similar process is the execution of a PM at 18τ.

4.2.2. Scenarios with different maintenance strategies

With the parameters given in Table 3, the expected cumulative costs in 20τ under three scenarios are compared:

(1) Scenario 1: The valve is only be repaired as-good-as-new once the failure has occurred, $\omega_a = 1$, $\omega_b = 0$.
(2) Scenario 2: The initial state is $X_0 = \omega_bL$ ($\omega_b \neq 0$), the system is repaired to as-good-as-new $X_0 = \omega_bL$ ($\omega_b \neq 0$) for both PM and CM with $\omega_a = 0.8$, $\omega_b = 0.1$.
(3) Scenario 3: The initial state is $X_0 = 0$, under the proposed maintenance strategy with $\omega_a = 0.8$, $\omega_b = 0.1$.

Two maintenance strategies are considered: One is reflected by Scenario 1, without PM; the other is reflected by Scenarios 2 and 3, with PMs. For the latter two, they are indicating different initial degradations occurred in manufacturing or installation. More specially, Scenario 3 means higher manufacturing and installation quality.

With the parameters in Table 3, the cost curves of these 3 scenarios are obtained as shown in Fig. 3.

It can be found that maintenance costs of the three scenarios are

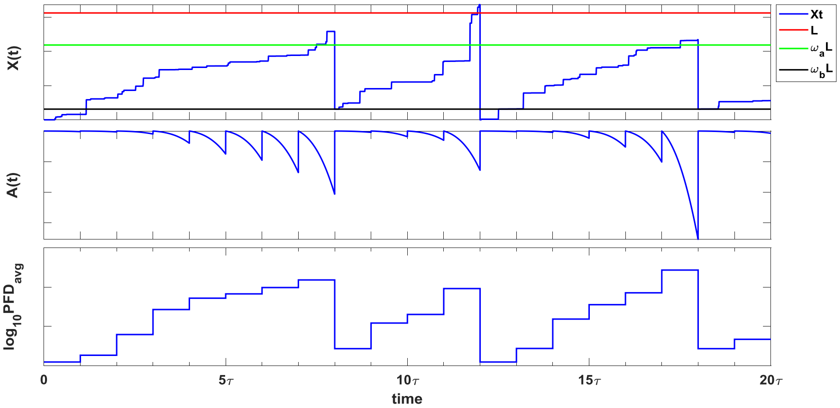


Fig. 2. A possible degradation path $X(t)$and the corresponding$A(t)$ and PFDavg.

almost same until around 10τ. By this time, PM or CM is seldom carried out. Then the cost of Scenario 1 increases significantly mainly due to the potential downtime cost. For Scenarios 2 and 3, their cost curves are very similar, with that of Scenario 2 a bit higher. By comparing the cumulative costs of Scenario 1 and Scenarios 2&3 in the total 20 test intervals, it can be found that PMs reduce the total lifetime cost dramatically, but the cost difference between Scenario 2 and Scenario 3 is quite small.

The PFD$_{avg}$ values of the SIS in different scenarios are shown in Fig. 4. At beginning, PFD$_{avg}$ increases with time (app. by 10τ) because of the continuous degrading process. For Scenario 1, PFD$_{avg}$ still increases after 10τ without PM and the SIS is within SIL1 most time, while for Scenarios 2 and 3, PFD$_{avg}$ is always lower, no worse than SIL2. Obviously, PMs improve SIS availability effectively, especially after the half of designed service time.

In practices, due to materials or mis-operation in the manufacturing or installation process, zero degradation is too ideal for a valve even it is new. In comparison of Scenarios 2 and 3, initial degradation is only found a slight negative effect on performance during the overall cycle. When rescheduling proof tests, it is not necessary to prioritize the considering of initial degradation.

4.2.3. *Effect of PM strategies on lifetime costs*

With the parameters in Table 3, the expected maintenance cost of the final element is calculated based on Eq. (4). The expected lifetime cost is a function of (ω_a,ω_b) with different (k_2, k_3) as shown in Fig. 5.

The CM cost is fixed as $k_2 = 10$, and Fig. 5 illustrates the impact of k_3 on the lifetime cost, i.e., the expensiveness of PMs. In general, when k_3 is larger, a PM is more costly, and the lifetime cost in 20 test intervals increases as well.

In Fig. 5(a), $k_3 = 1$ means that PM cost is very low, same as the test cost. Given a fixed ω_a, the total lifetime cost slightly increases with respect to ω_b. Even the higher ω_b can lead to more PMs, but due to the quite low PM cost in each time, the expected lifetime cost almost keeps unchanged under the same ω_a. However, given a fixed ω_b, the expected lifetime cost increases significantly with ω_a. When ω_a closes to 1, it means that the PM threshold $\omega_a L$ is near the failure threshold L, namely PMs are being avoided. CM cost is thus dominant for the increasement of lifetime cost.

In Fig. 5(b), compared to CM cost, PM cost is still quite low, so the overall tendency of lifetime cost is similar to that shown in Fig. 5(a). Within this assumed range of k_3 and (ω_a,ω_b), it can be obtained that the optimal value of (ω_a,ω_b) is (0.70,0).

In Fig. 5(c) and Fig. 5(d), PMs are more expensive. The lifetime cost increases with respect to ω_b, while decreases firstly and then increases with respect to ω_a. There is a trade-off between PM cost and the potential downtime cost. Because a smaller ω_a increases the PM expenses, but it results in a higher failure possibility that can increase CM and downtime costs. This phenomenon becomes more obvious in Fig. 5(d) when PM cost is equivalent to 80% CM cost.

For both Fig. 5(c) and Fig. 5(d), it is necessary to find an optimal (ω_a, ω_b) under the certain parameters. With calculation, the optimal

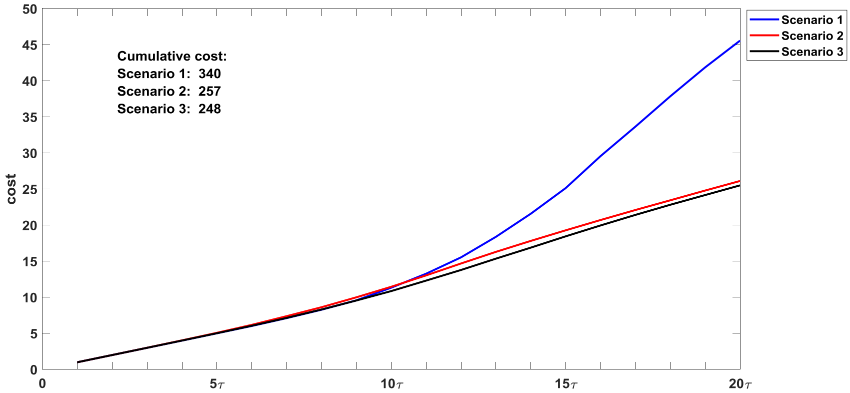


Fig. 3. Cumulative cost under different scenarios.

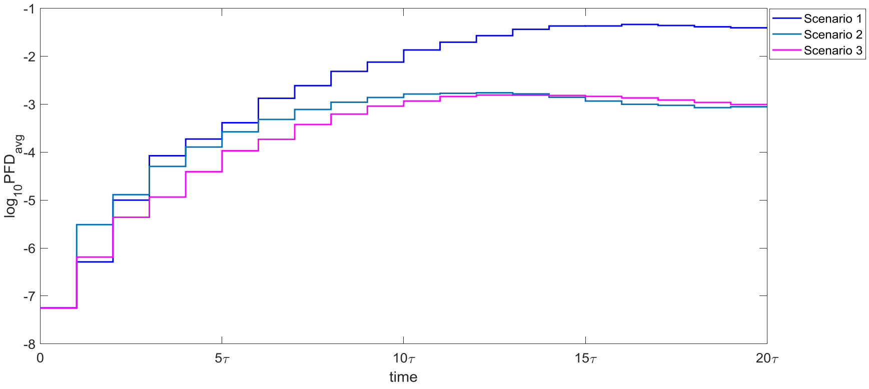


Fig. 4. $\mathrm{PFD}_{\mathrm{avg}}$ under different scenarios.

(ω_a, ω_b) is (0.75, 0) in Fig. 5(c), while the optimal (ω_a, ω_b) is (0.80, 0) in Fig. 5(d).

The findings can help the decision-making of maintenance crew of SISs. If PM costs are much lower than those led by a SIS failure, it is reasonable to take more PMs to keep the system safe. Otherwise, if PM costs are close to CM costs, many PMs are not essential.

However, we have an assumption so far that PM cost is same no matter what the value of ω_b is. In practices, when a system is aging, the PM cost often increases as well. The PM factor ω_b should link with system installation time and actual healthy status.

Meanwhile, the effects of failure threshold, L, and PM parameter, ω_a, on the lifetime cost are analyzed. The values of L are set as $[1.05, 1.15, 1.25, 1.35, 1.45] \times 10^{-3}$ respectively, and then lifetime cost of the final element is calculated with the result shown in Fig. 6.

When $L = 1.45 \times 10^{-3}$, the lifetime cost has minor increase from $\omega_a = 0.7$ to $\omega_a = 0.9$. This is because such a threshold is so high that

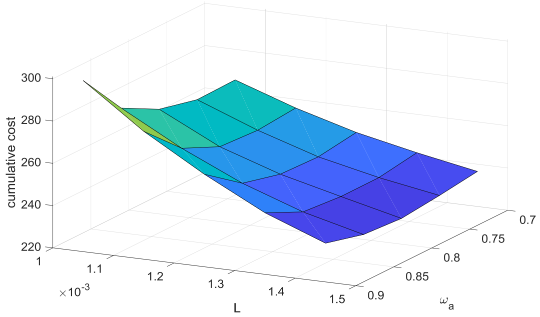
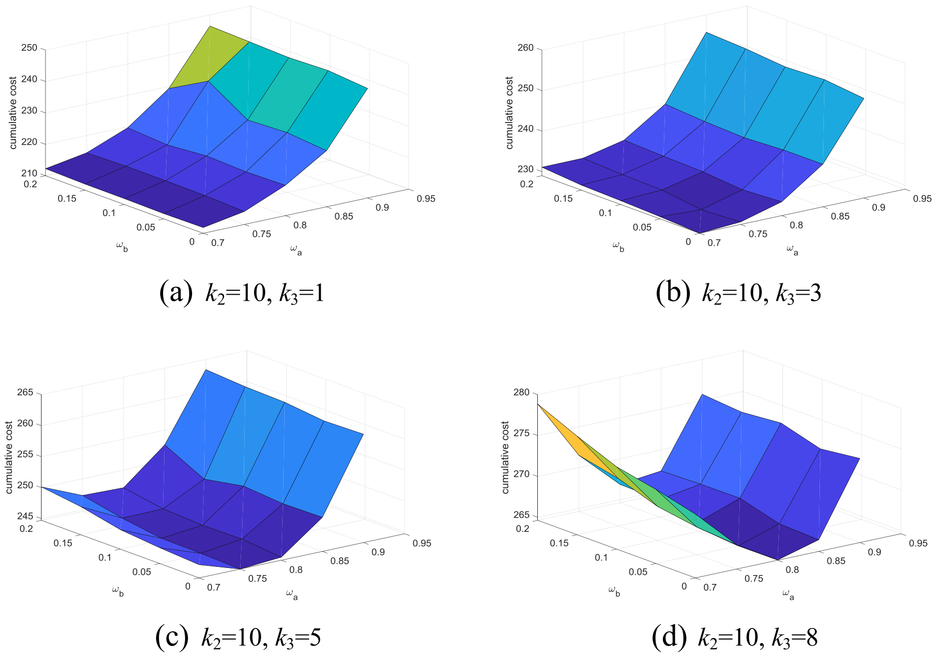


Fig. 6. Expected maintenance cost.



(a) k_2=10, k_3=1

(b) k_2=10, k_3=3

(c) k_2=10, k_3=5

(d) k_2=10, k_3=8

Fig. 5. Mesh plot the expected total maintenance cost on (k_2, k_3).

the chance of a failure event is very low. When the value of L is lower, e.g. 1.05×10^{-3}, the lifetime cost differences between the solutions of $\omega_a = 0.7$ and $\omega_a = 0.9$ is more apparent. For lower failure threshold with higher value of ω_a, the degradation level can exceed the failure threshold with higher possibility.

Given a fixed ω_a, the lifetime cost decreases with a higher threshold L, because a smaller threshold L will increase downtime.

The failure threshold L can be affected by manufacturing process and risk acceptance criteria. In manufacturing, high-quality material could lead to higher degradation-tolerant threshold. In operations, when it is acceptable to tolerate more risks to the EUC, the failure threshold also could be set higher.

In determining the optimal value of ω_a, failure threshold should also be considered. When the failure threshold is quite high, from the perspective of maintenance cost, ω_a could be set a higher value as of the low failure probability.

4.2.4. Effects of PM strategies on PFDavg

Here we study how PM strategies with different (ω_a, ω_b) influence PFD_{avg}.

The PFD_{avg} of such a SIS can be obtained using simulation based on Eqs. (9)–(11). PFD_{avg} in each test interval is illustrated in Fig. 7.

It is obvious that the PFD_{avg} has a strong correlation with parameters, (ω_a, ω_b).

The effect of ω_a on PFD_{avg} in Fig. 7(a) is analyzed with setting with $\omega_b = 0.1$. At early stage, for example, t is around $t = 8\tau$, PFD_{avg} increases over time but still remains within SIL3. After 8τ, PFD_{avg} falls into SIL2 for $\omega_a = 0.9$. PFD_{avg} starts to keep stable in each interval and just fluctuates in a small range (same SIL). These curves show that the value of PFD_{avg} in each test interval decreases with ω_a. With the lower ω_a, the earlier PM will be taken. After a PM, the degradation is mitigated so that the probability of failure is reduced.

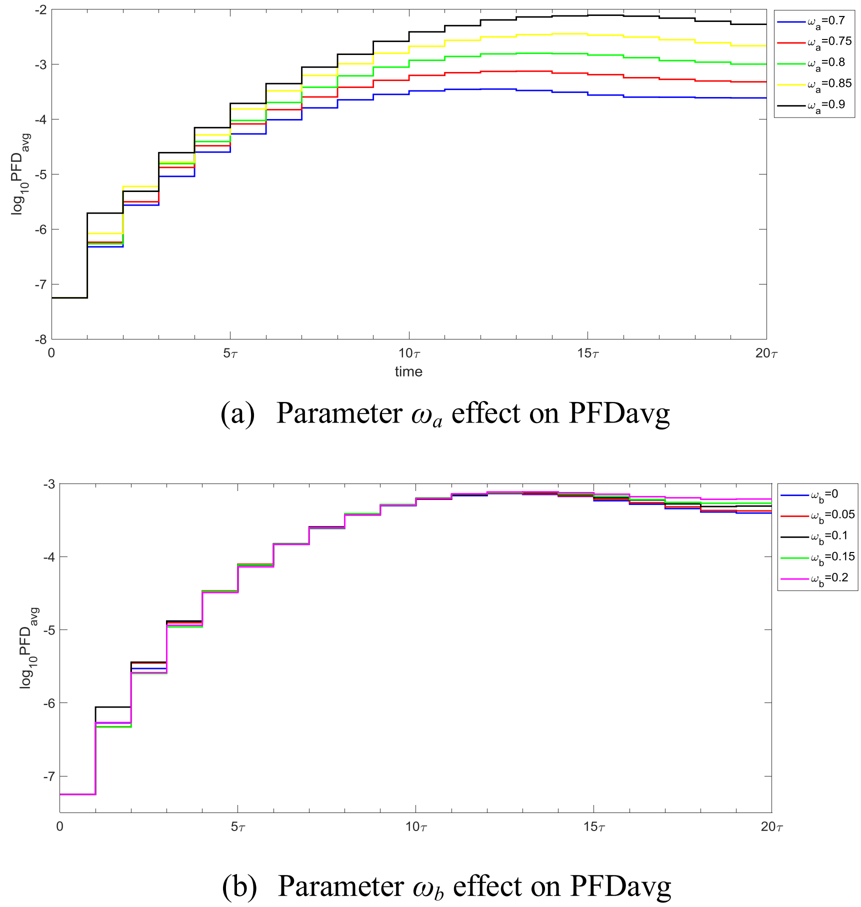
The effect of parameter ω_b on PFD_{avg} in Fig. 7(b) is evaluated with $\omega_a = 0.75$. Compared to ω_a, parameter ω_b has slight impact on system PFD_{avg}.

The combined effect of (ω_a, ω_b) on system PFD_{avg} in several intervals are then depicted in Fig. 8.

The overall tendency of PFD_{avg} in each test interval is almost same. Meanwhile, PFD_{avg} in each test interval is limited mainly in SIL3 and SIL2. Give a fixed ω_b, PFD_{avg} increases with ω_a. However, given a fixed ω_a, PFD_{avg} keeps almost the same value for different ω_b.

The values of failure threshold L are set $[1.05,1.15,1.25,1.35,1.45] \times 10^{-3}$, respectively, to observe the effect of threshold on PFD_{avg}. The mesh plot is shown in Fig. 9.

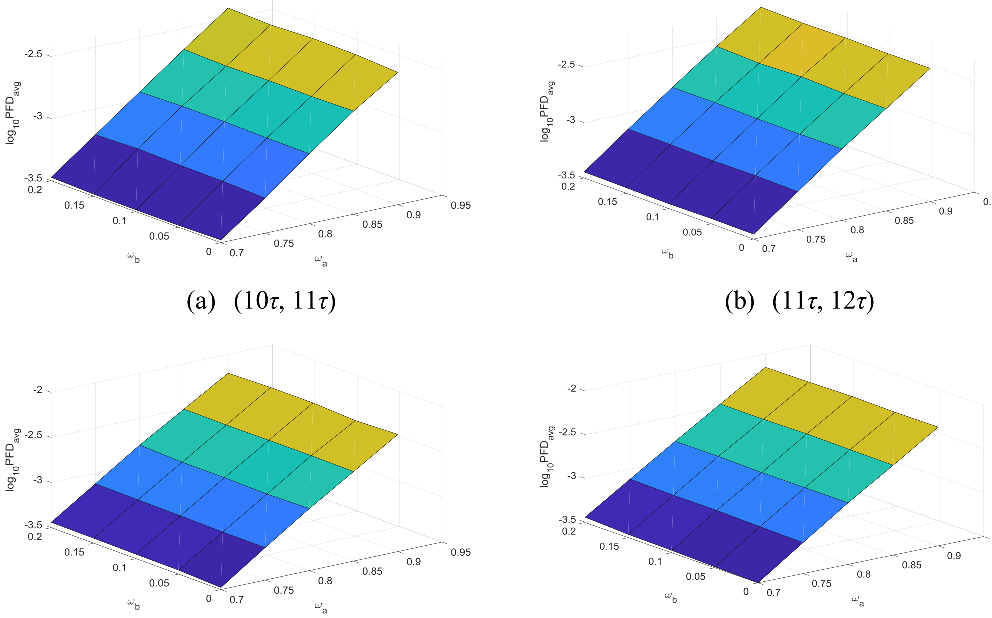
Given a same threshold L, PFD_{avg} is going down with lower ω_a. This finding can be regarded as a guideline for maintenance management. For the same SIS, the earlier the PM is executed, the more liable the system is. Without considering the PM cost, ω_a should be as small as



(a) Parameter ω_a effect on PFDavg

(b) Parameter ω_b effect on PFDavg

Fig. 7. (ω_a, ω_b) effect on PFDavg of the system in every test interval.



(a) $(10\tau, 11\tau)$

(b) $(11\tau, 12\tau)$

(c) $(12\tau, 13\tau)$

(d) $(13\tau, 14\tau)$

Fig. 8. Mesh plot $\mathrm{PFD}_{\mathrm{avg}}$ in several intervals.

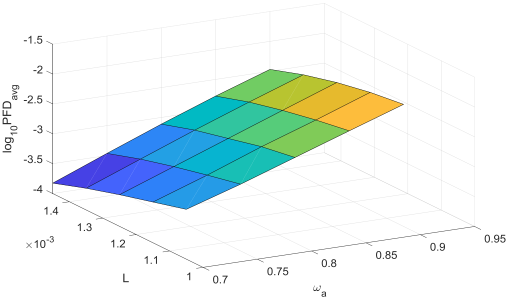


Fig. 9. Mesh plot $\mathrm{PFD}_{\mathrm{avg}}$ on failure threshold $L$and ω_a.

possible.

Meanwhile, for a fixed ω_a, $\mathrm{PFD}_{\mathrm{avg}}$ is going up with lower threshold L. For threshold $L = 1.45 \times 10^{-3}$, $\omega_a = 0.8$ is enough for the system to be limited within SIL3, whereas, $\omega_a = 0.7$ should be taken for $L = 1.05 \times 10^{-3}$.

5. Updating test intervals with the information from tests

For low demand SISs, it might not be always worthwhile running proof tests periodically, especially if the shutdown and restart of process is costly. In this case, the date of the next proof test can be determined based on degradation state observed in the current test. Interval to the next test can be longer if the SIS element is very healthy, and the interval should be shorter as the element deteriorates. When the degradation level is closing to PM threshold, more tests are expected.

Having considered degradation and diverse maintenance strategies, it is interesting to introduce non-periodic proof tests. According to the study of [45], to keep system safety, 3 years is roughly set as the maximum length of a proof test interval.

In consideration of degradations, PM parameters are set as $\omega_a = 0.75$ and $\omega_b = 0.05$. The general expected test interval length is generated by Monte Carlo simulation.

The main steps of simulation algorithm for the expected test intervals are shown here.

- Step 1: Set $X_t = 0$ and $N = 1$. If $N \le N_{\max}$ the process goes to steps.
- Step 2: Generate n degradation paths. Then the arrival time of the first reach failure threshold L can be obtained.
- Step 3: Get the 5-th percentile value as potential arrival time τ_1. Compare τ_1 and 3 years. If $\tau_1 < 3$ years, then take τ_1 as the new test interval of the system; if $\tau_1 \ge 3$ years, then 3 years are used as the new test interval.
- Step 4: Use the mean value and variance of Gamma process in Section 2.2 to estimate the increment $X_{0\sim\tau 1}$ between $(0, \tau_1)$. At the same time, safety margin is also considered. The 97.5-th percentile ($\rho = 0.975$) is used as the potential increment in $(0, \tau_1)$.
- Step 5: Compare the potential degradation level at time τ_1, $X_{\tau 1}$, with PM threshold or CM threshold to decide whether a maintenance strategy is required here. The $X_{\tau 1}$ after comparison is the new starting point.
- Step 6: Repeat Step 2~ Step 5 and set $N = N + 1$.

The time to failure threshold L from $X_t = 0$ is verified to follow normal distribution. Different increment percentiles are investigated as the result shown in Table 4.

The updated general lengths of each test interval are listed in Table 4. We can see that with different percentile values, test interval length becomes different from the third updated test. With $\rho = 0.975$, a PM is executed after the second interval and the degradation is mitigated. When ρ is set as 0.90 or 0.825, the third test interval is shorter with the length of 0.5τ and 1.2τ, respectively.

It is worth mentioning that the degradation parameters (α, β) affect

Table 4
Updated test intervals under different increment percentiles.

	1st	2nd	3rd	4th	5th	6th	7th	8th
$P = 0.975$	$(0, 3\tau)$	$(3\tau, 6\tau)$	$(6\tau, 9\tau)$	$(9\tau, 11.5\tau)$	$(11.5\tau, 14.5\tau)$	$(14.5\tau, 17\tau)$	$(17\tau, 20\tau)$	$(20\tau, 22.5\tau)$
$P = 0.90$	$(0, 3\tau)$	$(3\tau, 6\tau)$	$(6\tau, 6.5\tau)$	$(6.5\tau, 9.5\tau)$	$(9.5\tau, 12.5\tau)$	$(12.5\tau, 15.5\tau)$	$(15.5\tau, 18.5\tau)$	$(18.5\tau, 21.5\tau)$
$P = 0.825$	$(0, 3\tau)$	$(3\tau, 6\tau)$	$(6\tau, 7.2\tau)$	$(7.2\tau, 10.2\tau)$	$(10.2\tau, 13.2\tau)$	$(13.2\tau, 14.2\tau)$	$(14.2\tau, 17.2\tau)$	$(17.2\tau, 20.2\tau)$

*$\tau = 8760\ h = 1\ year$.

the degradation rate directly. The simulation results in Table 4 are based on assumed (α, β) in Table 3. It only acts as a reference method for updating test intervals.

If the exact degradation level μ can be observed in each proof test. When updating the test lengths, the main constraint is the required SIL. Considering the degradation process, the first interval τ_1 can be calculated based on Eq. (12) with the given limit values of PFD$_{\text{avg}}$.

$$\text{PFD}_{\text{avg}}^1 = \frac{1}{\tau_1}\int_0^{\tau_1} \bar{A}(t)dt = \frac{1}{\tau_1}\int_0^{\tau_1} \Pr(X(t) > L)dt \tag{12}$$

For calculating the second interval, the degradation level μ_1 at τ_1 is taken into consideration.

$$\text{PFD}_{\text{avg}}^2 = \frac{1}{\tau_2 - \tau_1}\int_{\tau_1}^{\tau_2} \bar{A}(t)dt = \frac{1}{\tau_2 - \tau_1}\int_{\tau_1}^{\tau_2} \Pr(X(t) > L|X_{\tau_1} = \mu_1)dt \tag{13}$$

Using Eq. (13), the value of τ_2 can also be updated. By following the similar solution process for the latter intervals, the flexible test interval can be calculated and updated.

6. Conclusion

A stochastic process-based availability analysis for the final element of a SIS is carried out, and three states of the element are considered. This forms the basis for determining the maintenance strategies following proof tests. The algorithms of instantaneous availability of the SIS element and expected lifetime cost in the SIS operation are developed. PFD$_{\text{avg}}$ of the SIS element is calculated based on the homogeneous gamma process.

The findings in the case studies have shown that PM strategies, i.e. the optimal values of (ω_a, ω_b), and the expensiveness of PMs to CMs, are influential factors of the lifetime cost and SIL of a SIS.

PFD$_{\text{avg}}$ of the SIS is affected by the PM threshold ω_a significantly, especially after half of the service lifetime, but not too much affected by ω_b. Effects of ω_a on PFD$_{\text{avg}}$ are becoming more obvious with lower threshold L. When the failure threshold L is quite high, the value of ω_a has slight effects on PFD$_{\text{avg}}$ given the low possibility of failure.

Based on the above findings, suggestions on updating test intervals are given. Maintenance crews can be beneficiary of these suggestions, by saving maintenance costs through reducing frequency of proof tests.

For further studies, it would be interesting to consider the availability and maintenance cost on k-out-of-n architectures.

Declaration of Competing Interest

The authors declared that they have no conflicts of interest to this work. We declare that we do not have any commercial or associate interest that represents a conflict of interest in connection with the submitted manuscript, which entitled, 'Optimization of maintenances following proof tests for the final element of a safety-instrumented system'.

Acknowledgement

The authors acknowledge the financial support provided by China Scholarship Council (201706440015), and the secondment opportunities for joint research provided by the RISEN project (No 691135) under EU Marie Curie RISE program.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.ress.2019.106779.

References

[1] Rausand M. Reliability of safety-critical systems: theory and applications. John Wiley & Sons; 2014.
[2] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. 2010.
[3] Hauge S, Kråknes T, Håbrekke S, Jin H. Reliability prediction method for safety instrumented systems - PDS Method handbook 2013 edition. 2013.
[4] Bukowski JV. A comparison of techniques for computing PFD average. Annu Reliab Maintainab Symp 2005:590–5.
[5] Mechri W, Simon C, Bicking F, Othman KB. Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment. J Loss Prev Process Ind 2013;26:594–604. https://doi.org/10.1016/j.jlp.2012.12.002.
[6] Mechri W, Simon C, BenOthman K. Switching Markov chains for a holistic modeling of SIS unavailability. Reliab Eng Syst Saf 2015;133:212–22. https://doi.org/10.1016/j.ress.2014.09.005.
[7] Zhang N, Fouladirad M, Barros A. Optimal imperfect maintenance cost analysis of a two-component system with failure interactions. Reliab Eng Syst Saf 2018. https://doi.org/10.1016/j.ress.2018.04.019.
[8] Liu Y, Rausand M. Reliability assessment of safety instrumented systems subject to different demand modes. J Loss Prev Process Ind 2011;24:49–56.
[9] Liu Y, Rausand M. Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems. Reliab Eng Syst Saf 2016;145:366–72. https://doi.org/10.1016/j.ress.2015.06.016.
[10] Liu Y. Discrimination of low-and high-demand modes of safety-instrumented systems based on probability of failure on demand adaptability. Proc Inst Mech Eng Part O J Risk Reliab 2014;228(4):409–18.
[11] 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. https://doi.org/10.1016/j.jlp.2017.12.007.
[12] Rogova E, Lodewijks G, Lundteigen MA. Analytical formulas of PFD and PFH calculation for systems with nonconstant failure rates. Proc Inst Mech Eng Part O J Risk Reliab 2017;231:373–82. https://doi.org/10.1177/1748006x17694999.
[13] Wu S, Zhang L, Barros A, Zheng W, Liu Y. Performance analysis for subsea blind shear ram preventers subject to testing strategies. Reliab Eng Syst Saf 2018;169:281–98. https://doi.org/10.1016/J.RESS.2017.08.022.
[14] Innal F, Lundteigen MA, Liu Y, Barros A. PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models. Reliab Eng Syst Saf 2016;150:160–70. https://doi.org/10.1016/J.RESS.2016.01.022.
[15] Langeron Y, Barros A, Grall A, Bérenguer C. Combination of safety integrity levels (SILs): a study of IEC61508 merging rules. J Loss Prev Process Ind 2008;21:437–49. https://doi.org/10.1016/J.JLP.2008.02.003.
[16] Srivastav H, Guilherme AV, Barros A, Lundteigen MA, Pedersen FB, Hafver A, et al. Optimization of periodic inspection time of SIS subject to a regular proof testing. Safety and reliability–safe societies in a changing world–proceeding of the 28th International. European. safety and reliability conference ESREL 2018. 2018.
[17] Zhou Y, Ma L, Mathew J. A non-gaussian continuous state space model for asset degradation. Proceeding 3rd world congress on engineering asset management intelligence maintaince system conference 1(1). 1. 2008. p. 1981–92.
[18] Wang Q, Liu W, Zhong X, Yang J, Yuan Q. Development and application of equipment maintenance and safety integrity management system. J Loss Prev Process Ind 2011;24:321–32. https://doi.org/10.1016/j.jlp.2011.01.008.
[19] Zio E. Some challenges and opportunities in reliability engineering. IEEE Trans Reliab 2016;65:1769–82. https://doi.org/10.1109/TR.2016.2591504.
[20] Rausand M, Høyland A. System reliability theory: models, statistical methods, and applications. John Wiley & Sons; 2004.
[21] Lundteigen MA, Rausand M. Partial stroke testing of process shutdown valves: how to determine the test coverage. J Loss Prev Process Ind 2008. https://doi.org/10.1016/j.jlp.2008.04.007.
[22] Fouladirad M, Grall A. Condition-based maintenance for a system subject to a non-homogeneous wear process with a wear rate transition. Reliab Eng Syst Saf 2011;96:611–8. https://doi.org/10.1016/J.RESS.2010.12.008.

[23] Mercier S, Pham HH. A preventive maintenance policy for a continuously monitored system with correlated wear indicators. Eur J Oper Res 2012;222:263–72. https://doi.org/10.1016/J.EJOR.2012.05.011.

[24] Deloux E, Castanier B, Bérenguer C. Predictive maintenance policy for a gradually deteriorating system subject to stress. Reliab Eng Syst Saf 2009;94:418–31. https://doi.org/10.1016/J.RESS.2008.04.002.

[25] Zhu W, Fouladirad M, Bérenguer C. Condition-based maintenance policies for a combined wear and shock deterioration model with covariates. Comput Ind Eng 2015;85:268–83. https://doi.org/10.1016/J.CIE.2015.04.005.

[26] Huynh KT, Grall A, Bérenguer C. A parametric predictive maintenance decision-making framework considering improved system health prognosis precision. IEEE Trans Reliab 2019;68:375–96. https://doi.org/10.1109/TR.2018.2829771.

[27] Castro I, Barros A, Grall A. Age-based preventive maintenance for passive components submitted to stress corrosion cracking. Math Comput Model 2011. https://doi.org/10.1016/j.mcm.2011.03.003.

[28] Huynh KT, Castro IT, Barros A, Berenguer C. On the use of mean residual life as a condition index for condition-based maintenance decision-making. IEEE Trans Syst Man, Cybern Syst 2014. https://doi.org/10.1109/TSMC.2013.2290772.

[29] Huynh K, Barros A, Bérenguer C, Castro I. A periodic inspection and replacement policy for systems subject to competing failure modes due to degradation and traumatic events. Reliab Eng Syst Saf 2011;96:497–508. https://doi.org/10.1016/j.ress.2010.12.018.

[30] Hosktad P., Håbrekke S., Johnsen R., Sangesland S. Ageing and life extension for offshore facilities in general and for specific systems. 2010.

[31] Medjaher K, Skima H, Zerhouni N. Condition assessment and fault prognostics of microelectromechanical systems. Microelectron Reliab 2014. https://doi.org/10.1016/j.microrel.2013.09.013.

[32] Travé-Massuyès, L., Pons, R., Ribot, P., Pencolé, Y., & Jauberthie C.Condition-based monitoring and prognosis in an error-bounded framework. DX@ Safeprocess, 2015, p. 83–90.

[33] Singpurwalla ND. Survival in dynamic environments. Stat Sci 2007. https://doi.org/10.1214/ss/1177010132.

[34] Huynh KT, Langeron Y, Grall A. Degradation modeling and RUL estimation of deteriorating systems in S-Plane. IFAC-PapersOnLine 2017. https://doi.org/10.1016/j.ifacol.2017.08.2036.

[35] van Noortwijk JM. A survey of the application of gamma processes in maintenance. Reliab Eng Syst Saf 2009. https://doi.org/10.1016/j.ress.2007.03.019.

[36] Blain C, Barros A, Grall A, Lefebvre Y. Modelling of stress corrosion cracking with stochastic processes - Application to steam generators. Proceeding of the European safety reliability conference. 2007, ESREL 2007 - risk, reliability society and safety. 2007.

[37] Grall A, Bérenguer C, Dieulle L. A condition-based maintenance policy for stochastically deteriorating systems. Reliab Eng Syst Saf 2002;76:167–80. https://doi.org/10.1016/S0951-8320(01)00148-X.

[38] Van P D, Bérenguer C. Condition-based maintenance with imperfect preventive repairs for a deteriorating production system. Qual Reliab Eng Int 2012;28:624–33. https://doi.org/10.1002/qre.1431.

[39] Mercier S, Pham HH. A condition-based imperfect replacement policy for a periodically inspected system with two dependent wear indicators. Appl Stoch Model Bus Ind 2014;30:766–82. https://doi.org/10.1002/asmb.2011.

[40] Barata J, Soares CG, Marseguerra M, Zio E. Simulation modelling of repairable multi-component deteriorating systems for “on condition” maintenance optimisation. Reliab Eng Syst Saf 2002. https://doi.org/10.1016/S0951-8320(02)00017-0.

[41] Lin Y, Li Y, Zio E. A comparison between Monte Carlo simulation and finite-volume scheme for reliability assessment of multi-state physics systems. Reliab Eng Syst Saf 2018. https://doi.org/10.1016/j.ress.2018.01.008.

[42] Malefaki S, Koutras VP, Platis AN. Multi-state deteriorating system dependability with maintenance using Monte Carlo simulation. Proceeding. - 2nd international symposium on stochastic models in reliability engineering life sciences operations management SMRLO 2016 2016. https://doi.org/10.1109/SMRLO.2016.21.

[43] Nadjafi M, Farsi MA, Jabbari H. Reliability analysis of multi-state emergency detection system using simulation approach based on fuzzy failure rate. Int J Syst Assur Eng Manag 2017. https://doi.org/10.1007/s13198-016-0563-7.

[44] Alaswad S, Xiang Y. A review on condition-based maintenance optimization models for stochastically deteriorating system. Reliab Eng Syst Saf 2017;157:54–63. https://doi.org/10.1016/j.ress.2016.08.009.

[45] Hauge S., Lundteigen M.A., Onshus T., Bodsberg L. Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase PDS -multiclient safety sikkerhet operation drift. 2008.

Article V

Zhang, A., Srivastav, H., Barros, A., & Liu, Y. (2020). Study of testing and maintenance strategies for redundant final elements in SIS with imperfect detection of degraded state. Reliability Engineering & System Safety, 107393.

Study of testing and maintenance strategies for redundant final elements in SIS with imperfect detection of degraded state

Aibo Zhang[a], Himanshu Srivastav[a], Anne Barros[b], Yiliu Liu[a,*]

[a] *Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway*
[b] *CentraleSupelec, Paris Saclay University, France*

Abstract

Safety-instrumented systems (SISs) have been widely installed to lower risks of equipment/ process by performing the designed safety functions in cases of demands. Final elements remain dormant mostly in a low demand mode but become vulnerable due to degradation along with time. Tests and maintenances are key activities to prevent the SIS from any failures, including those thank to degradation, to activate upon demands. This paper models the degradation of SIS final elements by considering an intermediate degraded state between the working- and failed states. Sometimes, the actual system states are not distinguished perfectly during proof tests. Such imperfectness in state revealing, consequently, weakens the real performance of follow-up maintenances. The effects of imperfect degradation state revealing are quantified, together with three testing and maintenance strategies for 1-out-of-2 configured SISs. Time-dependent PFD of the system and cumulative life-cycle cost are then estimated in a finite service time. Numerical examples under proposed strategies are presented to provide clues in selection of optimal testing and maintenance strategies for 1oo2 final element in SISs.

Keywords: Safety-instrumented system, degrading final element, imperfect state revealing, testing and maintenance strategy, performance analysis

1. Introduction

Safety-instrumented systems (SISs) are widely applied in different industries to detect the onset of hazardous event and/or to mitigate their consequences, such as emergency shutdown (ESD)

[☆] Fully documented templates are available in the elsarticle package on CTAN.

[*] Corresponding author

Email address: yiliu.liu@ntnu.no (Yiliu Liu) systems on an oil & gas production platform, high pressure protection systems (HIPPSs) in the process industry. Normally, a SIS consists of sensor(s) (e.g. pressure transmitters), logic solver(s) and final element(s) (e.g. shutdown valves) [1, 2].

Both ESD and HIPPS are typical SISs operating in a low demand mode, where the activation frequency is less than once per year in general. Some failure modes of final elements will stay hidden until a proof test is executed or an undesired event occurs on the equipment under control (EUC) by the SIS [2]. These hidden failures are called dangerous undetected (DU) failures if they can lead to dangerous events with severe consequences. Redundant structures are often used in SISs to improve the system availability and so to enhance safety. IEC 61508[3] recommends the average probability of failure on demand (PFD_{avg}) as a measure in the performance evaluation of SISs in the low demand mode.

Some widely used methods have been developed for the calculation of PFD_{avg}, including simplified formulas [1, 2, 4], fault tree analysis [5, 6, 7, 8], Markov methods [9, 10, 11, 12, 13], Bayesian methods [14, 15, 16], Petri Nets [17, 18, 19] and AltaRica modeling [20]. The common for most of these methods is assumed that all elements in a SIS are as-good-as-new after a repair in case a DU is revealed in a proof test. Such an assumption is valid for electronic components with exponentially distributed lifetime, but its validity for mechanical component is in question.

There exists literature in abundance for reliability assessment of units like safety valves under various maintenance strategies such as as-bad-as-old(ABAO) under corrective maintenance or imperfect maintenance under preventive maintenance. The important assumption with these methods is binary state model [21, 22, 23, 24].

The final execution elements of SISs, mainly consisted of mechanical components, may not always fail at a constant failure rate. They are rather vulnerable to creeping or other degradation processes [25]. In general, the reliability of a mechanical system decreases as the degradation processes develop [26], which contribute to a time-dependent failure rate. Thus, several dynamic reliability methods with advantage of represent time- and age-dependent performance have been applied to address degradation mechanisms of such mechanical components, e.g. stochastic process [27, 28, 29], multi-phase Markov process [9, 11, 30, 31, 32].

For SIS final elements with degradation, Mechri et al.[9] have considered the imprecision on the failure rates of components in performance evaluation of the SIS in low demand using fuzzy multi-phase Markov process. Innal et al. [31] have generalized PFD_{avg} formulas by including partial and full periodic tests. Wu et al. [11] have conducted the time dependent unavailability analysis of blind shear ram preventers (BSRPs) by incorporating testing strategies into multi-phase Markov process. Three states for 1oo1 configuration have been considered, including functioning, failed and waiting for repair. Zhang et al. [29] have performed the $\mathrm{PFD}_{\mathrm{avg}}$ of a 1oo1 configuration subjected to continuous aging degradation process. Different follow-ups based on the system state in proof test are considered. Srivastav et al. [32] have considered the negative effects of proof tests on SIS by adding discrete degraded states between working and failed state.

On the other hand, with the development of sensor technologies, more data about operation conditions and system status can be collected. Numerous parameters such as the lubricant ingredients, vibration signal, thermography picture, corrosion extent and so on can be measured and analyzed for failure prediction and diagnosis [33]. For example, a series of studies have been conducted on choke valve erosion based on the flow coefficient obtained from process parameters [34, 35, 36, 37]. The deviation between actual value and reference value is regarded as one useful indicator for choke valve erosion. When the deviation is beyond the acceptable level, the valve is regarded to be failed.

Health indicators are helpful to implement condition-based maintenance on SISs, namely corresponding maintenance actions are conducted based on the observed states. After a proof test on a SIS final element, different following-ups are possible based on the system state of working, degraded or failed. The presence of the degraded state is beyond the scope of binary-state system analysis, and several studies have been conducted on such multi-state systems reliability analysis and maintenance optimization [38, 39, 40, 41, 42, 43]. However, the existing literature relies on an assumption that system degradation state revealing is perfect [39, 44, 45]. This is not always right for SISs because the degradation level of a SIS is not observed directly in many cases but is determined by the difference between a reference value and an estimate value of status, while the estimated value is calculated from some relevant process parameters [34, 37]. When the collected data in a proof test, e.g. by sensors, process conditions and media in valve, is imprecise or different from working conditions, these inaccurate measurements will be passed into the physical condition estimation for valves. These unintended errors can be amplified or diminished in calculation of actual status of valves. Errors can also come from inaccurate setting of the threshold between working and degradation [29].

Secondly, existing studies on testing strategies for redundant SISs mainly focus on addressing uncertainty [46] and common cause failures (CCFs) [2, 5, 47], neglecting degrading units and preventive maintenance policies. In this context of imperfect degradation revealing, it is worth studying to analyze how the degradation of a single unit affects the whole redundant structure under different testing strategies. In addition, the life-cycle cost of an SIS in the designed service time (e.g. 20 years) is more of interest, compared to existing studies focusing on the average long-run cost rate [48, 49].

As a response, this paper is aiming to take potential imperfect state revealing into account of state-based SIS assessment, to make a comparison among different testing and maintenance strategies. The specific objectives include:

- Modeling and quantifying the imperfectness of state revealing in proof tests and their effects on the performance of redundant final elements in SISs.
- Evaluating condition-based maintenance strategies in the contexts where different testing approaches are used.
- Incorporating and balancing system availability and life cycle costs in seeking testing and maintenance strategies and providing guidance to operational decision-makers of SISs.

The remainder of this paper is organized as follows: Section 2 illustrates the characteristics of final elements in SIS, as well as the testing and maintenance strategies; Section 3 investigates the calculation of system PFD_{avg} and cumulative life-cycle cost given the certain assumptions; Section 4 conducts a numerical example to present the system performance and cumulative cost with state revealing coverage under different test and maintenance strategies and discusses the pros and cons of different strategies; Concluding remarks are given in Section 5.

2. System description

2.1. Structure and operations of a SIS

As mentioned, a typical SIS consists of sensor(s), logic solver(s) and final element(s). Without losing generality, a high pressure protection system (HIPPS) in oil & gas industry is used to study SIS operations and tests here, whose architecture is shown in Fig. 1. Two redundant shutdown valves (Valve 1 and 2), serving as the final elements in HIPPS, are installed on the same pipeline to stop the flow and relieve pressure in case the downstream pressure is too high. When one of two valves cannot be activated, the process, namely EUC, is still safe if the other valve works. Such kind of configuration is called as 1-out-of-2 (1oo2), which can improve system availability and so to enhance safety to some extent.

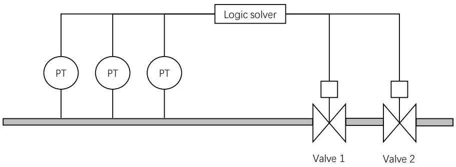


Figure 1: Example of a HIPPS

The performance measure of valves in HIPPS is expressed by an average probability that the item will not be able to perform its required safety function if the demand occurs, and it is denoted as Probability of Failure on Demand (PFD_{avg}) [2]. IEC 61508[3] specifies the requirement into four safety integrity levels (SILs), with SIL1 being the least reliable and SIL4 being the most reliable. To fulfill the requirements of a SIL, the SIS in low demand mode must have a PFD_{avg} in the corresponding interval.

Given the inevitable degradation mechanisms in valves, the actual performance of a mechanically final element always degrades along with time. Through the life-cycle of valves, at least three distinguishable states can be defined which are linked with the physical condition of system.

Table 1: System state definition

State	status	notation	state description
1	Working	W	System is working as specified
2	Degraded	D	System has a degraded performance but still functioning
3	Failed	F	System has a fault and fails to function

2.2. Proof test and maintenance strategies

Proof tests address the necessary functional safety requirements of SIS, including functions such as response time and leakage class of safety valves, with reflecting real conditions as accurately as possible. During a test it is possible to check the actual performance of valves, e.g. fully open/closed, the time to perform safety function and leakage rate in closed position. These kind of information can be employed as indirect indicators which provide us an opportunity to prognostics the valve condition [50].

In the designed phase of SISs, the final elements, such as valves, are allocated a target value with acceptable deviation to meet the specified performance requirement, e.g. leakage rate and closing time. When the leakage rate or closing time exceeds the acceptable deviation, as a safety barrier, the valve will not meet the performance requirements for risk mitigating of EUC. The corresponding failure modes are called 'leakage (through the valve) in a closed position (LCP)' and 'closing too slowly', respectively. In most cases, it is not possible to observe such kind of failure without activating the valve, so these failures are DU failures. When DU failure presents, the SIS will be into a fault state as losing the corresponding pre-designed safety function.

LCP failure mode is mainly caused by erosion on the gate or the seat [2]. Referring to the existing studies of erosion in valves, a series of work have been conducted on selection of performance indicator. A potential erosion indicator is the difference value between the calculated result from collected information and a reference value from vendor data sheet. Complied to the performance requirement of SIS, when the difference is too big, the valve is said to be failed (in a fault state).

Considering state classification and the updated status indicator after a proof test, the condition-based maintenance can be adopted to improve system performance: (1) no action if the difference value is quite small, it means the system is the working condition; (2) preventive maintenance (PM) is executed if the difference value is quite big but still within the required range, in this case, the performance is not satisfying even though is still kind of working; (3) corrective maintenance (CM) if the difference value exceeds the required range, namely, a DU is found (with respect to this particular function).

3. SIS modeling and performance analysis

This part firstly presents the relevant modeling assumptions. Markov chain is one approach quoted in IEC 61511 [51] for reliability assessment of SIS. When using Markov chains, it is possible to make a dynamic analysis of the system in each test interval. The state of the tested units are observed and known through periodic proof test, which implies the inapplicability of the classical Markov chain. Thus, the probability that the SIS sojourns in a certain state is known or partially known in each proof test. The proof test and its follow-up maintenance reallocate the distribution of system states from the modeling perspective, and create a new phase in the Markov chain for latter phase. Thus, a multi-phase Markov process is used to model the performance of SIS.

3.1. Assumptions

For unavailability and maintenance analysis, the following assumptions are needed as most of the existing literature:

- DU failures of units follow the exponential distribution;
- All units are repairable and repair time is negligible;
- Proof tests are executed periodically to check system performance and independently for units.
- Both preventive and corrective maintenance once conducted are perfect to make the objective as-good-as-new (AGAN).
- Common cause failures (CCFs) are excluded, with the purpose to illustrate the effects of α_i in a single unit on the redundant structure apparently.

In this study, proof tests are imperfect in revealing degraded states with a revealing probability or testing coverage α_i for unit i. When identifying failed states, tests are perfect.

3.2. Performance analysis

Considering the discrete states assumption, a system can be in $r+1$ distinct states with a state space $\{1, \cdots, r+1\}$. We define the stochastic process $\{X(t), t \geqslant 0\}$ to represent the system state at time t. Vector $\mathbf{P}(t) = [\mathbf{P}_1(t), \mathbf{P}_2(t), \cdots, \mathbf{P}_{r+1}(t)]$ stands for the probabilities of the process in each state at time t. The system is always in one of states, so that the sum of state probabilities should be equal to 1 at any time. A generic mathematical notion of a Markov model is

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{QP}(t) \tag{1}$$

where $\mathbf{Q}$ is the Markov transition matrix containing all transition rates (assumed to be constant in each phase). Considering the periodic proof tests, the overall life cycle of system could be modeled by multi-phase Markov process, the i testing intervals are denoted as $[0, \mathrm{T_1}], [\mathrm{T_1}, \mathrm{T_2}], \cdots, [\mathrm{T_{(i-1)}}, \mathrm{T_i}]$, accompanying with Markov transition matrix $\mathbf{Q}_i$ and $\mathbf{M}_i$ to represent the transition rates and probability matrix of different states after a testing/repair action in the i-th test phase, respectively.

To accompany the set of equations, a set of initial state probabilities $\mathbf{P}(t=0)=\mathbf{P}_0$ is also required. Then by solving Chapman-Kolmogorov's equation, we can calculate system state probabilities at time t in first test phase $[0, \mathrm{T}_1]$.

$$\mathbf{P}(t)=\mathbf{P}_0 \cdot exp(\mathbf{Q}_1 \cdot t) \tag{2}$$

If the time immediately before a test (pretest) at time T_1 is indicated as T_1^- and immediately after a test (post-test) as T_1^+, the effect of test and maintenance actions at time T_1 can be described as

$$\mathbf{P}(\mathrm{T}_1^+)=\mathbf{P}(\mathrm{T}_1^-) \cdot \mathbf{M}_1 \tag{3}$$

where $\mathbf{M}_1$ represents the probability matrix of different states after a testing and repair action. $\mathbf{P}(\mathrm{T}_1^+)$ stands for the state probabilities at time T_1. So, the system state probabilities at time t in second phase can be calculated as:

$$\begin{aligned}
\mathbf{P}(t) &= \mathbf{P}(\mathrm{T}_1^+) \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{t}-\mathrm{T}_1)) \\
&= \mathbf{P}(\mathrm{T}_1^-) \cdot \mathbf{M}_1 \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{t}-\mathrm{T}_1)) \\
&= \mathbf{P}_0 \cdot exp(\mathbf{Q}_1 \cdot \mathrm{T}_1) \cdot \mathbf{M}_1 \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{t}-\mathrm{T}_1))
\end{aligned} \tag{4}$$

Therefore, we can have $\mathbf{P}(\mathrm{T}_2^-)$

$$\begin{aligned}
\mathbf{P}(\mathrm{T}_2^-) &= \mathbf{P}(\mathrm{T}_1^+) \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{T}_2-\mathrm{T}_1)) \\
&= \mathbf{P}_0 \cdot exp(\mathbf{Q}_1 \cdot \mathrm{T}_1) \cdot \mathbf{M}_1 \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{T}_2-\mathrm{T}_1))
\end{aligned} \tag{5}$$

Similarly, $\mathbf{P}(\mathrm{T}_{(\mathrm{i}-1)}^-)$ could be calculated as

$$\begin{aligned}
\mathbf{P}(\mathrm{T}_{(\mathrm{i}-1)}^-) &= \mathbf{P}(\mathrm{T}_{\mathrm{i}-2}^+) \cdot \exp(\mathbf{Q}_{\mathrm{i}-1} \cdot (\mathrm{T}_{\mathrm{i}-2}-\mathrm{T}_{\mathrm{i}-1})) \\
&= \mathbf{P}_0 \prod_{n=1}^{i-2} (exp(\mathbf{Q}_n \cdot (\mathrm{T}_\mathrm{n}-\mathrm{T}_{\mathrm{n}-1})) \cdot \mathbf{M}_\mathrm{n}) \cdot \exp(\mathbf{Q}_\mathrm{i} \cdot (\mathrm{T}_{\mathrm{i}-1}-\mathrm{T}_{\mathrm{i}-2}))
\end{aligned} \tag{6}$$

Then if t is in the i testing phase $[\mathrm{T}_{(\mathrm{i}-1)}, \mathrm{T}_\mathrm{i}]$, we can have $\mathbf{P}(t)$

$$\begin{aligned}
\mathbf{P}(t) &= \mathbf{P}(\mathrm{T}_{\mathrm{i}-1}^-) \cdot \mathbf{M}_{\mathrm{i}-1} \cdot \exp(\mathbf{Q}_\mathrm{i} \cdot (\mathrm{t}-\mathrm{T}_{\mathrm{i}-1})) \\
&= \mathbf{P}_0 \prod_{n=1}^{i-1} (exp(\mathbf{Q}_n \cdot (\mathrm{T}_\mathrm{n}-\mathrm{T}_{\mathrm{n}-1})) \cdot \mathbf{M}_\mathrm{n}) \cdot \exp(\mathbf{Q}_\mathrm{i} \cdot (\mathrm{t}-\mathrm{T}_{\mathrm{i}-1}))
\end{aligned} \tag{7}$$

For a 1oo1 configuration, the system will not be functional in the failed state, and the instantaneous PFD(t) in each testing phase is given by

$$\mathrm{PFD}(t)=\Pr(X(t)=F)=\mathbf{P}(t) \cdot [0,0,1]^{\mathbf{T}} \tag{8}$$

Meanwhile, for a 1oo2 configuration, the system will not be functional when both of two units are in the failed states, then the instantaneous PFD(t) is given by

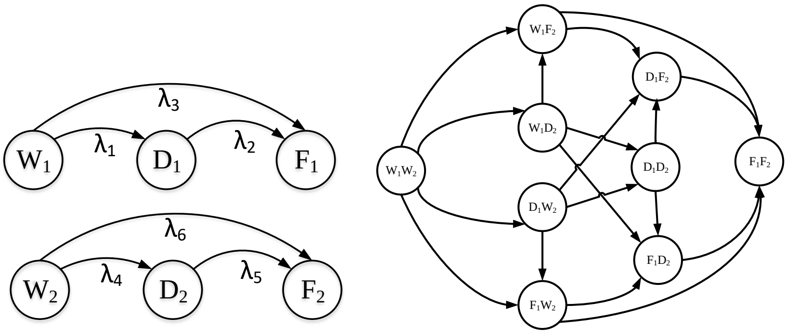
$$\mathrm{PFD}(t) = \Pr(X(t) = \mathrm{FF}) = \mathbf{P}(t) \cdot [0, 0, 0, 0, 0, 0, 0, 0, 1]^{\mathbf{T}} \tag{9}$$

Then performance measure of system, $\mathrm{PFD}^{\mathrm{i}}_{\mathrm{avg}}$, in i-th testing phase is given by

$$\mathrm{PFD_{avg}}^{i} = \frac{1}{T_i - T_{i-1}} \int_{T_{i\ \ 1}}^{T_i} \mathrm{PFD}(t)dt \tag{10}$$

3.3. Modeling for proof tests and maintenances

In this paper, each unit in a 1oo2 configuration is assumed to have three states, including working, degraded and failed. The transition diagram for 1oo1 and 1oo2 configuration is shown in Fig. 2, the corresponding transition matrix is **Q** as shown in Appendix B.



(a) (b)

Figure 2: state transition diagrams for (a)1oo1 configuration and (b) 1oo2 configuration

As assumptions in Section 3.1, proof tests are perfect in revealing failed states, but imperfect in revealing degraded states. To quantify such imperfectness, a coverage indicator α is defined as the conditional probability that a degraded state will be detected by the proof test, given that degradation has occurred when initiating the proof test.

$$\alpha = \Pr(\text{Degradation is detected in a proof test } |\text{Degradation has occurred}) \tag{11}$$

The parameter α does not affect the transition matrix and diagram as the unrevealed degraded state is physically in degraded. Since the maintenance actions are based on the detected state of system, the imperfectness in revealing of degraded state should be taken into matrix which upon testing and maintenance actions.

3.3.1. Testing strategies

Two different testing strategies for a redundant structure of SIS final element will be investigated here, include:

- Simultaneous testing: Two units are tested at (almost) same time with a fixed interval τ. The i-th proof test is executed at time $t_i = i\tau, (i = 1, 2, \cdots)$, and independently for two units.
- Staggered testing: Two units are tested at different times with a constant test interval. Here, we assume that unit 1 is tested at time $t_{2j-1} = (2j-1)\times\tau/2$ and unit 2 at time $t_{2j} = (2j)\times\tau/2$, $(j = 1, 2, \cdots)$, since $\tau/2$ has been identified as the optimal interval [52].

3.4. Follow-up maintenance strategies

Considering the aforementioned testing strategies, several optional maintenance strategies are proposed for 1oo2 configuration:

- Strategy I: Under the simultaneous testing policy, the tests for two units are two separate processes. A PM or CM action will be executed if any unit is found in the degraded or failed state in test. Both PM and CM actions are perfect and make units as-good-as-new.
- Strategy II: Under the staggered testing policy, repair actions are only executed on the tested unit. A PM or CM will be executed when the tested unit is in degraded or failed state, respectively. Since no information of another unit is collected during the testing, then no repair is executed on the untested unit.
- Strategy III: Opportunistic maintenance with perfect action under the staggered testing policy. The maintenance policy is described as follows: 1. PM will be executed for tested degraded unit and perform CM if the tested unit fails. 2. At the moment of CM, this opportunity is taken to perform a replacement action on the other unit no matter the actual state is.

3.5. Life-cycle cost

Life-cycle cost for final elements in SISs mainly consists of purchase, installation, maintenance and disposal, while almost three-quarters of total cost goes for maintenance while one fifth goes for purchase[53]. The huge proportion for maintenance cost represents an opportunity for cost reduction.

The acknowledged maintenance criteria is to optimize certain parameter with renewal theorem. Differ from usual production systems, most SISs are designed with finite service time and thus the steady-state criteria is not applicable[29]. Therefore, the life-cycle cost of SISs could be estimated by the sum of expected cost after each proof test.

To quantify the life-cycle cost, several cost items related maintenance and testing actions are defined as: C_0,C_{PT},C_{PM},C_{CM} represents one-time installation cost per unit, proof test cost per unit, preventive maintenance cost and corrective maintenance cost (purchase) per unit, respectively.

The expected maintenance cost after i-th test (EC_i) should equal to the sum of proof test cost (EC_{PT}), expected PM cost (EC_{PM}) and CM cost (EC_{CM}) in i-th test interval, where expected cost depends on the system state probability and corresponding maintenance actions.

$$EC_i = EC_{PT} + EC_{\text{PM}} + EC_{\text{CM}} \tag{12}$$

Considering the imperfectness of revealing degraded state, the expected maintenance cost should be linked with parameter α, for 1oo1 configuration after the first test,

$$\begin{aligned} EC_{\text{PM}} &= \mathbf{P}_2(\tau^-) \cdot \mathrm{C}_{\text{PM}} = \mathbf{P}_2(\tau^+) \cdot \alpha \cdot \mathrm{C}_{\text{PM}} \\ EC_{\text{CM}} &= \mathbf{P}_3(\tau^-) \cdot \mathrm{C}_{\text{CM}} = \mathbf{P}_3(\tau^+) \cdot \mathrm{C}_{\text{CM}} \end{aligned} \tag{13}$$

Then the expected maintenance cost EC_1 for 1oo1 configuration SIS after first test can be expressed as following,

$$EC_1 = C_{PT} + \mathbf{P}((\tau)^+) \cdot \begin{pmatrix} 0 \\ \alpha \cdot C_{\text{PM}} \\ C_{\text{CM}} \end{pmatrix} \tag{14}$$

Afterwards, the total expected life-cycle cost (LCC) for 1oo1 configured SIS in n test intervals can be estimated as

$$\text{LCC} = C_0 + \sum_{i=1}^{n} EC_i \tag{15}$$

Similarly, the expected maintenance cost for 1oo2 configuration after single proof test with 200 Strategy I can be estimated as Eq. (16),

$$EC_i = 2C_{PT} + \mathbf{P}((i\tau)^+) \cdot \begin{pmatrix} 0 \\ \alpha_2 \cdot C_{\text{PM}} \\ C_{\text{CM}} \\ \alpha_1 \cdot C_{\text{PM}} \\ \alpha_1 \cdot (1-\alpha_2) \cdot C_{\text{PM}} + \alpha_1 \cdot (1-\alpha_2) \cdot C_{\text{PM}} + 2 \cdot \alpha_1 \cdot \alpha_2 \cdot C_{\text{PM}} \\ \alpha_1 \cdot (C_{\text{PM}} + C_{\text{CM}}) + (1-\alpha_1) \cdot C_{\text{CM}} \\ C_{\text{CM}} \\ \alpha_2 \cdot (C_{\text{PM}} + C_{\text{CM}}) + (1-\alpha_2) \cdot C_{\text{CM}} \\ 2C_{\text{CM}} \end{pmatrix} \tag{16}$$

the total expected life-cycle cost (LCC) for 1oo2 configured SIS with Strategy I in n test intervals can be estimated as

$$\text{LCC} = 2 \cdot C_0 + \sum_{i=1}^{n} EC_i \tag{17}$$

For Strategy II, unit 1 is tested at time $t_{2j-1} = (2j-1) \times \tau/2$ and unit 2 at time $t_{2j} = (2j) \times \tau/2$, $(j = 1, 2, \cdots)$, the expected cost after single test can be estimated by Eq. (18).

$$\begin{aligned} EC_{2j-1} &= C_{PT} \\ &\quad + \mathbf{P}(((2j-1) \cdot \tau/2)^+) \cdot (0, 0, 0, \alpha_1 \cdot C_{\text{PM}}, \alpha_1 \cdot C_{\text{PM}}, \alpha_1 \cdot C_{\text{PM}}, C_{\text{CM}}, C_{\text{CM}}, C_{\text{CM}})^{\mathbf{T}} \\ EC_{2j} &= C_{PT} \\ &\quad + \mathbf{P}(((2j) \cdot \tau/2)^+) \cdot (0, \alpha_2 \cdot C_{\text{PM}}, C_{\text{CM}}, 0, \alpha_2 \cdot C_{\text{PM}}, C_{\text{CM}}, 0, \alpha_2 \cdot C_{\text{PM}}, C_{\text{CM}})^{\mathbf{T}} \end{aligned} \tag{18}$$

Similarly, for Strategy III, the expected cost after each test can be estimated by Eq. (19).

$$\begin{aligned} EC_{2j-1} &= C_{PT} \\ &\quad + \mathbf{P}(((2j-1) \cdot \tau/2)^+) \cdot (0, 0, 0, \alpha_1 \cdot C_{\text{PM}}, \alpha_1 \cdot C_{\text{PM}}, \alpha_1 \cdot C_{\text{PM}}, 2C_{\text{CM}}, 2C_{\text{CM}}, 2C_{\text{CM}})^{\mathbf{T}} \\ EC_{2j} &= C_{PT} \\ &\quad + \mathbf{P}(((2j) \cdot \tau/2)^+) \cdot (0, \alpha_2 \cdot C_{\text{PM}}, 2 \cdot C_{\text{CM}}, 0, \alpha_2 \cdot C_{\text{PM}}, 2 \cdot C_{\text{CM}}, 0, \alpha_2 \cdot C_{\text{PM}}, 2 \cdot C_{\text{CM}})^{\mathbf{T}} \end{aligned} \tag{19}$$

Using Eq. (17), the total expected LCC for 1oo2 configuration under Strategy I in a finite lifetime can be estimated by summing up the expected cost from Eq. (16). Similar equations could be conducted for Strategy II and Strategy III by summing up results from Eq. (18) and Eq. (19), respectively.

4. Numerical example

To illustrate the proposed model and maintenance strategies, a numerical example is conducted here. Assumed parameters for transition rates in the example are listed in Table 2.

Table 2: Parameter value

Parameter	value
λ_1	8E-6
λ_2	2E-5
λ_3	4E-6
λ_4	8E-6
λ_5	2E-5
λ_6	4E-6
τ	8760

4.1. Effect of α on the performance of a 1oo1 configuration

To investigate the effect of imperfectness in revealing degraded state α on the 1oo1 configuration, a perfect PM or CM will be executed if the system is manifested in degraded or failed state in proof tests. The effect of coverage α of proof test in revealing degraded state is shown in Fig. 3. It is easy to notice that the testing coverage α has an obvious effect on system PFD(t). In the first test phase $(0, \tau)$, system PFD(t) is overlapped when $\alpha = 0, 0.5, 1$, thanks to the same initial state probability $\mathrm{P}(t) = [1, 0, 0]$ at $t = 0$. When $\alpha = 1$, the proof testings are perfect in revealing degraded states and failed state, the element will reach a stable and lowest tendency since the initial state is $\mathrm{P}(t) = [1, 0, 0]$ in each test phase. When $\alpha < 1$, the system is still possible in the degraded state after perfect PM or CM, and then the initial state of the system in each phase is $\mathrm{P}(t) = [1 - \alpha\mathrm{P}_2(t^-), \alpha\mathrm{P}_2(t^-), 0]$. Consequently, system PFD(t) is increasing with time under imperfect testing as $\alpha = 0$ and $\alpha = 0.5$ in each test phase as shown in Fig. 3. When $\alpha = 0$, the system PFD(t) reaches the highest value in same test phase.

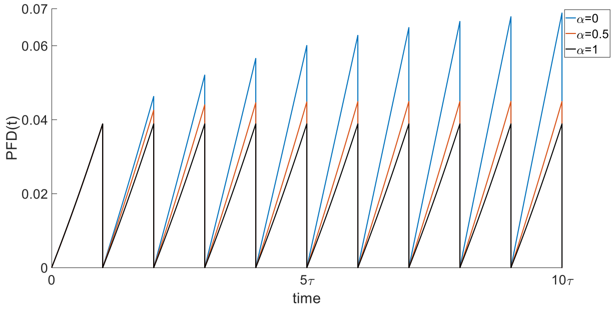


Figure 3: PFD(t) of 1oo1 configuration

4.2. Effect of α on the performance of a 1oo2 configuration

Performance of a 1oo2 configuration is analyzed according to the proposed testing and maintenance strategies respectively.

4.2.1. Simultaneous testing with maintenance strategy I

For strategy I, given the imperfect revealing coverage on degraded state for two units, undoubtedly, the observed state probabilities will not be equal to the actual physical ones when $\alpha_i < 1$. According to assumptions in section 3.1, test and repair time is assumed to be negligible. The instantaneous state transition process at time time $i\tau, i = 1, 2, ...$ with revealing coverage α_1 and α_2 on degraded state for selected states are shown in Table. 3. The whole matrix regarding test and repair is shown as $\mathbf{M}$ in Appendix B.

System PFD(t) and selected state probabilities of 1oo2 configuration with strategy I are shown in Fig. 4.

System PFD(t) is increasing under strategy I with the set parameters in Table 2 when $\alpha_i < 1$, meaning that system unavailability is increasing in each testing phase. In Fig. 4(a), the test coverage of revealing degraded state α_1 for unit 1 has a more evident effect on PFD(t) with time when $\alpha_2 = 1$. When α_1 closes to 1, PFD(t) has a slowing decrease with α_1 in each test interval. System PFD(t) with $\alpha_1 = 0.8$ is almost overlapping with that of $\alpha_1 = 1$. Selected state probabilities with $\alpha_1 = 0.2, \alpha_2 = 1$ is shown are 4(b). When $\alpha_2 = 1$, the degraded state of unit 2 will be revealed perfectly after each test. Then the state probabilities for state 2 (W_1D_2) and 5 (D_1D_2) will decrease to 0 at the beginning of each test phase. Meanwhile, the state probability of state 4

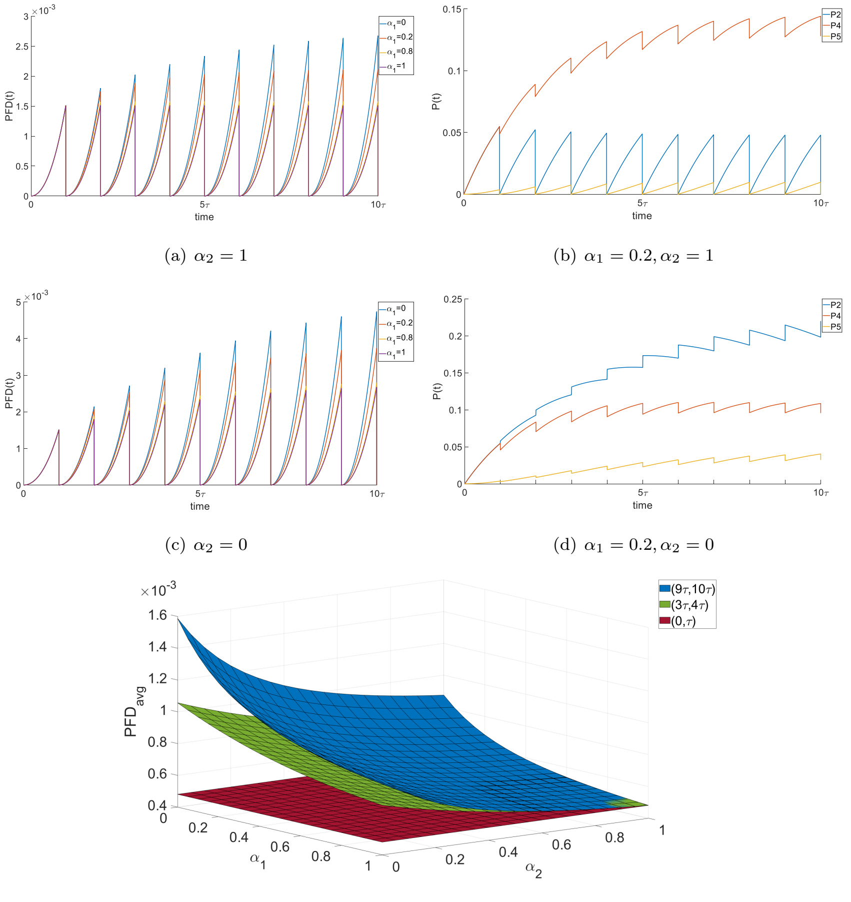
Table 3: Instantaneous state transition at test time $i\tau$ with strategy I

physical at $i\tau^-$	after test	after repair	physical at $i\tau^+$
F_1D_2	α_2 F_1D_2	α_2 W_1W_2	α_2 W_1W_2
	$1-\alpha_2$ F_1W_2	$1-\alpha_2$ W_1W_2	$1-\alpha_2 W_1D_2$
D_1D_2	$\alpha_1\alpha_2$ D_1D_2	$\alpha_1\alpha_2$ W_1W_2	$\alpha_1\alpha_2$ W_1W_2
	$\alpha_1(1-\alpha_2)$ D_1W_2	$\alpha_1(1-\alpha_2)$ W_1W_2	$\alpha_1(1-\alpha_2)W_1D_2$
	$(1-\alpha_1)\alpha_2$ W_1D_2	$(1-\alpha_1)\alpha_2$ W_1W_2	$(1-\alpha_1)\alpha_2D_1W_2$
	$(1-\alpha_1)(1-\alpha_2)$ W_1W_2	-	$(1-\alpha_1)(1-\alpha_2)$ D_1D_2
D_1F_2	α_1 D_1F_2	α_1 W_1W_2	α_1 W_1W_2
	$1-\alpha_1$ W_1F_2	$1-\alpha_1$ W_1W_2	$1-\alpha_1D_1W_2$

(D_1W_2) should theoretically equal to 0. But, given the imperfect revealing coverage for unit 1, the state probability $P_4(i\tau^-)$ decreases at each test point ($P_4(i\tau^-) < P_4(i\tau^+)$) with overall increases ($P_4(i\tau^-) < P_4((i+1)\tau^-)$) instead, which comes from the partly imperfect repair of state 5 (D_1D_2) and 6 (D_1F_2) as shown in Table 3.

Similar as system PFD(t) tendency in Fig. 4(a), PFD(t) in Fig. 4(c) is also increasing along with time. In each test phase, PFD(t) monotonically increases in each test phase and reaches a maximum at $i\tau^+, i = 1, 2, \cdots$. PFD($t$) decreases slowly with a higher α_1. State probabilities $P_2(t), P_4(t)$ and $P_5(t)$ in Fig. 4(d) show different tendencies compared to Fig. 4(b). Since $\alpha_2 = 0$, no degraded state for unit 2 is revealed in proof tests. For state 2 (W_1D_2), $P_2(i\tau^+) > P_2(i\tau^-)$, the increment comes from the partly repair of state 5 (D_1D_2) and 6 (D_1F_2) as described in Table 3. $P_5(i\tau^-)$ will be divided into four possible states 5(D_1D_2), 4(D_1W_2), 2(W_1D_2)and 1(W_1W_2) with portions 0,0.2,0,0.8, respectively. When the system is in $P_5(i\tau^-)$, it has 20% of probability to be repaired, and the probability of being skipped is 80%.

System PFD_{avg} with α_1 and α_2 in selected test phases is shown in Fig. 4(e). In first test phase (0,τ), PFD_{avg} shows a flat surface with the value of 4.81×10^{-4} for independent on α_1 and α_2. It means that the system performance in first phase is only depending on the initial state vector and the length of test. It is reasonable to conclude that system PFD_{avg} is increasing with time, since showing a highest value for 10th with an intermediate and lowest value for 4th and 1st test phase in Fig. 4(e), respectively. Meanwhile, it is not difficult to notice that PFD_{avg} reaches a minimum



(a) $\alpha_2 = 1$

(b) $\alpha_1 = 0.2, \alpha_2 = 1$

(c) $\alpha_2 = 0$

(d) $\alpha_1 = 0.2, \alpha_2 = 0$

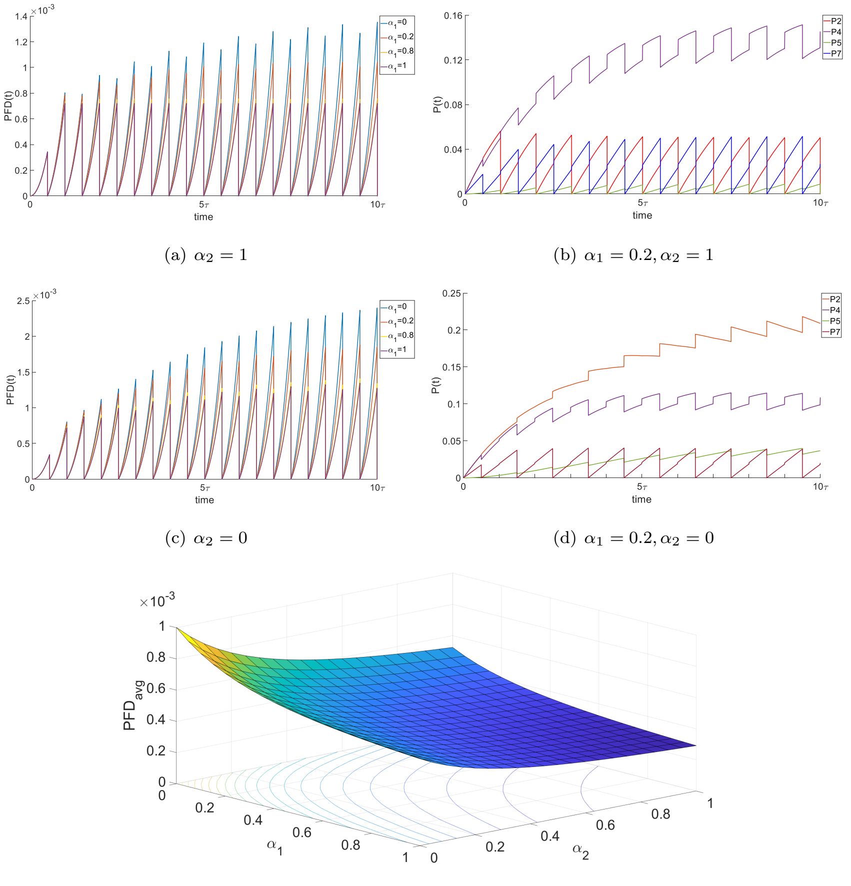
(e) $\mathrm{PFD}_{\mathrm{avg}}$ in 1st, 4th and 10th test phase

Figure 4: PFD(t) and selected state probabilities of 1oo2 configuration under strategy I

value when $\alpha_1 = \alpha_2 = 1$ and a maximum value when $\alpha_1 = \alpha_2 = 0$ with up to 1.59×10^{-3} for 10th and 1.06×10^{-3} in 4th test phase. This finding also provide clues to take system $\mathrm{PFD}_{\mathrm{avg}}$ in final test phase as a reference in the whole life-cycle in the further discussions.

4.2.2. Staggered testing with maintenance strategy II

The point of testing for unit 1 is shifted with a time $\tau/2$ compared to the unit 2. And unit 1 is tested at $t_{2j-1} = (2j-1) \times \tau/2$ and unit 2 at time $t_{2j} = (2j) \times \tau/2$, $(j = 1, 2, \cdots)$. System PFD(t) of 1oo2 configuration with strategy II is shown in Fig. 5. In the first testing phase, system PFD(t) has no relation with either α_1 or α_2 thanks to the same initial state probability $\mathbf{P}_0$.



(a) $\alpha_2 = 1$

(b) $\alpha_1 = 0.2, \alpha_2 = 1$

(c) $\alpha_2 = 0$

(d) $\alpha_1 = 0.2, \alpha_2 = 0$

(e) PFD$_{\text{avg}}$ in $(9.5\tau, 10\tau)$

Figure 5: PFD(t) and selected state probabilities of 1oo2 configuration under strategy II

As mentioned in section 3.4, the staggered testing procedure introduces two separate matrices, which are shown in Appendix B, $\mathbf{M}_{U_1}$ is valid after a test of unit 1 and $\mathbf{M}_{U_2}$ is valid after a test of unit 2. When $\alpha_2 = 1$, in Fig. 5(a), system PFD(t) increases with a lower value of α_1 in each testing phase. Several system states, e.g. state 4(D_1W_2), state 5(D_1D_2) and state 6(D_1F_2) will still be hidden and not be repaired during the testing of unit 1 when $\alpha_1 \neq 0$. Because of the alternation and imperfect coverage, these hidden states after testing of unit 1 contribute to a fluctuating PFD(t) in the consecutive testing phase of unit 2. Similar tendencies are demonstrated in Fig. 5(c) with $\alpha_2 = 0$.

Selected state probabilities with $\alpha_1 = 0.2, \alpha_2 = 1$ are shown in Fig. 5(b). For example, state probability $P_4(t)$ for state 4 (D_1W_2) decreases instantly after testing of unit 1 because of the imperfect coverage α_1 but jumps to a higher value given the repair of state 5 (D_1D_2) and state 6 (D_1F_2) after testing of unit 2. Similarly, compared to Fig. 5(b), the lower increment magnitude of $P_4(t)$ in Fig. 5(d) comes from the the repair of state 6 (D_1F_2) since no state 5 (D_1D_2) is revealed with $\alpha_2 = 0$ in tests of unit 2.

It is worth noting that there are two specific cases: (1) $\alpha_1 = 0, \alpha_2 = 0$ (2) $\alpha_1 = 1, \alpha_2 = 1$.

(1) When $\alpha_1 = 0, \alpha_2 = 0$, it means that even the physical state of unit has shifted from working to degraded state, but no degraded states for either unit 1 or unit 2 are revealed in tests. Consequently, no PM will be executed. Therefore, system PFD(t) reaches a maximum value in each test phase, as shown in Fig. 5(c). This finding is also demonstrated by the maximum value of system PFD_{avg} in $(9.5\tau, 10\tau)$ after test of unit 1 at time 9.5τ in Fig. 5(e). Meanwhile, PFD_{avg} increases with a higher magnitude when either α_1 or α_2 is closing to 0.

(2) When $\alpha_1 = 1, \alpha_2 = 1$, it means that degraded state of unit 1 and unit 2 will be perfectly revealed in the tests. Corresponding repair actions are taken, system PFD(t) reaches a stable tendency and minimum value after few phases since two units are assumed identical with same transition rates.

To demonstrate the effect of transition rates, a brief study is conducted here. The transition rates for unit 1 keep the same values as in Table 2. Four optional unit 2 for 1oo2 configuration, which marked as Unit 21, 22, 23 and 24, are listed in Table 4 with different transition rates. For the simplification in the following, symbol 'set i' is employed to stand for the 1oo2 configuration with unit 1 and unit 2i.

Table 4: Different transition rates for unit 2

Parameter	Value			
	Unit 21	Unit 22	Unit 23	Unit 24
λ_4	0.5×8E-6	8E-6	2×8E-6	3×8E-6
λ_5	0.5×2E-5	2E-5	2×2E-5	3×2E-5
λ_6	0.5×4E-6	4E-6	2×4E-6	3×4E-6

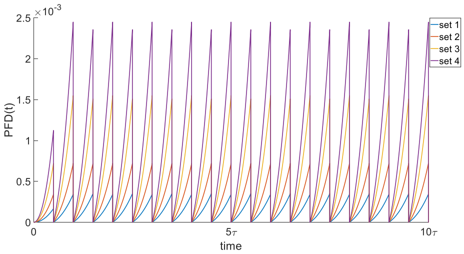


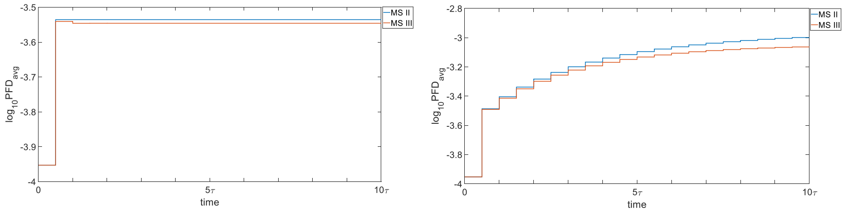
Figure 6: PFD(t) of 1oo2 configuration under strategy II

The calculation result of PFD(t) for the 1oo2 configuration under strategy II with nonidentical units are shown in Fig. 6. It is obvious that system PFD(t) increases with higher values of transition rates for unit 2. Given the unequal transition rates for two units, system PFD(t) fluctuates when $\alpha_1 = \alpha_2 = 1$ with the test of unit 1 and 2 except a stable tendency for set 2.

4.2.3. Staggered testing with maintenance strategy III

The main difference between strategy II and strategy III is an additional replace action on the untested unit. It is easy to infer that system PFD_{avg} will be to some extent lower with strategy III compared to strategy II. Similarly as strategy II, the staggered testing procedure introduces two separate matrices, which are shown in Appendix B, $\mathbf{M}_{U_1}$ is valid after a test of unit 1 and $\mathbf{M}_{U_2}$ is valid after a test of unit 2.

System PFD_{avg} results with parameters from Table 2 under two strategies are shown in Fig.7. When $\alpha_1 = \alpha_2 = 1$, in Fig. 7(a), system PFD_{avg} reaches a constant value 2.91×10^{-4} with strategy II and a lower value with strategy III, at 2.84×10^{-4}, representing 2.45% decrease.



(a) $\alpha_1 = \alpha_2 = 1$

(b) $\alpha_1 = \alpha_2 = 0$

Figure 7: System $\mathrm{PFD}_{\mathrm{avg}}$ comparison between strategy II and strategy III

When $\mathrm{PFD}_{\mathrm{avg}}$ if $\alpha_1 = \alpha_2 = 0$, only failed unit will be restored to working state. In Fig. 7(b), it is obvious that system $\mathrm{PFD}_{\mathrm{avg}}$ keeps increasing with time with strategy II and III. Strategy III has a more evident advantage along with time on $\mathrm{PFD}_{\mathrm{avg}}$.

The main shortcoming of strategy III is the abuse of restoring the untested unit, which consequently will contribute to a increasing maintenance cost. Therefore, the upcoming consideration is how to balance the decreased $\mathrm{PFD}_{\mathrm{avg}}$ and economic loss.

4.2.4. $\mathrm{PFD}_{\mathrm{avg}}$ *comparisons among proposed strategies*

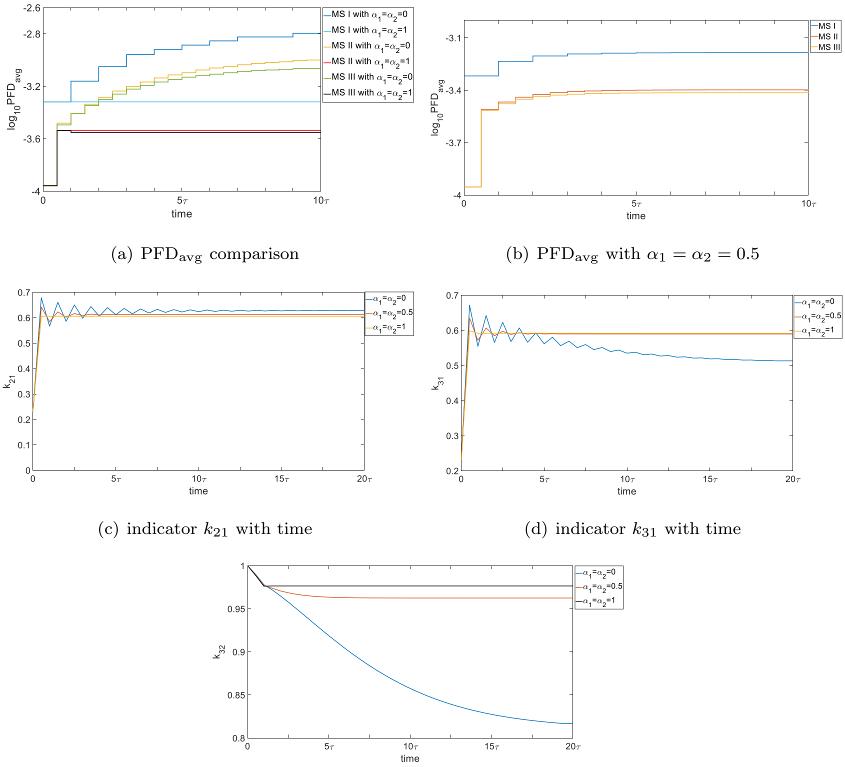
For strategy I with $\alpha_1 = \alpha_2 = 1$, either degraded or failed state will be repaired. The system state probabilities will be same as initial vector $\mathbf{P}_0$, which leads to a stable performance of system in each test phase. As proved in previous sections, system will have a lower $\mathrm{PFD}_{\mathrm{avg}}$ with $\alpha_1 = \alpha_2 = 1$ in same strategy. When α_1 and α_2 take same values, staggered test (strategy II and III) can lead to a better system performance than simultaneous test (strategy I).

For $\alpha_1 = \alpha_2 = 1$, in Fig. 8(a), system $\mathrm{PFD}_{\mathrm{avg}}$ under strategy II and III is up to 60.6% and 59.2% of that under strategy I, respectively. In $(9.5\tau, 10\tau)$, the corresponding value is 63.1% and 54.4% for $\alpha_1 = \alpha_2 = 0$. It is worth mentioning that, in Fig. 8(b), system performance meet SIL 3 with $\alpha_1 = \alpha_2 = 0.5$ under any of proposed maintenance strategy.

To quantify the differences for $\mathrm{PFD}_{\mathrm{avg}}$ under proposed strategies, an indicator k_{ji} is proposed here as following,

$$k_{ji} = \frac{\mathrm{PFD}_{\mathrm{avg}} \text{ with strategy } j}{\mathrm{PFD}_{\mathrm{avg}} \text{ with strategy } i} \tag{20}$$

In Fig. 8(c) and Fig. 8(d), indicator k_{21} and k_{31} fluctuates with time thanks to the unstable performance for 1oo2 configuration in the early stage when $\alpha_1 = \alpha_2 = 0$, meanwhile, fluctuations



(a) $\mathrm{PFD}_{\mathrm{avg}}$ comparison

(b) $\mathrm{PFD}_{\mathrm{avg}}$ with $\alpha_1 = \alpha_2 = 0.5$

(c) indicator k_{21} with time

(d) indicator k_{31} with time

(e) indicator k_{32} with time

Figure 8: Summary of system $\mathrm{PFD}_{\mathrm{avg}}$ based on proposed strategies

of k_{21} and k_{31} decreases gradually along with time.

From Fig. 8(c), the indicator k_{21} gradually reaches a constant value under the specified value of α_1 and α_2 after around 10τ. The overall of effects of strategy II can be approximated estimated in the range of $(0.6, 0.65)$ of strategy I. To infer from these findings that indicator k_{21} has quite weak relation with the value of α_1 and α_2 when the service time is quite long.

However, the indicator k_{31} shows a non-identical tendency in Fig. 8(d). $\mathrm{PFD}_{\mathrm{avg}}$ of strategy III mainly located in the range of $(0.5, 0.6)$ with that of strategy I. Imprecision of revealing coverage in tests shows a more obvious effect on $\mathrm{PFD}_{\mathrm{avg}}$ when α_1 and α_2 is less than 0.5. For example, k_{31}

equals to 0.513 for $\alpha_1 = \alpha_2 = 0$ at 20τ, while 0.589 and 0.592 for $\alpha_1 = \alpha_2 = 0.5$ and $\alpha_1 = \alpha_2 = 1$, respectively.

Fig. 8(e) depicts the differences between strategy II and III regarding imprecision revealing coverage α_1 and α_2 in tests. It demonstrates that system has a better performance under strategy III than strategy II as the indicator $k_{32} < 1$, which complies to the findings in Fig. 8(a) and Fig. 8(b). Similar as k_{31} in Fig. 8(d), indicator k_{32} shifts from 0.817 to 0.962 when α_1 and α_2 from 0 to 0.5 at 20τ, while only from 0.962 to 0.976 when α_1 and α_2 from 0.5 to 1. In the long run, strategy III results in an optimistic system performance compared to strategy I and II when the test coverage is quite low.

To conclude, for system PFD_{avg}, staggered test could lead to a better system performance that simultaneous test when the state revealing coverage α_i takes same value. Meanwhile, strategy III is ahead of strategy II to some extent, which is strongly linked with parameter α_i.

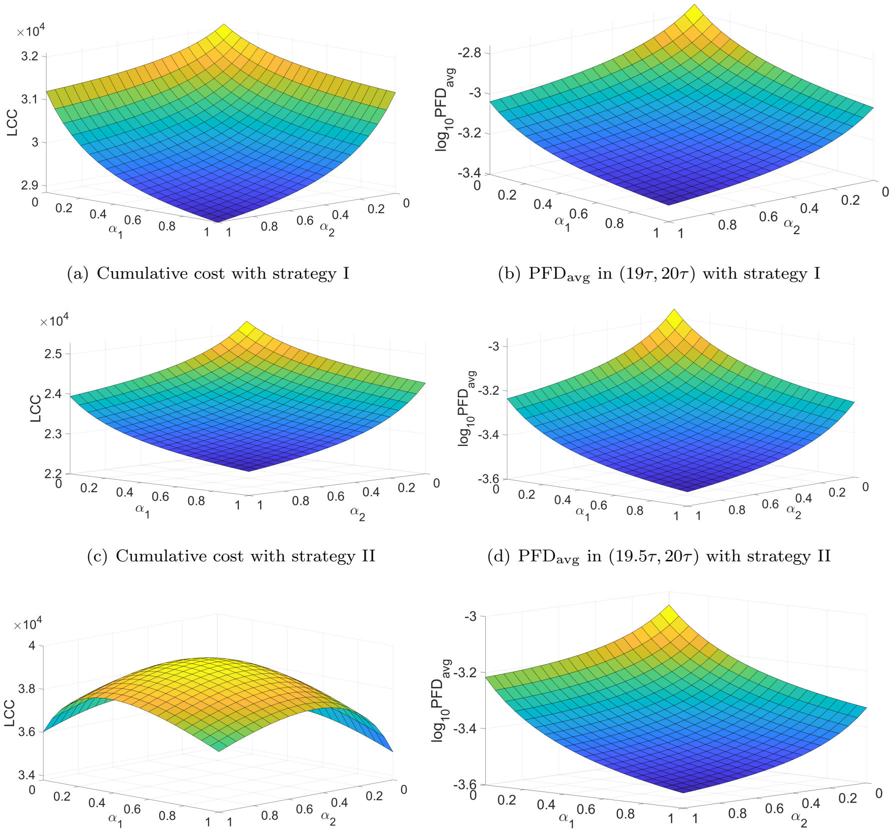
4.2.5. Life-cycle cost

Life-cycle cost items and corresponding values are partly adopted from [47]. Maintenance cost parameters and values are presented in the following Table. 5. Based on the finding in Section 4.2, system PFD_{avg} in final test phase is used as a reference of system performance in the whole life-cycle.

Table 5: Parameter value regarding maintenance and test items

Parameter	Item	value
C_0	One-time installation cost per unit	600
C_{PT}	test cost per unit	60
C_{PM}	preventive maintenance cost per unit	240
C_{CM}	corrective maintenance (purchase) cost per unit	6940

Cumulative maintenance cost for 1oo2 configuration in 20τ with different strategies are depicted in Fig. 9.



(a) Cumulative cost with strategy I

(b) $\mathrm{PFD_{avg}}$ in $(19\tau, 20\tau)$ with strategy I

(c) Cumulative cost with strategy II

(d) $\mathrm{PFD_{avg}}$ in $(19.5\tau, 20\tau)$ with strategy II

(e) Cumulative cost with strategy III

(f) $\mathrm{PFD_{avg}}$ in $(19.5\tau, 20\tau)$ with strategyIII

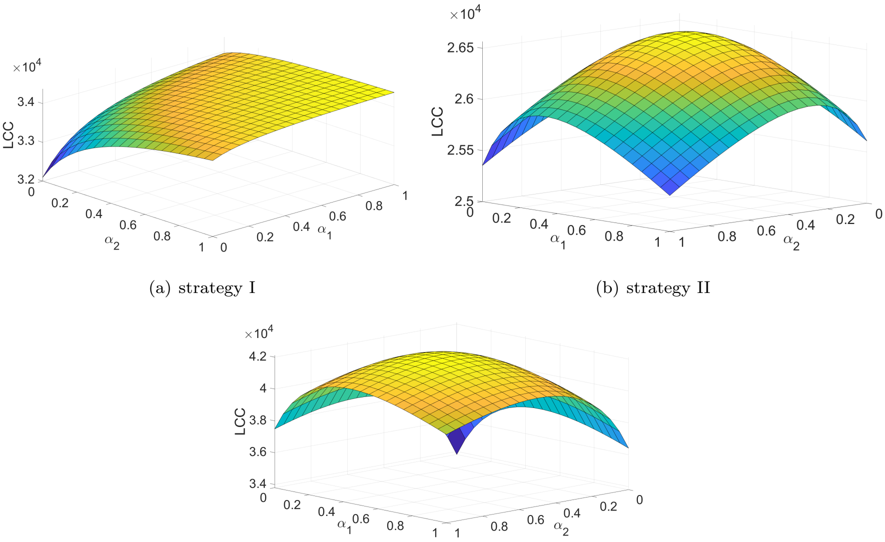
Figure 9: Cumulative maintenance cost in 20τ

In Fig. 9(a), it is obvious that cumulative maintenance cost reaches a maximum value with $\alpha_1 = \alpha_2 = 0$ and a minimum value when $\alpha_1 = \alpha_2 = 1$. Cumulative maintenance cost decreases universally with a higher state revealing probability α_i. When the revealing probability is quite low, the SIS will be remained at the degraded state after proof test. The hidden degraded state will gradually develop to failed state, which will contribute an expensive CM cost compared to PM. This finding is demonstrated by the tendency of $\mathrm{PFD_{avg}}$ in $(19\tau, 20\tau)$ in Fig. 9(b). System performance in $(19\tau, 20\tau)$ locates in SIL2 with quite low revealing test coverage, while in SIL3 with a better revealing coverage.

LCC with coverage α_i under strategy II in Fig. 9(c) shows a similar tendency but a lower value than that under strategy I in Fig. 9(a). Considering different test sequences of units 1 and 2, $\mathbf{P}(i\tau^+)$ will redistribute after the prior test and maintenance. The redistribution of state probabilities contributes to the phenomena that LCC is asymmetry about $\alpha_1 = \alpha_2$ given the certain testing sequences of unit 1 and 2, similar result also can be drawn for strategy III in Fig. 9(e).

Distinguished from those by strategies I and II, LCC under strategy III reaches a minimum value when $\alpha_1 = \alpha_2 = 0$, namely, CM would only be executed when an item fails. When $\alpha_i \neq 0$, an additional CM on untested unit will be executed along with the PM for tested unit. Consequently, this maintenance action contributes to a higher life-cycle cost. Given $\mathbf{P}(i\tau^+)$ is time-dependent and α_i-dependent, the whole LCC in 20τ is not a monotonic with α_i. In fact LCC increases with α_i and reaches a peak, subsequently, decreases slightly. When revealing coverage α_i is quite low, less PMs will be taken, but which could lead to higher possibility of CM. PM cost contributes to an increment in accumulation with coverage α_i at first. When the efficiency of proof tests on degraded state is higher, PM increases and potential CM cost decreases as well. Decrement of potential CM contributes to a decline accumulative cost with higher coverage α_i.

Another potential doubt here is that PM cost is far less than CM (purchase) with values in Table. 5. Therefore, a further calculation is conducted here with $C_{\text{PM}} = 2400$. PFD_{avg} should be independent with the value of C_{PM}. The accumulative LCC in 20 years with different strategies is shown in Fig. 10.



(a) strategy I

(b) strategy II

(c) strategy III

Figure 10: Cumulative maintenance cost in 20τ with an expensive PM cost

It is obvious that each strategy has a higher cost with an expensive PM cost than previous results in Fig. 9. Inconsistent with the result in Fig. 9(a), LCC under strategy I has a minimum value when $\alpha_1 = \alpha_2 = 0$ and a maximum value when $\alpha_1 = \alpha_2 = 1$. It implies that the cumulative PM cost takes a higher proportion in life-cycle. For strategy II, LCC increases with α_i and reaches a peak, subsequently, decreases slightly, which is similar as the result with strategy III in Fig. 9(e). When it comes to strategy III, thanks to the opportunistic replacement of untested unit when maintenance action is executed on tested unit, the tendency of accumulative cost should be consistent with Fig. 9(e).

Combined the results from Fig. 9 and Fig. 10, generally, from the aspect of LCC, it is easy to conclude that strategy III > strategy I >strategy II in 20τ. But when the PM cost is quite high, the LCC in 20τ have an obvious increment, namely, the maintenance actions also need to be considered carefully. As for PFD_{avg}, from the result in Fig. 9(b), Fig. 9(d) and Fig. 9(f), system performance with staggered test is universally better than simultaneous test. System with simultaneous test in

$(19\tau, 20\tau)$ is within SIL2 and SIL3. For strategy II, except the extreme low revealing coverage of degraded state ($\alpha_1 < 0.2$ and $\alpha_2 < 0.2$), system performance mainly in SIL3. Namely, strategy II contributes to a better system performance than strategy I. Compared to strategy II, system PFD_{avg} in $(19.5\tau, 20\tau)$ complies to SIL3 totally with strategy III.

The universal pros and cons of proposed maintenance strategies without taking the values of revealing coverage α_i into consideration are listed in Table. 6.

Table 6: Comparisons among proposed maintenance strategies

Strategy	PFD_{avg}	LCC
strategy I	Poor	Medium
strategy II	Medium	Low
strategy III	Good	High

In reality, following the previous findings, if the α_i quite high ($\alpha_i > 0.5$), from Fig. 9, PFD_{avg} under each maintenance strategy is within SIL3. Therefore, LCC should be prioritized to reduce unnecessary economic loss. That is, the proposed strategy II is the optimal option. On the contrary, if the α_i quite low ($\alpha_i < 0.5$), not all system SIL complies to SIL3, PFD_{avg} is in the higher priority when it comes to select optimal test and maintenance strategy.

Meanwhile, it is obvious to conclude from Fig. 8 and Fig. 9 that the proposed strategy III can lead to the highest LCC and optimum PFD_{avg} regardless of the value of α_i. Nevertheless, in terms of PFD_{avg}, it has slight improvement compared to strategy II especially when α_i quite high ($\alpha_i > 0.5$). The high LCC is the definite disadvantage of the proposed strategy III.

Given that the inevitable degradation phenomena in mechanical elements, it is needed to study how dynamic monitoring can be better utilized. An indicator reflecting the working condition and system status could provide clues for maintenance actions. When a PM is implemented (parameter $\alpha_i > 0$ in this paper), the system performance is better, but LCC is higher. A systematic testing and maintenance policy for the SIS with coordinating the trade-off between PFD_{avg} and LCC should be carefully considered in the designed phase.

5. Concluding remarks

This paper has presented a state-based approach for performance analysis of redundant final elements in SIS subject to imperfect degradation state revealing. The system performance is calculated based on a multi-phase Markov process. Estimation methods for maintenance cost in a finite time regarding imperfect state revealing have been proposed.

A numerical example is given to illustrate the usefulness of the proposed strategies. Based on the assumption, for a 1oo2 configuration, we found that staggered tests can contribute to a better system performance compared to simultaneous tests. From the aspect of LCC, strategy III > strategy I > strategy II in 20τ. Through the proposed method and discussions, a systematic consideration in incorporating system availability and life cycle cost need to be conducted, for reliability practitioners of SISs, when choose testing and maintenance strategy in the overall lifecycle for redundant final element.

This paper focuses on the comparisons among three proposed testing and maintenance strategies for 1oo2 SIS subject to imperfect state revealing. However, several limitations have been remained here in terms of testing and maintenance for SISs, e.g. partial test, common cause failures (CCFs), time-dependent degradation state revealing probability and imperfect maintenance etc. Another point here is about the estimation of potential economic loss of EUC due to the testing and maintenance of SISs.

For further studies, it would be interesting to extend and apply this model to realistic issues of SISs with risk-based EUC cost involved.

Acknowledgment

The authors are grateful to three anonymous reviewers for their useful comments and suggestions to the original version of this paper.

Appendix

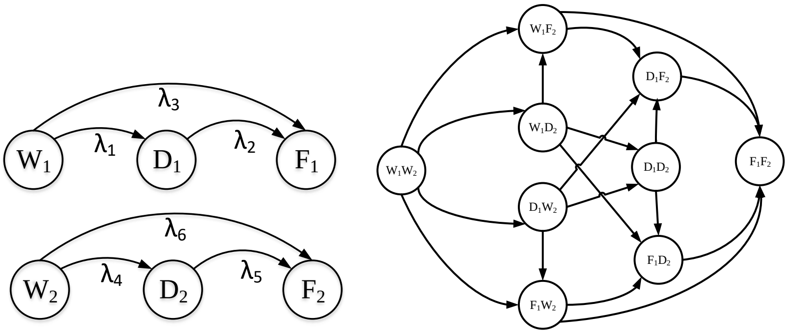
A. possible states for 1oo2 configuration

Table A.1: Possible states for 1oo2 configuration

state	notation
1	W_1W_2
2	W_1D_2
3	W_1F_2
4	D_1W_2
5	D_1D_2
6	D_1F_2
7	F_1W_2
8	F_1D_2
9	F_1F_2

B. Matrices mentioned in this paper

There are 3 possible states for each single unit under study. They are denoted by State W (working), State D (degraded) and State F (failed).



(a) (b)

Figure A.1: state transition diagrams for (a)1oo1 configuration and (b) 1oo2 configuration

Transition rate matrix $\mathbf{Q}_{U_1}$ and $\mathbf{Q}_{U_2}$ for unit 1 and 2:

$$\mathbf{Q}_{U_1} = \begin{array}{c|ccc|} & \mathrm{W}_1 & \mathrm{D}_1 & \mathrm{F}_1 \\ \mathrm{W}_1 & -(\lambda_1+\lambda_3) & \lambda_1 & \lambda_3 \\ \mathrm{D}_1 & & -\lambda_2 & \lambda_2 \\ \mathrm{F}_1 & & & \end{array} \mathbf{Q}_{U_2} = \begin{array}{c|ccc|} & \mathrm{W}_2 & \mathrm{D}_2 & \mathrm{F}_2 \\ \mathrm{W}_2 & -(\lambda_4+\lambda_6) & \lambda_4 & \lambda_6 \\ \mathrm{D}_2 & & -\lambda_5 & \lambda_5 \\ \mathrm{F}_2 & & & \end{array}$$

Transition rate matrix $\mathbf{Q}$ for 1oo2 configuration

$$\mathbf{Q} = \begin{array}{c|ccccccccc|} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & -\Sigma & \lambda_4 & \lambda_6 & \lambda_1 & & & \lambda_3 & & \\ 2 & & -\Sigma & \lambda_5 & & \lambda_1 & & & \lambda_3 & \\ 3 & & & -\Sigma & & & \lambda_1 & & & \lambda_3 \\ 4 & & & & -\Sigma & \lambda_4 & \lambda_6 & \lambda_2 & & \\ 5 & & & & & -\Sigma & \lambda_5 & & \lambda_2 & \\ 6 & & & & & & -\Sigma & & & \lambda_2 \\ 7 & & & & & & & -\Sigma & \lambda_4 & \lambda_6 \\ 8 & & & & & & & & -\Sigma & \lambda_5 \\ 9 & & & & & & & & & -\Sigma \end{array}$$

The coverage indicator α_i is defined as the conditional probability that a degraded state will be detected by the proof test of unit i, given that degradation has occurred when initiating the proof test.

$$\alpha_i = \Pr(\text{Degradation is detected in a proof test }|\text{Degradation has occurred})$$

$\mathbf{M}$ represents the probability matrix of different states after a testing and repair action.

$\mathbf{M}_{U_1}$ represents the probability matrix of different states after a testing and repair action of unit 1.

$\mathbf{M}_{U_2}$ represents the probability matrix of different states after a testing and repair action of unit 2.

Matrix $\mathbf{M}$ for simultaneous testing with testing coverage α_i and maintenance strategy I

$$\mathbf{M} = \begin{array}{c|ccccccccc|} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 1 & & & & & & & & \\ 2 & \alpha_2 & 1-\alpha_2 & & & & & & & \\ 3 & 1 & & & & & & & & \\ 4 & \alpha_1 & & & 1-\alpha_1 & & & & & \\ 5 & \alpha_1\alpha_2 & (1-\alpha_2)\alpha_1 & & (1-\alpha_1)\alpha_2 & (1-\alpha_1)(1-\alpha_2) & & & & \\ 6 & \alpha_1 & & & 1-\alpha_1 & & & & & \\ 7 & 1 & & & & & & & & \\ 8 & \alpha_2 & 1-\alpha_2 & & & & & & & \\ 9 & 1 & & & & & & & & \end{array}$$

Matrix $\mathbf{M}$ for staggered testing with testing coverage α_i and maintenance strategy II

$$\mathbf{M}_{U_1} = \begin{array}{c|ccccccccc|}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & 1 & & & & & & & & \\
2 & & 1 & & & & & & & \\
3 & & & 1 & & & & & & \\
4 & \alpha_1 & & & 1-\alpha_1 & & & & & \\
5 & & \alpha_1 & & & 1-\alpha_1 & & & & \\
6 & & & \alpha_1 & & & 1-\alpha_1 & & & \\
7 & 1 & & & & & & & & \\
8 & & 1 & & & & & & & \\
9 & & & 1 & & & & & &
\end{array}
\mathbf{M}_{U_2} = \begin{array}{c|ccccccccc|}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & 1 & & & & & & & & \\
2 & \alpha_2 & 1-\alpha_2 & & & & & & & \\
3 & 1 & & & & & & & & \\
4 & & & & 1 & & & & & \\
5 & & & & \alpha_2 & 1-\alpha_2 & & & & \\
6 & & & & 1 & & & & & \\
7 & & & & & & & 1 & & \\
8 & & & & & & & \alpha_2 & 1-\alpha_2 & \\
9 & & & & & & & 1 & &
\end{array}$$

Matrix $\mathbf{M}$ for staggered testing with testing coverage α_i and maintenance strategy III

$$\mathbf{M}_{U_1} = \begin{array}{c|ccccccccc|}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & 1 & & & & & & & & \\
2 & & 1 & & & & & & & \\
3 & & & 1 & & & & & & \\
4 & \alpha_1 & & & 1-\alpha_1 & & & & & \\
5 & & \alpha_1 & & & 1-\alpha_1 & & & & \\
6 & & & \alpha_1 & & & 1-\alpha_1 & & & \\
7 & 1 & & & & & & & & \\
8 & 1 & & & & & & & & \\
9 & 1 & & & & & & & &
\end{array}
\mathbf{M}_{U_2} = \begin{array}{c|ccccccccc|}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & 1 & & & & & & & & \\
2 & \alpha_2 & 1-\alpha_2 & & & & & & & \\
3 & 1 & & & & & & & & \\
4 & & & & 1 & & & & & \\
5 & & & & \alpha_2 & 1-\alpha_2 & & & & \\
6 & 1 & & & & & & & & \\
7 & & & & & & & 1 & & \\
8 & & & & & & & \alpha_2 & 1-\alpha_2 & \\
9 & 1 & & & & & & & &
\end{array}$$

References

[1] M. Rausand, A. Høyland, System reliability theory: models, statistical methods, and applications, Vol. 396, John Wiley & Sons, 2003.

[2] M. Rausand, Reliability of safety-critical systems: theory and applications, John Wiley&Sons, 2014.

[3] IEC 61508 functional safety of electrical/electronic/programmable electronic safety-related systems (2010).

[4] S. Hauge, M. A. Lundteigen, P. Hokstad, S. Håbrekke, Reliability prediction method for safety instrumented systems–pds method handbook, 2010 edition, SINTEF report STF50 A 6031.

[5] A. E. B. Longhi, A. A. Pessoa, P. A. de Almada Garcia, Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees, Reliability Engineering & System Safety 142 (2015) 525–538.

[6] A. E. Summers, Viewpoint on ISA TR84. 0.02-simplified methods and fault tree analysis, ISA Transactions 39 (2000) 125–131.

[7] Z. Chiremsel, R. N. Said, R. Chiremsel, Probabilistic fault diagnosis of safety instrumented systems based on fault tree analysis and bayesian network, Journal of failure analysis and prevention 16 (5) (2016) 747–760.

[8] Y. Dutuit, F. Innal, A. Rauzy, J.-P. Signoret, Probabilistic assessments in relationship with safety integrity levels by using fault trees, Reliability Engineering & System Safety 93 (12) (2008) 1867–1876.

[9] W. Mechri, C. Simon, F. Bicking, K. B. Othman, Fuzzy multiphase markov chains to handle uncertainties in safety systems performance assessment, Journal of Loss Prevention in the Process Industries 26 (4) (2013) 594–604.

[10] W. Mechri, C. Simon, K. BenOthman, Switching markov chains for a holistic modeling of sis unavailability, Reliability Engineering & System Safety 133 (2015) 212–222.

[11] S. Wu, L. Zhang, A. Barros, W. Zheng, Y. Liu, Performance analysis for subsea blind shear ram preventers subject to testing strategies, Reliability Engineering & System Safety 169 (2018) 281–298.

[12] H. Azizpour, M. A. Lundteigen, Analysis of simplification in Markov-based models for performance assessment of Safety Instrumented System, Reliability Engineering & System Safety 183 (2019) 252–260.

[13] E. S. Torres, S. Sriramula, D. Celeita, G. Ramos, Reliability model and sensitivity analysis for electrical/electronic/programmable electronic safety-related systems, IEEE Transactions on Industry Applications 56 (4) (2020) 3422–3430.

[14] B. Cai, L. Huang, M. Xie, Bayesian networks in fault diagnosis, IEEE Transactions on Industrial Informatics 13 (5) (2017) 2227–2240.

[15] B. Cai, M. Xie, Y. Liu, Y. Liu, Q. Feng, Availability-based engineering resilience metric and its corresponding evaluation methodology, Reliability Engineering & System Safety 172 (2018) 216–224.

[16] B. Cai, X. Kong, Y. Liu, J. Lin, X. Yuan, H. Xu, R. Ji, Application of bayesian networks in reliability evaluation, IEEE Transactions on Industrial Informatics 15 (4) (2018) 2146–2157.

[17] Y. Liu, M. Rausand, Reliability assessment of safety instrumented systems subject to different demand modes, Journal of Loss Prevention in the Process Industries 24 (1) (2011) 49–56.

[18] Y. Liu, Discrimination of low-and high-demand modes of safety-instrumented systems based on probability of failure on demand adaptability, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 228 (4) (2014) 409–418.

[19] Y. Liu, M. Rausand, Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems, Reliability Engineering & System Safety 145 (2016) 366–372.

[20] H. Meng, L. Kloul, A. Rauzy, Modeling patterns for reliability assessment of safety instrumented systems, Reliability Engineering & System Safety 180 (2018) 111–123.

[21] M. Čepin, B. Mavko, Probabilistic safety assessment improves surveillance requirements in technical specifications, Reliability Engineering & System Safety 56 (1) (1997) 69–77.

[22] S. Martorell, A. Sanchez, V. Serradell, Age-dependent reliability model considering effects of maintenance and working conditions, Reliability Engineering & System Safety 64 (1) (1999) 19–31.

[23] J. Vaurio, On time-dependent availability and maintenance optimization of standby units under various maintenance policies, Reliability Engineering & System Safety 56 (1) (1997) 79–89.

[24] P. Martorell, I. Martón, A. Sánchez, S. Martorell, Unavailability model for demand-caused failures of safety components addressing degradation by demand-induced stress, maintenance effectiveness and test efficiency, Reliability Engineering & System Safety 168 (2017) 18–27.

[25] S. Wu, L. Zhang, M. A. Lundteigen, Y. Liu, W. Zheng, Reliability assessment for final elements of siss with time dependent failures, Journal of Loss Prevention in the Process Industries 51 (2018) 186–199.

[26] E. Zio, Some challenges and opportunities in reliability engineering, IEEE Transactions on Reliability 65 (4) (2016) 1769–1782.

[27] A. Zhang, A. Barros, Y. Liu, Performance analysis of redundant safety-instrumented systems subject to degradation and external demands, Journal of Loss Prevention in the Process Industries 62 (2019) 103946.

[28] A. Zhang, Y. Liu, A. Barros, E. Kassa, A degrading element of safety-instrumented systems with combined maintenance strategy, in: Proceedings of the 29th European Safety and Reliability Conference (ESREL). 22–26 September 2019 Hannover, Germany, Research Publishing Services, 2019.

[29] A. Zhang, T. Zhang, A. Barros, Y. Liu, Optimization of maintenances following proof tests for the final element of a safety-instrumented system, Reliability Engineering & System Safety 196 (2020) 106779.

[30] Y. Langeron, A. Barros, A. Grall, C. Bérenguer, Combination of safety integrity levels (SILs): A study of iec61508 merging rules, Journal of Loss Prevention in the Process Industries 21 (4) (2008) 437–449.

[31] F. Innal, M. A. Lundteigen, Y. Liu, A. Barros, PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase markov models, Reliability Engineering & System Safety 150 (2016) 160–170.

[32] H. Srivastav, A. Barros, M. A. Lundteigen, Modelling framework for performance analysis of SIS subject to degradation due to proof tests, Reliability Engineering & System Safety 195 (2020) 106702.

[33] W. Qingfeng, L. Wenbin, Z. Xin, Y. Jianfeng, Y. Qingbin, Development and application of equipment maintenance and safety integrity management system, Journal of Loss Prevention in the Process Industries 24 (4) (2011) 321–332.

[34] B. H. Nystad, G. Gola, J. E. Hulsund, D. Roverso, Technical condition assessment and remaining useful life estimation of choke valves subject to erosion, in: Annual Conference of the Prognostics and Health Management Society, 2010, pp. 11–13.

[35] B. H. Nystad, G. Gola, J. E. Hulsund, Lifetime models for remaining useful life estimation with randomly distributed failure thresholds, in: First european conference of the prognostics and health management society, Vol. 3, 2012.

[36] G. Gola, B. H. Nystad, Prognostics and health management of choke valves subject to erosion: A diagnostic-prognostic frame for optimal maintenance scheduling, in: Diagnostics and Prognostics of Engineering Systems: Methods and Techniques, IGI Global, 2013, pp. 313–331.

[37] Y. Zhang, A. Barros, A. Rauzy, Assessment of a condition-based maintenance policy for subsea systems: A preliminary study, Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016 (Glasgow, Scotland, 25-29 September 2016).

[38] G. Levitin, A. Lisnianski, Optimization of imperfect preventive maintenance for multi-state systems, Reliability Engineering & System Safety 67 (2) (2000) 193–203.

[39] I. W. Soro, M. Nourelfath, D. Aït-Kadi, Performance evaluation of multi-state degraded systems with minimal repairs and imperfect preventive maintenance, Reliability Engineering & System Safety 95 (2) (2010) 65–69.

[40] Y. Liu, H.-Z. Huang, Optimal replacement policy for multi-state system under imperfect maintenance, IEEE Transactions on Reliability 59 (3) (2010) 483–495.

[41] M. Nourelfath, E. Châtelet, N. Nahas, Joint redundancy and imperfect preventive maintenance optimization for series–parallel multi-state degraded systems, Reliability Engineering & System Safety 103 (2012) 51–60.

[42] S.-H. Sheu, C.-C. Chang, Y.-L. Chen, Z. G. Zhang, Optimal preventive maintenance and repair policies for multi-state systems, Reliability Engineering & System Safety 140 (2015) 78–87.

[43] C. I. Ossai, Remaining useful life estimation for repairable multi-state components subjected to multiple maintenance actions, Reliability Engineering & System Safety 182 (2019) 142–151.

[44] Y. Liu, H.-Z. Huang, Z. Wang, Y. Li, Y. Yang, A joint redundancy and imperfect maintenance strategy optimization for multi-state systems, IEEE Transactions on Reliability 62 (2) (2013) 368–378.

[45] S. Alaswad, Y. Xiang, A review on condition-based maintenance optimization models for stochastically deteriorating system, Reliability Engineering & System Safety 157 (2017) 54–63.

[46] R. Sal, R. Nait-Said, M. Bourareche, Dealing with uncertainty in effect analysis of test strategies on safety instrumented system performance, International Journal of System Assurance Engineering and Management 8 (2) (2017) 1945–1958.

[47] A. Torres-Echeverria, S. Martorell, H. Thompson, Modelling and optimization of proof testing policies for safety instrumented systems, Reliability Engineering & System Safety 94 (4) (2009) 838–854.

[48] I. T. Castro, A. Barros, A. Grall, Age-based preventive maintenance for passive components submitted to stress corrosion cracking, Mathematical and Computer Modelling 54 (1-2) (2011) 598–609.

[49] K. T. Huynh, I. T. Castro, A. Barros, C. Bérenguer, On the use of mean residual life as a condition index for condition-based maintenance decision-making, IEEE Transactions on Systems, Man, and Cybernetics: Systems 44 (7) (2013) 877–893.

[50] E. M. Laskowska, J. Vatn, State modelling and prognostics of safety valves used in the oil and gas industry., in: Proceedings of the 29th European Safety and Reliability Conference(ESREL)., 2019.

[51] IEC 61511 functional safety safety instrumented systems for the process industry sector (2016).

[52] Y. Liu, Optimal staggered testing strategies for heterogeneously redundant safety systems, Reliability Engineering & System Safety 126 (2014) 65–71.

[53] M. Williams, Lower your operating costs with regular valve maintenance, Tech. rep., PlantServices, https://www.plantservices.com/articles/2004/212/ (Oct. 2004).

Article VI

Optimal activation strategies for heterogeneous channels of safety instrumented systems subject to aging and demands.

This article is awaiting publication and is therefore not included.

ISBN 978-82-471-4982-9 (printed ver.)
ISBN 978-82-471-4991-1 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

NTNU
Norwegian University of
Science and Technology