공학박사학위논문

복잡한 공학 시스템에 대한 오경보를 고려한 리질리언스 해석 및 설계 방법론 연구

Resilience Analysis and Design Methodology Considering False Alarms for Complex Engineered Systems

2018 년 02 월

서울대학교 대학원

기계항공공학부

윤 정 택

Abstract

Resilience Analysis and Design Methodology Considering False Alarms for Complex Engineered Systems

Joung Taek Yoon
Department of Mechanical and Aerospace Engineering
The Graduate School
Seoul National University

Most engineered systems are designed with a passive and fixed design capacity and, therefore, may become unreliable in the presence of adverse events. In order to handle this issue, the resilience-driven system design (RDSD) has been proposed to make engineered systems adaptively reliable by incorporating the prognostics and health management (PHM) method. PHM tracks the health degradation of an engineered system, and provides health state information supporting decisions on condition-based maintenance. Meanwhile, one of the issues awaiting solution in the field of PHM, as well as in RDSD, is to address false alarms. A false alarm is an erroneous report on the health state of an engineered system; it estimates a healthy engineered to be faulty, resulting unnecessary system shutdown, inspection, and – in the case of incorrect inspection – unnecessary system repair or replacement. Although false alarms make a system unavailable with capital loss, it has not been considered in resilience engineering.

To cope with false alarm problems, this research is elaborated to advance the resilience engineering considering false alarms. Specifically, this consists of three research thrusts: 1) resilience analysis considering false alarms, 2) resilience-driven system design considering false alarms (RDSD-FA), and 3) resilience-driven system design considering time-dependent false alarms (RDSD-TFA). In the first research thrust, a resilience measure is newly formulated considering false alarms. This enables the evaluation of resilience decrease due to false alarms, resulting in accurate analysis of system resilience. Based upon the new resilience measure, RDSD-FA is proposed in the second research thrust. This aims at designing a resilient system to satisfy a target resilience level while minimizing life-cycle cost. This is composed of three hierarchical tasks: resilience allocation problem, reliability-based design optimization (RBDO), and PHM design. The third research thrust presents RDSD-TFA that considers time-dependent variability of an engineered system. This makes one to estimate life-cycle cost in an accurate and rigorous manner, and to design an engineered system more precisely while minimizing its life-cycle cost. The framework of RDSD-TFA consists of four tasks: system analysis, PHM analysis, life-cycle simulation, and design optimization. Through theoretical analysis and case studies, the significance of false alarms in engineering resilience and the effectiveness of the proposed ideas are demonstrated.

Keywords : resilience, reliability, prognostics and health management (PHM), false alarm, system design

Student Number : 2011-20729

Table of Contents

Abstract ..... **i**

Nomenclatures ..... **xiii**

Chapter 1. Introduction **1**

1.1 Motivation 1

1.2 Research Scope and Overview 3

1.3 Dissertation Layout 6

Chapter 2. Literature Review **8**

2.1 Resilience Engineering (Analysis and Design) 8

2.1.1 Resilience Analysis for Mechanical Systems 9

2.1.2 Resilience-Driven System Design (RDSD) for Mechanical Systems 16

2.2 False and Missed Alarms in Prognostics and Health Management 29

2.2.1 Definition of False and Missed Alarms 29

2.2.2 Quantification of False and Missed Alarms 34

2.3 Summary and Discussion 37

Chapter 3. Resilience Analysis Considering False Alarms **39**

3.1 Resilience Measure Considering False Alarms 39

3.2 Case Studies 44

3.2.1 Numerical Example 44

3.2.2 Electro-Hydrostatic Actuator (EHA) 46

3.3 Summary and Discussion 56

Chapter 4. Resilience-Driven System Design Considering False Alarms (RDSD-FA) 58

4.1 Overview of RDSD-FA Framework 58

4.2 Resilience Allocation Problem Considering False Alarms 59

4.3 Prognostics and Health Management (PHM) Design Considering False Alarms 64

4.4 Case study: Electro-Hydrostatic Actuator (EHA) 65

4.4.1 Step 1: Resilience Allocation Considering False Alarms 65

4.4.2 Step 2: Reliability-Based Design Optimization 68

4.4.3 Step 3: PHM Design Considering False Alarms 73

4.4.4 Comparison of Design Results from RDSD and RDSD-FA 78

4.5 Summary and Discussion 80

Chapter 5. Resilience-Driven System Design Considering Time-Dependent False Alarms (RDSD-TFA) 82

5.1 Time-Dependent False and Missed Alarms in PHM 84

5.2 Resilience-Driven System Design Considering Time-Dependent False Alarms (RDSD-TFA) 89

5.2.1 Overview of RDSD-TFA Framework 89

5.2.2 Task 1: System Analysis 92

5.2.3 Task 2: PHM Analysis 95

5.2.4 Task 3: Life-Cycle Simulation 97

5.2.5 Task 4: Design Optimization 104
5.3 Case studies 105
5.3.1 Numerical Example of Life-Cycle Simulation 105
5.3.2 Electro-Hydrostatic Actuator (EHA) 116
5.4 Summary and Discussion 134
Chapter 6. Conclusions 137
6.1 Summary and Contributions 137
6.2 Suggestions for Future Research 140
References 143
Appendix 166
Abstract(Korean) 169

List of Tables

Table 2-1 Lists of RBDO algorithms 24

Table 2-2 False alarms in PHM 30

Table 2-3 Health estimation matrix of two health states 35

Table 2-4 Health estimation matrix of multiple health states 35

Table 3-1 Health estimation matrix of sample case study data 45

Table 3-2 Resilience measure calculation of numerical examples 46

Table 3-3 Statistics of EHA simulation model parameters 48

Table 3-4 Extracted health features for EHA health state estimation 50

Table 3-5 EHA health estimation matrix of multi-health state 53

Table 3-6 EHA health estimation matrix of bi-health state 53

Table 4-1 Parameters of life-cycle cost model for resilience allocation problem 67

Table 4-2 Resilience allocation results according to PHM implementation . 67

Table 4-3 RBDO problem parameters 70

Table 4-4 RBDO problem random variables 70

Table 4-5 Initial and optimal design of hydraulic cylinder 71

Table 4-6 Statistics of EHA simulation model parameters 75

Table 4-7 Optimal PHM designs of three PHM algorithm with their costs .. 78

Table 4-8 Comparison of design results from RDSD and RDSD-FA 79

Table 5-1 Health estimation matrix of two health states 87

Table 5-2 Four events and their probabilities in system operation..... 101

Table 5-3 Maintenance cost and usage time update of four events..... 104

Table 5-4 Statistical information of random variables in RDSD-TFA of EHA 124

Table 5-5 Parameters in RDSD-TFA of EHA..... 125

Table 5-6 Optimal design variables and resulting costs 128

Table 5-7 Comparison of RDSD-FA and RDSD-TFA 136

List of Figures

Figure 1-1 Research scope and three research thrusts of dissertation 4

Figure 2-1 Example of reliability calculation 11

Figure 2-2 Description of restoration action 13

Figure 2-3 Change of resilience due to the degree of reliability and restoration 15

Figure 2-4 Hierarchical resilience-driven system design framework 18

Figure 2-5 Example of resilience allocation for a series-parallel system 19

Figure 2-6 Comparison of deterministic design and reliability-based design optimization (RBDO) 22

Figure 2-7 Comparison of (a) schedule-based maintenance and (b) condition-based maintenance with prognostics and health management 26

Figure 2-8 Example of health diagnostics 27

Figure 2-9 Example of health prognostics 27

Figure 2-10 Example of a false alarm 31

Figure 2-11 Example of a missed alarm 32

Figure 2-12 Resisting and recovering actions to maintain system functionality 38

Figure 3-1 Resilience scenario using the existing resilience measure [11] 41

Figure 3-2 Resilience scenario considers false alarms 42

Figure 3-3 Schematic diagram of an electro-hydrostatic actuator (EHA) simulation model 47

Figure 3-4 Sensory signals of EHA in four health states 50

Figure 3-5 Health features of randomly generated datasets 52

Figure 3-6 Evaluated EHA false alarm rates with different sensors 54

Figure 3-7 EHA resilience, as evaluated by two resilience measures 56

Figure 4-1 Hierarchical resilience-driven system design framework considering false alarms 59

Figure 4-2 Example of resilience allocation result for a series-parallel system considering false alarms 62

Figure 4-3 Electro-hydrostatic actuator system and its subsystems 66

Figure 4-4 Five performance constraints of hydraulic cylinder 69

Figure 4-5 False and missed alarm rates with different weights and PHM algorithm 76

Figure 4-6 Error bar of false alarm and missed rates 77

Figure 5-1 Example of time-dependent health feature distributions 86

Figure 5-2 Example of calculated time-dependent false alarm rate and reliability 86

Figure 5-3 Overall framework of resilience-driven system design considering time-dependent false alarms 91

Figure 5-4 Example of analyze time-dependent health feature and time-

dependent reliability for brushless direct current (BLDC) fan 94

Figure 5-5 Time-dependent false alarm rates estimation..... 97

Figure 5-6 Framework of life-cycle simulation for total maintenance cost analysis 99

Figure 5-7 Example of event decision..... 103

Figure 5-8 Models for numerical example 108

Figure 5-9 Health features of power transformers [59]..... 108

Figure 5-10 Time-dependent reliability, false alarm and missed alarm rates110

Figure 5-11 Calculated event probabilities and decided events..... 110

Figure 5-12 Histogram of total maintenance cost from life-cycle simulation112

Figure 5-13 Error bar of total maintenance cost 113

Figure 5-14 Histogram of total maintenance cost with alarm weight adjustment..... 114

Figure 5-15 Sensitivity analysis results..... 116

Figure 5-16 Overall EHA models and variables for life-cycle cost estimation 118

Figure 5-17 Percolation channels due to roughness of contact surface [98]119

Figure 5-18 Schematic diagram of a hydraulic cylinder (double-acting)... 120

Figure 5-19 Time-dependent rod position control error of EHA 129

Figure 5-20 Time-dependent reliability of EHA..... 129

Figure 5-21 Event probabilities of the design by RDSD-TFA without PHM130

Figure 5-22 Time-dependent cross-line leakage coefficient of EHA 131

Figure 5-23 Event probabilities of the design by RDSD-TFA with PHM .. 132

Figure 5-24 Error bar of maintenance occurrences 133

Figure 5-25 Histogram of life-cycle cost 134

Nomenclatures

RDSD	Resilience-driven system design
FA	False alarms
TFA	Time-dependent false alarms
EHA	Electro-hydrostatic actuator
RAP	Resilience allocation problem
RBDO	Reliability-based design optimization
PHM	Prognostics and health management
LCS	Life-cycle simulation
HS	Health state
HF	Health feature
MCS	Monte Carlo simulation
R	Servomotor rotary speed sensor
D	Cylinder rod displacement sensor
P	Pressure sensor
T	Servomotor temperature sensor
LDA	Linear discriminant analysis classifier
SVM	Support vector machine
kNN	k-nearest neighbor classifier
Ψ, Ψ_{FA}	Engineering resilience of RDSD and -FA
R	Reliability
ρ	Restoration
$G(\cdot)$	Constraint function
E_{mr}	Successful mitigation and recovery (M/R; maintenance) event

E_{cp}	Correct prognosis event
E_{cd}	Correct diagnosis event
E_{sf}	System failure event
κ	Probability of E_{mr}
Λ_P	Probability of E_{cp}
Λ_D	Probability of E_{cd}
$\Lambda, \Lambda_{\mathrm{FA}}$	PHM efficiency of RDSD and -FA
ε_ρ	Restoration efficiency
$\mathbf{X}$	Random variable vector
$\mathbf{d}$	Design variable vector
$\mathbf{d}^{\mathrm{SYS}}$	System design variable vector
$\mathbf{d}^{\mathrm{PHM}}$	PHM design variable vector
$\mathbf{d}_P^{\mathrm{PHM}}$	Prognosis design vector
$\mathbf{d}_D^{\mathrm{PHM}}$	Diagnosis design vector
$\mathbf{d}_{\mathrm{sensor}}^{\mathrm{PHM}}$	PHM sensor selection vector
$\mathbf{d}_{\mathrm{alg}}^{\mathrm{PHM}}$	PHM algorithm selection vector
$\mathbf{d}_{\theta}^{\mathrm{PHM}}$	PHM algorithm parameter vector
$I_k(\cdot)$	Indication function of *k*-th element
FA	False alarm rate
MA	Missed alarm rate
$\mathrm{E}_{\mathrm{healthy}}^{\mathrm{true}}$ or H	Event of a healthy engineered system
$\mathrm{E}_{\mathrm{faulty}}^{\mathrm{true}}$ or F	Event of a faulty engineered system
$\mathrm{E}_{\mathrm{healthy}}^{\mathrm{esti}}$ or $\hat{\mathrm{H}}$	Event of estimating an engineered system to be healthy
$\mathrm{E}_{\mathrm{faulty}}^{\mathrm{esti}}$ or $\hat{\mathrm{F}}$	Event of estimating an engineered system to be faulty
w_{FA}	False alarm weight

w_{MA}	Missed alarm weight
$N_{\alpha\widehat{\beta}}, N_{\alpha\widehat{\beta}}^{\mathrm{multi}}$	The number of samples estimated to be β health state given the true α health state in the binary- and multi-health states
$LCC, LCC_{\mathrm{FA}}, LCC_{\mathrm{TFA}}$	Life-cycle cost of RDSD, -FA, and -TFA
$C^{\mathrm{I}}, C_{\mathrm{FA}}^{\mathrm{I}}, C_{\mathrm{TFA}}^{\mathrm{I}}$	Initial development cost of RDSD, -FA, and -TFA
$C^{\mathrm{PHM}}, C_{\mathrm{FA}}^{\mathrm{PHM}}, C_{\mathrm{TFA}}^{\mathrm{PHM}}$	PHM development cost of RDSD, -FA, and -TFA
$C^{\mathrm{M}}, C_{\mathrm{FA}}^{\mathrm{M}}, C_{\mathrm{TFA}}^{\mathrm{M}}$	Total maintenance cost of RDSD, -FA, and -TFA
$C^{\mathrm{PM}}, C_{\mathrm{FA}}^{\mathrm{PM}}$	Expected predictive maintenance cost of RDSD and -FA
$C^{\mathrm{CM}}, C_{\mathrm{FA}}^{\mathrm{CM}}$	Expected corrective maintenance cost of RDSD and -FA
$C^{\mathrm{UM}}, C_{\mathrm{FA}}^{\mathrm{UM}}$	Expected unnecessary maintenance cost of RDSD and -FA
c^{PM}	Predictive maintenance cost
c^{CM}	Corrective maintenance cost
c^{UM}	Unnecessary maintenance cost
$\psi_j^t, \psi_{\mathrm{FA},j}^t$	Target resilience measure of *j*-th subsystem of RDSD and RDSD-FA
$r_j^t, \mathbf{r}^t$	Target reliability for *j*-th subsystem and its vector
$\lambda_j^t, \boldsymbol{\lambda}^t$	Target PHM efficiency for *j*-th subsystem and its vector
$m_j, \mathbf{m}$	Redundancy of *j*-th subsystem and its vector
$FA_j^t, \mathbf{FA}^t$	Target false alarm rate for *j*-th subsystem and its vector
$MA_j^t, \mathbf{MA}^t$	Target missed alarm rate for *j*-th subsystem and its vector
$\psi_j, \psi_{\mathrm{FA},j}$	Resilience measure of *j*-th subsystem of RDSD and RDSD-FA
r_j	Reliability of *j*-th subsystem
λ_j	PHM efficiency of *j*-th subsystem component
FA_j	False alarm rates of *j*-th subsystem component
MA_j	Missed alarm rates of *j*-th subsystem component

$\mathbf{X}_j^{\mathrm{C}}$	Random variable vector of *j*-th subsystem component
$\mathbf{d}_j^{\mathrm{C}}$	Design variable vector of *j*-th subsystem component
$\mathbf{d}_j^{\mathrm{PHM}}$	PHM design vector of *j*-th subsystem component
C_j^{I}	Initial development cost of *j*-th subsystem component
C_j^{PHM}	PHM development cost for *j*-th subsystem component
C_j^{M}	Total maintenance cost of *j*-th subsystem
$c_j^{\mathrm{UM}}, c_j^{\mathrm{PM}}, c_j^{\mathrm{CM}}$	Unnecessary, predictive, and corrective maintenance costs of a component in the *j*-th subsystem
R_{LCS}	Reliability of LCS
FA_{LCS}	False alarm rate of LCS
MA_{LCS}	Missed alarm rate of LCS
P_O	Probability of normal operation
P_{UM}	Probability of unnecessary maintenance
P_{CM}	Probability of corrective maintenance
P_{PM}	Probability of predictive maintenance
t_i	*i*-th life-cycle time
c_M	Incurred maintenance cost at t_i
τ_i	*i*-th usage time
N	The number of total time steps for the designed life-cycle
z	Uniformly distributed random number
$c_{\mathrm{R}},\ c_{\mathrm{D}},\ c_{\mathrm{P}},\ c_{\mathrm{T}}$	Costs of R, D, P, and T sensor
$Q_{99}(\cdot)$	99% quantile function

Chapter 1. Introduction

1.1 Motivation

Engineered systems offer not only immeasurable benefits to our lives, but also give us inconvenience or safety concerns in the event of sudden failures. The unexpected failures yield enormous damage such as human fatality, breakdown of artificial and natural system, and monetary loss. This risk is getting increased along the growing dependency of human society upon the engineered systems. For example, it is reported that the Canadian economy suffers an annual damage over 167 billion CAD due to unexpected electrical power outages in 2013, which corresponds 769,700 CAD per an incident [1]. North American businesses lose $26.5 billion every year due to unexpected IT downtime [2]. In this respect, the potential failures of an engineered system must be prevented.

There have been tremendous efforts to maintain the engineered system without failures. Corresponding techniques can be categorized into two groups according to an application stage: (1) design and (2) operation. Design stage techniques aim at designing engineered systems to endure and survive against uncertainty factors such as material property uncertainty, manufacturing tolerance, variable loading conditions, and so on. Whereas, operation stage techniques aim at proactively preventing the system failures against adverse events such as health (or performance) degradation, natural disaster, or human error. One of emerging operation stage techniques is the prognostics and health management (PHM) technique which evaluates current health states, predicts potential failures, and helps properly manage an engineered system to maintain

its functionality through their life-cycle.

Along with these techniques, resilience-driven system design (RDSD) was proposed [24]. RDSD aims to design an engineered system to be resilient to sustain required functionality. In engineering, resilience is defined as the ability of a component or a system to maintain its required functionality by resisting and recovering from adverse events. The resisting and the recovering properties are realized separately: resistance or reliability is enhanced through reliability-based design optimization (RBDO) of design stage technique, and recovery or PHM efficiency is realized through PHM of operation stage technique. Compared to conventional separate implementation of design stage and operation stage techniques, a cohesive incorporation of techniques for both stages can prevent excessive or insufficient implementations, while minimizing life-cycle cost.

One of the issues awaiting solution in the field of PHM, as well as in RDSD, is to address false and missed alarms. False and missed alarms are erroneous reports on the health state of an engineered system. A false alarm estimates a healthy engineered system to be faulty resulting incorrect alarm with unnecessary system shutdown, inspection, and repair or replacement cost in case of incorrect inspection. Whereas, a missed alarm does vice versa that estimates a faulty engineered system to be healthy resulting no alarms and system failure. False and missed alarms can thus make PHM and RDSD unreliable and hinder their applications.

However, PHM and RDSD currently do not consider false alarms, but focus on missed alarms only. In addition to missed alarms which can result in system

failure, false alarms also cause in loss of system availability with tremendous financial loss. For example, false alarms in the F/A-18C fighter aircraft mainly caused 75% of "cannot duplicate" (CND) maintenance [3]; CND is also called "no fault found," "fault not found," or "retest okay." [4, 5] These false alarms resulted in 46.3 man-years of wasted maintenance and 2.96 years of unnecessary aircraft downtime with $1.7M [3]. Beniaminy and Joseph estimated the financial loss of the air transport association due to NFF as $100M annually [6]. The U.S. Defense Department reported its losses due to NFF at $2B annually in 2012 [7]. Clearly, not only missed alarms but also false alarms must be addressed for the sake of successful implementation of PHM and RDSD.

1.2 Research Scope and Overview

This dissertation aims at advancing resilience engineering, which currently does not consider false alarms, to address false alarms. Specifically, this is dedicated for (1) resilience analysis and (2) resilience-driven system design (RDSD). Resilience analysis considering false alarms can accurately estimate the degree of resilience of an engineered system. This can help to determine operation action (failure probability and risk analysis, maintenance, design modification, etc.) to maintain system performance. RDSD considering false alarms is capable of designing an resilient engineered system against not only adverse events but also false alarm problems. This dissertation proposes two RDSD frameworks considering time-independent false alarms, and time-dependent false alarms respectively. Figure 1-1 lists three research thrusts regarding resilience

engineering considering false alarms and their overviews are followed below.

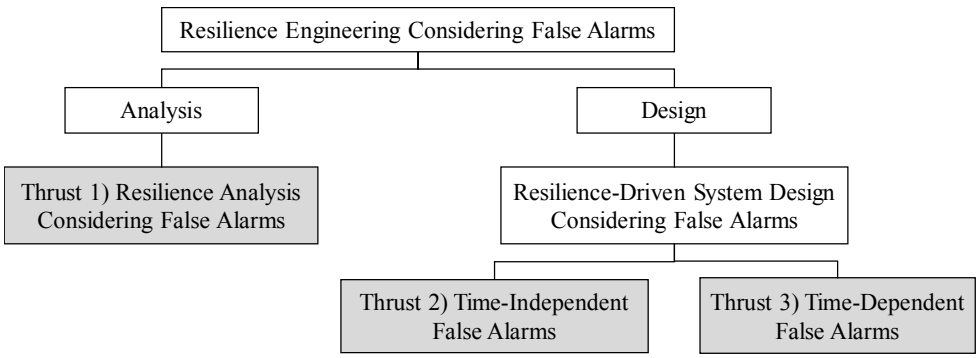


Figure 1-1 Research scope and three research thrusts of dissertation

Research Thrust 1: Resilience analysis considering false alarms

Research Thrust 1 proposes a new resilience measure considering false alarms. False alarms (false positive or false faulty) as well as missed alarms (false negative or false healthy), are considered. They result in unnecessary system shutdown and unexpected system failure respectively. The degrees of false and missed alarms are quantified with the use of a detectability matrix with sampling-based uncertainty propagation methods. Then the resilience measure is newly formulated based upon the probability theory. Two components of a resilience measure, the reliability and the restoration, are revised to include the false and missed alarms, respectively. Compared to the conventional resilience measure, a newly formulated resilience measure can estimate system resilience in a rigorous and accurate manner. The significance of false alarms in resilience and the effectiveness of the proposed resilience measure is demonstrated by numerical and electro-hydrostatic actuator (EHA) case studies.

Research Thrust 2: Resilience-driven system design considering false alarms (RDSD-FA)

RDSD by Youn et al. [24] designs an engineered system to satisfy a target resilience level (e.g., 95% or 99%) while minimizing life-cycle cost. That is, the outcome of system design is highly dependent on the formulation of resilience measure. If the evaluation of the system's resilience is not accurate due to the ignorance of false alarms, the system will not satisfy the intended target resilience level and will be prone to the false alarm problems. In order to resolve this problem, Research Thrust 2 proposes RDSD based on a resilience measure considering false alarms proposed in Research Thrust 1. The resilient system design is processed with three hierarchical steps: (i) resilience allocation problem (RAP), (ii) reliability-based design optimization (RBDO), and (iii) prognostics and health management (PHM) design. The effectiveness of proposed method compared to the original RDSD method is demonstrated with an Electro-hydrostatic actuator (EHA) design problem.

Research Thrust 3: Resilience-driven system design considering time-dependent false alarms (RDSD-TFA)

As an engineered system operates, its health state changes due to health degradation by adverse events, and health restoration by maintenance actions. Correspondingly, health-related probabilities including reliability, false and missed alarm rates, and resilience change along with time. However, they are regarded as time-independent or static values in RDSD-FA as well as RDSD.

This regarding helps to design a resilient engineered system in a time-efficient manner, but the estimation of resilience and life-cycle cost can be inaccurate, resulting unexpected financial loss. Therefore, Research Thrust 3 proposes an alternative RDSD framework considering time-dependent false alarms (RDSD-TFA). This framework aims at minimizing life-cycle cost of an engineered system through four tasks: system analysis, PHM analysis, life-cycle simulation, and design optimization. In order to incorporate systems' time-dependent variability, the concept and quantification method of time-dependent false and missed alarm rates are newly proposed. The consideration of time-dependent probabilities (i.e., reliability, false alarm rate, and missed alarm rate) enables accurate and rigorous life-cycle cost estimation. This helps to design an engineered system more precisely for the minimization of life-cycle cost.

1.3 Dissertation Layout

This dissertation is organized as follows. Chapter 2 reviews the current state of knowledge regarding resilience engineering (i.e., resilience analysis and resilient-system design) and false alarms in PHM. Chapter 3 presents a resilience measure considering false alarms with the quantification method of false alarms in PHM (Research Thrust 1). Chapter 4 proposes a RDSD framework based upon the resilience measure proposed in Chapter 3 (Research Thrust 2). Chapter 5 presents a RDSD framework considering time-dependent false alarms (Research Thrust 3). Finally, Chapter 6 summarizes the dissertation with its contributions and suggests future researches.

Chapter 2. Literature Review

This chapter presents the literature reviews of the knowledge within the scope of this dissertation: (1) resilience analysis, (2) resilience-driven system design, and (3) false and missed alarms in prognostics and health management (PHM).

2.1 Resilience Engineering (Analysis and Design)

The word "resilience" originated from the Latin word "resilire." "Resilire" means "to rebound, recoil;" "re" and "salire" mean "back" and "to jump, leap," respectively [8]. It is used in various research areas, but their definitions are slightly different as shown in Table A-1 in Appendix. In ecology, it is defined as "speed with which a system returns to its pre-disturbance level following a disturbance." [9] In economy, it is defined as "ability of an economy to recover from or adjust to the negative impacts of adverse exogenous shocks and to benefit from positive shocks." [10] And in mechanical engineering, Youn et al. [11] defined resilience as "degree of a passive survival rate plus a proactive survival rate against adverse events." The passive survival rate is the degree of intrinsic resistivity or durability of an engineered system to maintain its functionality. The proactive survival rate is the degree of restoring system functionality by predicting and recovering from potential failures with maintenance actions (e.g., repair or replacement).

According to Hollnagel et al. [12], there are three practices of resilience engineering: (1) to analyze resilience, (2) to improve resilience, and (3) to model and predict the effects of system change and operation decisions on resilience and risk. In mechanical engineering, they can be grouped into two: resilience

analysis of (1) and resilience-driven system design (RDSD) of (2) and (3). Resilience analysis estimates the degree of resilience of an engineered system which can help to determine operation action (failure probability and risk analysis, maintenance, design modification, etc.) to maintain system performance. RDSD explores and models the change of resilience according to design variables, and designs an engineered system to be resilient against adverse events to be of minimal life-cycle cost (LCC).

2.1.1 Resilience Analysis for Mechanical Systems

In order to analyze resilience, various measures (also called metrics, indices, indicators, or scales) have been proposed according to different disciplines and perspectives as shown in Table A-1 in Appendix.. For example, one measure quantifies the time-averaged performance for a life cycle [13] and another measure quantifies the rate of performance change during the failure and recovery process [14]. Among the many resilience measures shown in Table A-1, and the resilience measures described in the review papers [15, 16], three measures by Youn et al. [11], Li and Xi [17] and Hu and Mahadevan [18] are suitable for a mechanical system. These methods are suitable because they represent the probability of failure prevention directly and can be quantified through proven systematic approaches which will be discussed in following chapters. Among the three measures, this chapter reviews the more general resilience measure proposed by Youn et al. [11] in detail. The other resilience measures proposed by Li and Xi [17] and Hu and Mahadevan [18] are based on the method proposed by Youn et al. [11] that is discussed here. First, two components of the resilience measure, reliability and restoration, are briefly

explained. Then, the resilience measure will be reviewed.

2.1.1.1. Engineering Reliability

Reliability is defined as the ability of a component or a system to perform its required functions under stated conditions for a specified period of time. Required functions can sometimes not be satisfied due to uncertainty factors, including manufacturing tolerance, variant operating conditions, and uncertainties in the material properties. In order to define the uncertainties, reliability R is quantified as a probability using Eq. (2.1),

$$R(\mathbf{d}) = \Pr(G(\mathbf{X}; \mathbf{d}) \leq 0) \tag{2.1}$$

where $G(\cdot)$ is a performance function that indicates normal operation when its value is smaller than zero (e.g., G=stress−yield strength), $\mathbf{X}$ is a system random vector that varies due to the uncertainties, and $\mathbf{d}$ is a design vector such as the mean or standard deviation of $\mathbf{X}$. In Figure 2-1, samples of random variable X with mean value μ_X are spread due to uncertainty factors; correspondingly, the performance function values G(X) are distributed. The square-shaped samples (those for which performance values are above zero) indicate failure to operate normally. As a result, the reliability R is calculated through Eq. (2.1) and is equal to the shaded area in Figure 2-1.

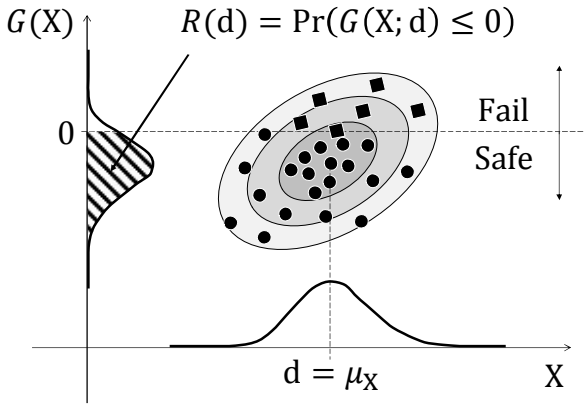


Figure 2-1 Example of reliability calculation

The calculation of reliability can formulated as below.

$$R(\mathbf{X}) = \int \dots \int_{\Omega^s} f(\mathbf{X})\, \mathrm{d}\mathbf{X} \qquad (2.2)$$

$$\text{where } \Omega^{\mathrm{s}} = \{\mathbf{X}\text{: } G_i(\mathbf{X}) \leq 0 \text{ for all } i\}$$

where $f(\mathbf{X})$ is a probability density function (PDF) of random vector $\mathbf{X}$; Ω^{s} is feasible or safe domain of random vector $\mathbf{X}$ that satisfy all the deterministic constraint functions $G_i(\mathbf{X}) \leq 0$. In practice, it is difficult to perform the multi-dimensional integration of Eq. (2.2) when the number of random variables is relatively large. In order to address this challenge, many reliability analysis (i.e., uncertainty quantification or uncertainty propagation) methods have been proposed such as sampling methods (e.g., Monte Carlo simulation (MCS) [19]), most probable points (MPP)-based method (e.g., first- or second-order reliability method (FORM/SORM) [20-22]), dimension reduction (DR) method [23, 24], and stochastic response surface-based method [25, 26].

2.1.1.2. Engineering Restoration

In engineering, the engineered components or systems can be gradually or abruptly damaged by unexpected adverse events, restoration is essential especially for highly risky systems. Restoration is defined as the ability to recover reliability when the failure of a component or a system is predicted. The reliability of a system decreases along its usage time, and thus failure probability (=1−reliability R) increases. When a system failure is predicted by the PHM technique, maintenance is performed to prevent the failure and to restore the decreased reliability. Youn et al. [11] formulated the restoration ρ as the probability of four consecutive events, as shown in Eq. (2.3),

$$\begin{aligned}
&\rho\left(\kappa, \mathbf{d}^{\mathrm{PHM}}, R\right) \\
&\quad = \Pr\left(\mathrm{E}_{mr}\mathrm{E}_{cp}\mathrm{E}_{cd}\mathrm{E}_{sf}\right) \\
&\quad = \Pr\left(\mathrm{E}_{mr}|\mathrm{E}_{cp}\mathrm{E}_{cd}\mathrm{E}_{sf}\right) \cdot \Pr\left(\mathrm{E}_{cp}|\mathrm{E}_{cd}\mathrm{E}_{sf}\right) \cdot \Pr\left(\mathrm{E}_{cd}|\mathrm{E}_{sf}\right) \cdot \Pr\left(\mathrm{E}_{sf}\right) \\
&\quad = \kappa \cdot \Lambda_P\left(\mathbf{d}_P^{\mathrm{PHM}}\right) \cdot \Lambda_D\left(\mathbf{d}_D^{\mathrm{PHM}}\right) \cdot (1-R) \\
&\quad = \kappa \cdot \Lambda\left(\mathbf{d}^{\mathrm{PHM}}\right) \cdot (1-R) = \varepsilon_\rho\left(\kappa, \mathbf{d}^{\mathrm{PHM}}\right) \cdot (1-R)
\end{aligned} \tag{2.3}$$

where $\mathbf{d}^{\mathrm{PHM}}$ is a PHM design vector that includes a prognosis design vector $\mathbf{d}_P^{\mathrm{PHM}}$ and a diagnosis design vector $\mathbf{d}_D^{\mathrm{PHM}}$, E_{mr} is a successful mitigation and recovery (M/R; maintenance) event, E_{cp} is a correct prognosis event, E_{cd} is a correct diagnosis event, E_{sf} is a system failure event – their probabilities are κ, Λ_P, Λ_D, and $(1-R)$, respectively – Λ is PHM efficiency, and ε_ρ is restoration efficiency. Here, κ is dependent on non-mechanical design factors such as fault inspection, maintenance strategy, and experts' performance; thus, it is set to be unity assuming that maintenance actions are always successfully performed. Λ_D is related to a sensor network (SN) design problem that designs or optimizes the

number, location, and type of sensors to classify system health state (HS) correctly under multiple failure modes. Λ_P is estimated from prognostic algorithm design problem that optimizes prognosis accuracy by adjusting the type and parameters of algorithms. As a result, the restoration ρ denotes the probability to successfully restore designed functionality in case of system failures. Figure 2-2 shows an example of a restoration action. The restoration action, including the system failure prediction and the successful maintenance action, will maintain the system's performance through its life-cycle. If the restoration is not implemented or does not successfully occur, the system will fail, as shown by the dotted line in Figure 2-2.

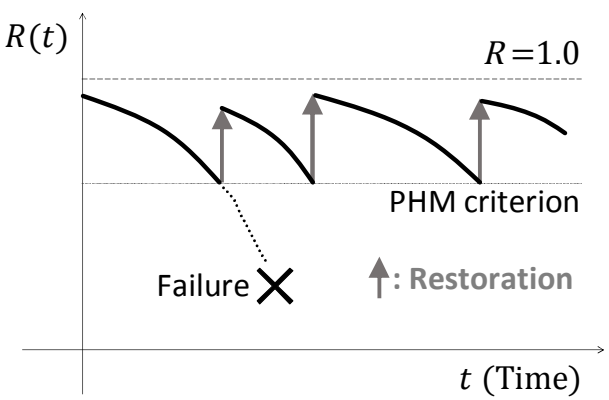


Figure 2-2 Description of restoration action

In order to calculate restoration of Eq. (2.3), it is necessary to calculate Λ_D and Λ_P. For the calculation of Λ_D, probability-of-detection (PoD) matrix is applicable [27, 28]. Its *i*-th row and *j*-th column element P_{ij} indicates the probability of health estimation to be *j*-th health state given *i*-th true health state. For the calculation of Λ_P, the metrics for accuracy evaluation of various health prognostics methods can be used such as relative accuracy, RUL error, and RUL

accuracy-precision index [11, 29, 30].

2.1.1.3. Engineering Resilience

In engineering, resilience is defined as the ability of a component or a system to maintain its required functionality by resisting and recovering from adverse events. Resisting and recovering properties correspond to "resist, withstand" and "adapt, return, recover, adjust, bounce back" in Table A-1 in the Appendix. Conceptually, Youn et al. [11] defined resilience as "the degree of a passive survival rate (or reliability) plus a proactive survival rate (or restoration)." Mathematically, it is a summation of the reliability (as outlined in Chapter 2.1.1.1) and the restoration (as described in Chapter 2.1.1.2). This is shown in Eq. (2.4).

$$
\begin{aligned}
&\text{Resilience } \Psi(\mathbf{d}, \kappa, \mathbf{d}_{\text{PHM}}) \\
&\quad = \text{Reliability } R(\mathbf{d}) + \text{Restoration } \rho\big(\kappa, \mathbf{d}_{\text{PHM}}, R(\mathbf{d})\big) \\
&\quad = R(\mathbf{d}) + \kappa \cdot \Lambda_P\big(\mathbf{d}^P_{\text{PHM}}\big) \cdot \Lambda_D\big(\mathbf{d}^D_{\text{PHM}}\big) \cdot \big(1 - R(\mathbf{d})\big) \\
&\quad = R(\mathbf{d}) + \kappa \cdot \Lambda(\mathbf{d}_{\text{PHM}}) \cdot \big(1 - R(\mathbf{d})\big) \\
&\quad = R(\mathbf{d}) + \varepsilon_\rho(\kappa, \mathbf{d}_{\text{PHM}}) \cdot \big(1 - R(\mathbf{d})\big) \\
&\quad = 1 - \big(1 - R(\mathbf{d})\big) \cdot \Big(1 - \varepsilon_\rho(\kappa, \mathbf{d}_{\text{PHM}})\Big)
\end{aligned}
\tag{2.4}
$$

According to this formulation, reliability and restoration are supplementary to each other: one can make up for the other's loss. Figure 2-3 shows the resilience measure Ψ, a function of the reliability R and the restoration efficiency ε_ρ. For a non-restorative system in which PHM is not implemented (Λ, κ, ε_ρ=0 → $\Psi_{\text{w/o PHM}}=R$), resilience is sensitive to the reliability; it cannot maintain its functionality when reliability decreases due to adverse events. In contrast, for a

restorative system (ε_ρ=0.8), the resilience is always above 0.8. This means that the system can prevent failures and maintain functionality with at least 80% probability. If a system is fully resistive (R=1), restoration is not needed. On the contrary, if a system is not resistive (R=0) at all, restoration must be fully functional. Here, the symbols and the definitions of some variables are changed from the original ones [11] to provide a better description.

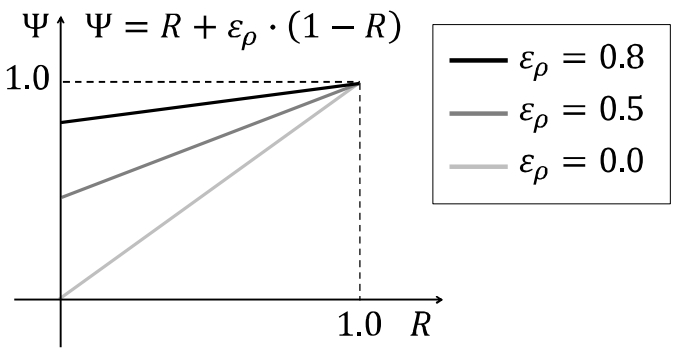


Figure 2-3 Change of resilience due to the degree of reliability and restoration

This resilience measure is different from other resilience measures from the viewpoint of the analysis approach. Other resilience measures are formulated in terms of the degree of health loss (vulnerability) due to adverse events and the degree of restoration such as "worse than before," "as good as before," and "better than before" [14, 18]. In contrast, the resilience measure Ψ is formulated in terms of the probabilities of health loss and restoration. The degrees of health loss and restoration are represented by the change of reliability R, as shown in Figure 2-2.

2.1.1.4. Issues with the Existing Resilience Measure

There are two main issues to be solved in the existing resilience measure. First,

false alarms are not considered. The PHM solution estimates the system's health state and helps engineers properly manage target systems. However, if the PHM solution is of poor quality and incorrectly estimates the system's health state, it can result in unnecessary system shutdown and inspection or an unpredicted system breakdown. There are two types of incorrect reporting by a PHM solution: a false alarm and a missed alarm. A false alarm estimates a healthy engineered system to be faulty resulting incorrect alarm with unnecessary system shutdown, inspection, and repair or replacement cost in case of incorrect inspection. Whereas, a missed alarm does vice versa that estimates a faulty engineered system to be healthy resulting no alarms and system failure. Although both alarms are significant regarding system availability, existing resilience measures consider only missed alarms and do not incorporate false alarms. Second, time dependency of the resilience measure is not considered. Resilience is not static; rather, it is variable as the system's health state changes along its operation time. The existing resilience measures are evaluated in terms of static reliability and static PHM efficiency, which are evaluated at a particular condition (e.g., specific time interval, partial data set). Hu and Mahadevan proposed a resilience measure that considers time-dependent reliability [18]; however, time-dependent PHM efficiency has not been incorporated in the resilience measure yet.

2.1.2 Resilience-Driven System Design (RDSD) for Mechanical Systems

In order to assign resilience into system, various methodologies have been proposed. Most of them proposes resilience measures or concepts applicable to specific or limited applications such as water distribution network [31, 32],

beam-to-column structure [33], supply chain [34, 35], computer processor thermal controller [36], and water resource system [37]. For the design of a mechanical engineered system, Youn et al. [11] proposed the framework of resilience-driven system design (RDSD). This aims at optimizing design variables to minimize life-cycle cost (LCC) while satisfying target resilience level. Compared to the other resilient system design methods, this can analyze the change of resilience according to various design variables, and can be generally applicable to various engineered systems. One of Research Thrusts is to advancing RDSD by Youn et al. [11] by considering false alarms, and thus it is reviewed in detail below.

2.1.2.1. Overview of RDSD

Figure 2-4 shows the framework of RDSD which is composed of three hierarchical design problems. The first design problem is "resilience allocation problem (RAP)" which allocates reliability, PHM efficiency, and redundancy levels into components while minimizing system LCC and satisfying a target system resilience. First bottom-level problem designs components to satisfy the allocated target reliability levels using system RBDO. And then, second bottom-level problem designs PHM units for the components to meet the allocated target PHM efficiency levels. Between the bottom-level design problems, physics of failure (PoF) information is shared which includes failure modes, failure probabilities, and PHM efficiencies.

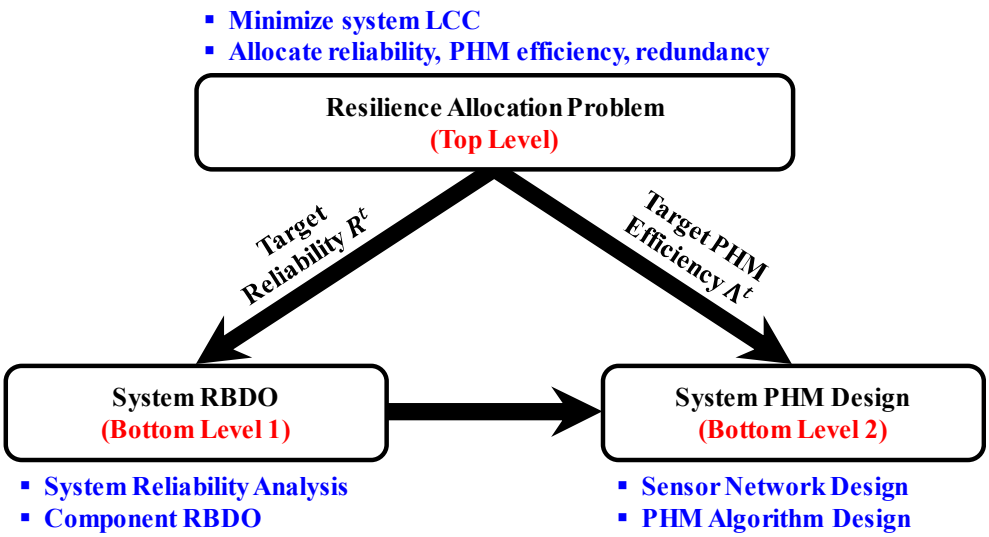


Figure 2-4 Hierarchical resilience-driven system design framework

2.1.2.2. Step 1: Resilience Allocation Problem (Top Level)

The top-level problem aims at allocating target reliability, target PHM efficiency, and redundancy levels to components so as to satisfy target resilience level while minimizing LCC. This can be formulated as below.

$$\begin{aligned} &\text{minimize}_{\mathbf{r}^t,\boldsymbol{\lambda}^t,\mathbf{m}} \quad LCC(\mathbf{r}^t,\boldsymbol{\lambda}^t,\mathbf{m}) \\ &\text{subject to} \quad \Psi^{\text{SYS}}(\mathbf{r}^t,\boldsymbol{\lambda}^t,\mathbf{m}) \geq \Psi^t \\ &\qquad\qquad \mathbf{0} \leq \mathbf{r}^t,\boldsymbol{\lambda}^t \leq \mathbf{1} \\ &\qquad\qquad 1 \leq m_j \leq m_j^U \ (j = 1,\dots,N) \end{aligned} \tag{2.5}$$

where $LCC(\cdot)$ is system LCC, Ψ^{SYS} is system resilience, and Ψ^t is target system resilience level; $\mathbf{r}^t$, $\boldsymbol{\lambda}^t$, and $\mathbf{m}$ are the vector of target reliability, target PHM efficiency, and redundancy level for N subsystems; $\mathbf{r}^t$ and $\boldsymbol{\lambda}^t$, quantified as probabilities, are between zero and one; the redundancy of j-th

subsystem m_j is positive integer.

Based upon the resilience measure in Chapter 2.1.1.3, the resilience of a series-parallel system Ψ^{SYS} can be calculated as below.

$$\Psi^{SYS}(\mathbf{r}^t, \boldsymbol{\lambda}^t, \mathbf{m}) = \prod_{j=1}^{N} \psi_j \left(r_j^t, \lambda_j^t, m_j\right) \tag{2.6}$$

$$\psi_j = 1 - \left[\left(1 - r_j^t\right) \cdot \left(1 - \lambda_j^t\right)\right]^{m_j} \tag{2.7}$$

where ψ_j is the resilience measure of j-th subsystem; r_j^t and λ_j^t are target reliability and target PHM efficiency for j-th subsystem. The Eq. (2.7) is based upon the assumption that the probability of successful mitigation and recovery κ is one, and the reliability and PHM efficiency of components in each subsystem are identical. The example result of resilience allocation problem is shown in Figure 2-5. The 2nd subsystem without PHM unit has zero PHM efficiency, and resulted system resilience Ψ^{SYS} is 99.82% according to Eq. (2.6).

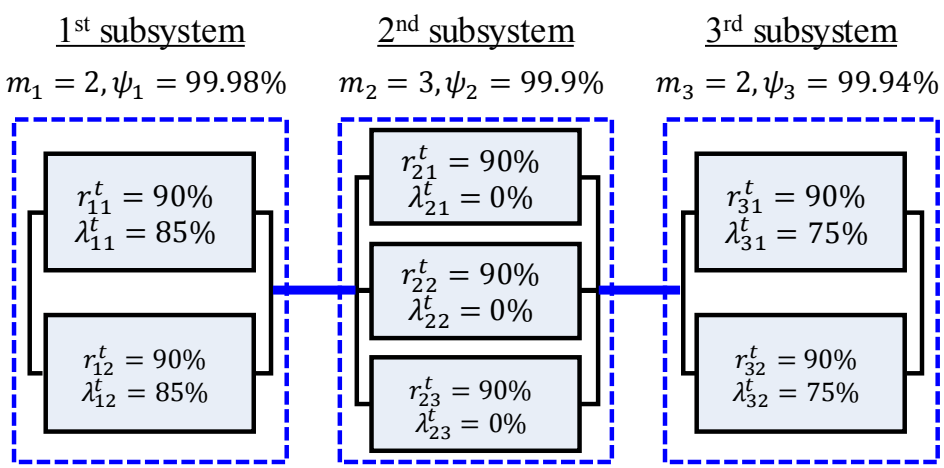


Figure 2-5 Example of resilience allocation for a series-parallel system

The life-cycle cost LCC is defined as a sum of initial development cost (C^{I}), PHM development cost (C^{PHM}), and predictive and corrective maintenance costs (C^{PM} and C^{CM}). C^{I} is the total development cost of system components. C^{PHM} consists of hardware cost (e.g., sensor unit cost, signal processing unit cost, installation/maintenance cost) and software cost (e.g., algorithm training data acquisition cost, expert consulting fee, qualification cost). C^{PM} is the expected cost of preventing potential failures which PHM units successfully predict. This cost is incurred when system failure and correct PHM estimation occur simultaneously, and thus its probability is the joint probability of two events as $\left(1-r_j^t\right)\cdot\lambda_j^t$. C^{CM} is the expected cost of system correction cost after the failures which PHM units fails to detect. The probability of C^{CM} is $\left(1-r_j^t\right)\cdot\left(1-\lambda_j^t\right)$, which corresponds to joint probability of system failure event and wrong PHM estimation event. Two maintenance cost includes shutdown cost, inspection cost, repair or replacement cost, and so on. As a result, life-cycle cost and their component costs are formulated as a function of reliability, PHM efficiency, and redundancy as below.

$$LCC = C^{\mathrm{I}} + C^{\mathrm{PHM}} + C^{\mathrm{PM}} + C^{\mathrm{CM}} \tag{2.8}$$

$$C^{\mathrm{I}} = \sum_{j=1}^{N} \alpha_j^{\mathrm{I}} \cdot \left(-\frac{T}{\ln\left(r_j^t\right)}\right)^{\beta_j^{\mathrm{I}}} \cdot \left[m_j + \exp\left(\frac{m_j}{4}\right)\right] \tag{2.9}$$

$$C^{\mathrm{PHM}} = \sum_{j=1}^{N} \alpha_j^{\mathrm{PHM}} \cdot \left(-\frac{T}{\ln\left(\lambda_j^t\right)}\right)^{\beta_j^{\mathrm{PHM}}} \cdot m_j \tag{2.10}$$

$$C^{\mathrm{PM}} = \sum_{j=1}^{N} m_j \cdot \lambda_j^t \cdot \left(1-r_j^t\right) \cdot c_j^{\mathrm{PM}} \tag{2.11}$$

$$C^{\mathrm{CM}} = \sum_{j=1}^{N} m_j \cdot \left(1 - \lambda_j^t\right) \cdot \left(1 - r_j^t\right) \cdot c_j^{\mathrm{CM}} \tag{2.12}$$

where T is the required system mission time; α_j^{I} and β_j^{I} are constants representing the physical characteristics of each component in the *j*-th subsystem and can be determined based on the collected data of component cost and reliability; α_j^{PHM} and β_j^{PHM} denote constants representing the physical characteristics of each PHM unit in the *j*-th subsystem. c_j^{PM} and c_j^{CM} are predictive and corrective maintenance costs of each component in the *j*-th subsystem. Eq. (2.9) is formulated based upon an inverse power relationship between component cost and component failure rate assuming a constant failure [38, 39]. m_j and $\exp\left(\frac{m_j}{4}\right)$ account for the costs of redundancy and interconnecting parallel components respectively. Based upon Eq. (2.9), Eq. (2.10) is formulated by replacing r_j^t with λ_j^t, and eliminating the interconnecting cost term ($\exp\left(\frac{m_j}{4}\right)$) because PHM units are not interconnected to each other. Regarding Eqs. (2.11) and (2.12), the predictive and corrective maintenances are assumed to occur in case of any component failure. Regarding the more details of Eqs. (2.9)-(2.12) and related issues for RAP, please refer [11, 38-41].

By solving the RAP of Eq. (2.5), target reliability, target PHM efficiency, and redundancy are allocated to all subsystems and delivered to two bottom-level problems. Possible methodologies to solve this problem, which is a mixed-integer nonlinear programming (MINLP) problem, are linearization approaches for a mixed-integer linear problem (MILP) [42, 43] and meta-heuristic algorithms [44, 45] (e.g., genetic algorithm and simulated annealing).

2.1.2.3. Step 2: Reliability-based Design Optimization (RBDO) (Bottom-Level 1)

The first bottom-level problem conducts reliability-based design optimization (RBDO) to design system components by minimizing initial development cost and satisfying the allocated target reliability level. Figure 2-6 shows the concept of RBDO by comparing with deterministic design optimization. Deterministic design optimization does not consider system uncertainty but only consider its deterministic characteristic. This results in the optimum solution on the failure surface and the designed system can be infeasible ($G_i(\mathbf{X};\mathbf{d}) > 0$) with low reliability ($R = 40\%$). Whereas, RBDO considers system uncertainty, and makes conservative design to ensure high reliability ($R = 99\%$).

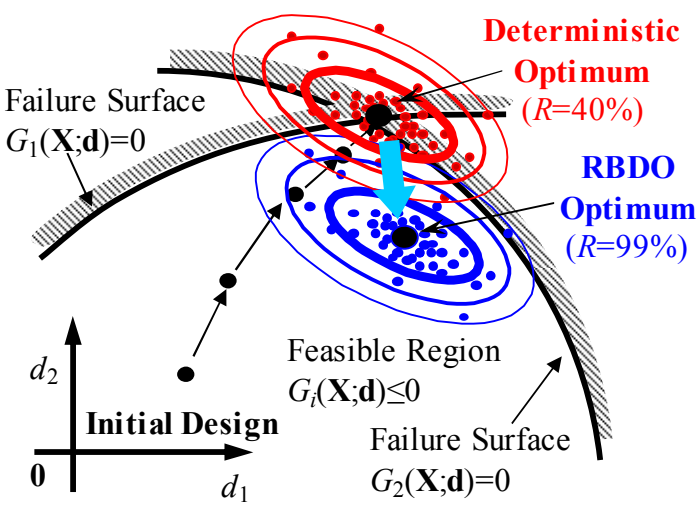


Figure 2-6 Comparison of deterministic design and reliability-based design optimization (RBDO)

The design problem for *j*-th subsystem component is formulated as below.

$$\begin{aligned} &\text{minimize}_{\mathbf{d}_j^C} \quad C_j^{\mathrm{I}}(\mathbf{d}_j^{\mathrm{C}}) \\ &\text{subject to} \quad r_j(\mathbf{d}_j^{\mathrm{C}}) = \Pr(\cap_{i=1}^{nc_j} G_j^i(\mathbf{X}_j^{\mathrm{C}}; \mathbf{d}_j^{\mathrm{C}}) \le 0) \ge r_j^t \\ &\qquad\qquad \mathbf{d}_j^{\mathrm{C,L}} \le \mathbf{d}_j^{\mathrm{C}} \le \mathbf{d}_j^{\mathrm{C,U}} \end{aligned} \tag{2.13}$$

where C_j^{I} is initial development cost of *j*-th subsystem component; $\mathbf{d}_j^{\mathrm{C}}$ is the vector of design variables of *j*-th subsystem component; $r_j(\cdot)$ is *j*-th subsystem reliability function; r_j^t is the allocated target reliability for *j*-th subsystem; nc_j is the number of constraints; $G_j^i(\cdot)$ is mutually exclusive performance function; $\mathbf{X}_j^{\mathrm{C}}$ is random variable vector; $\mathbf{d}_j^{\mathrm{C,L}}$ and $\mathbf{d}_j^{\mathrm{C,U}}$ are the lower and upper boundaries of $\mathbf{d}_j^{\mathrm{C}}$ respectively. Here, C_j^{I} can be formulated as system designer's interest, such as manufacturing cost, system volume and system mass. This is different from C^{I} in RAP problem (Eq. (2.9)) which is an empirical model based upon the assumptions [38, 39].

In order to solve RBDO problems such as Eq. (2.13), many methodologies have been elaborated for few decades. There are mainly three categories of RBDO algorithms according to how to handle reliability analysis within design optimization: double-loop, decoupled (or sequential) approach, and single-loop approach. The double-loop RBDO algorithms require two nested optimization loops – an outer loop for design optimization and an inner loop for reliability analysis. The latter is needed to evaluate probabilistic constraints at each design iteration. The decoupled RBDO algorithm decouples two loops into the outer loop for deterministic design optimization and the inner loop for reliability analysis. The separated two loops are performed sequentially until a design optimization converges. Compared to the double-loop RBDO, which

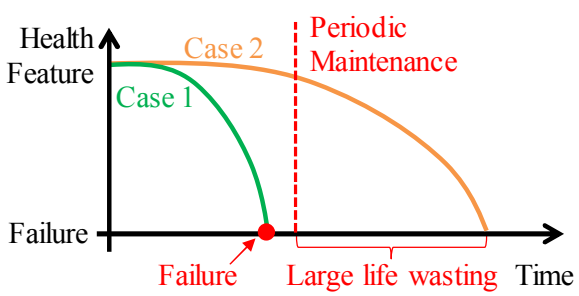
conducts the reliability analysis for all design changes in the outer loop, the decoupled RBDO conducts the reliability analysis only once after the deterministic optimum design from the outer loop is achieved. Another strategy to decouple the nested loop is the single-loop RBDO which eliminates the inner loop for the reliability analysis by approximating probabilistic constraints to deterministic ones. Probabilistic constraints are approximated into deterministic ones and then simple design optimization is conducted without additional reliability analysis. Table 2-1 lists three categories of RBDO with representative algorithms. The solution of RBDO, optimal component design is delivered to the second bottom-level problem.

Table 2-1 Lists of RBDO algorithms

Category	**RBDO algorithm**
Double-loop approaches	- Sensitivity-based approximation [46] - Reliability index approach (RIA)-based [47] - Performance measure approach (PMA)-based [48]
Decoupled approaches	- Safety factor-based [49] - Sequential optimization and reliability assessment (SORA) [50] - Direct decoupling approach [51]
Single-loop approaches	- Single-loop single vector (SLSV) [52] - SLSV with most-probable point [53] - SLSV with Karush-Kuhn-Tucker condition [54] - Complete single-loop [55] - Semi-single loop [56]

2.1.2.4. Step 3: Prognostics and Health Management (PHM) Design (Bottom-Level 2)

The objective of this problem is to design PHM unit by minimizing PHM development cost and satisfying the allocated PHM efficiency level from the RAP problem given the component design from the RBDO problem. Prognostics and health management (PHM) is a discipline of techniques that evaluates the current health state of an engineered system, detects failures in advance, and conducts optimal maintenance actions to minimize life-cycle maintenance costs. It allows a conventional maintenance strategy (scheduled or unscheduled) to be substituted with a condition-based maintenance (CBM) strategy that can prevent unexpected failures and reduce maintenance costs. Figure 2-7 shows the comparison of two maintenance strategies with two health degradation cases. As an engineered system operates, its health degrades gradually and failure occurs when health feature becomes zero. For the case 1 of fast health degradation prior to periodic maintenance, the scheduled maintenance strategy yields failure whereas the CBM with PHM proactively prevents failure. For the case 2 of slow degradation, the scheduled maintenance strategy would waste system life which is further remained whereas the CBM with PHM can effectively exploit system life.



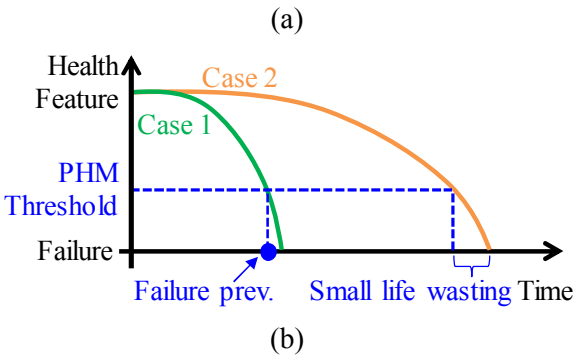


Figure 2-7 Comparison of (a) schedule-based maintenance and (b) condition-based maintenance with prognostics and health management

PHM is widely used for various applications, such as journal bearings [57], gear systems [58], power transformers [59], power generators [60], and fuel cells [61]. And along with recent advances in Internet of Things (IoT) and Industry 4.0, the demands on PHM keep increasing [62]. Related topics are sensor network design, health diagnostics, and health prognostics. Sensor network design makes data acquisition (DAQ) unit to acquire health-relevant data while minimizing sensor implementation cost [27, 28, 63-65]. Figure 2-8 and Figure 2-9 show the examples of health diagnostics and health prognostics respectively. Health diagnostics, also called as fault diagnostics, estimates the current health state of an engineered system as bi-health states (healthy or faulty) or multi health states (healthy, warning, or faulty) [57-60, 66-74]. Health prognostics predicts remaining useful life (RUL) of an engineered system, taking into account the tendency of future health degradation. [29, 30, 61, 74-86].

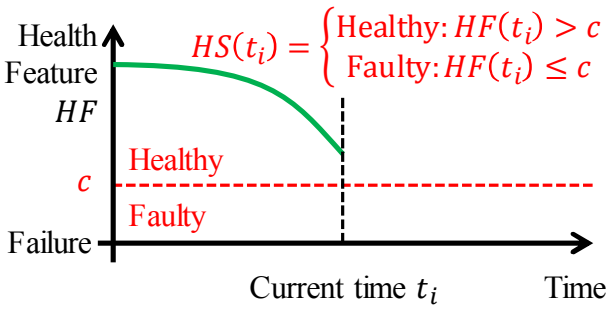


Figure 2-8 Example of health diagnostics

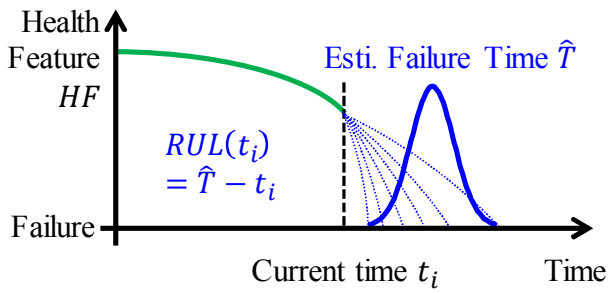


Figure 2-9 Example of health prognostics

The PHM unit design for j-th subsystem component is formulated as below.

$$\begin{aligned} &\text{minimize}_{\mathbf{d}_j^{PHM}} \quad C_j^{\text{PHM}}(\mathbf{d}_j^{\text{PHM}}) \\ &\text{subject to} \quad \lambda_j(\mathbf{d}_j^{\text{PHM}}) \ge \lambda_j^t \\ &\qquad \mathbf{d}_j^{\text{PHM,L}} \le \mathbf{d}_j^{\text{PHM}} \le \mathbf{d}_j^{\text{PHM,U}} \end{aligned} \tag{2.14}$$

where C_j^{PHM} is PHM development cost for j-th subsystem component; $\mathbf{d}_j^{\text{PHM}}$ is PHM design vector of j-th subsystem component of which lower and upper boundaries are $\mathbf{d}_j^{\text{PHM,L}}$ and $\mathbf{d}_j^{\text{PHM,U}}$ respectively; λ_j is the PHM efficiency of j-th subsystem component. C_j^{PHM} mainly consists of PHM algorithm

development cost and sensing unit costs related to sensor types and their numbers. $\mathbf{d}_j^{\mathrm{PHM}}$ consists of hardware and software design variables. The hardware design variables are sensor type, sensor number, and their locations. These variables are related to sensor network (SN) design problem which makes data acquisition (DAQ) unit to acquire health-relevant data while minimizing sensor implementation cost [27, 28, 63-65]. The software design variables are the type of PHM algorithm and corresponding parameters. The problem of Eq. (2.14) is a mixed-integer nonlinear programming (MINLP) problem, and thus can be solved using linearization approaches for a mixed-integer linear problem (MILP) [42, 43] and meta-heuristic algorithms [44, 45] as mentioned in RAP in Chapter 2.1.2.2.

2.2 False and Missed Alarms in Prognostics and Health Management

2.2.1 Definition of False and Missed Alarms

False and missed alarms in PHM mean an erroneous report on the health state of an engineered system. Their possible causes are sensor malfunction, imperfection in the PHM design, unexpected failure modes, human error, measurement uncertainty, and so on. A false alarm (false positive or false faulty) estimates a healthy engineered system to be faulty and a missed alarm (false negative or false healthy) estimates a faulty engineered system to be healthy. Assuming that maintenance actions are solely determined by the health estimation result from PHM, a false alarm yields unnecessary system shutdown and unnecessary maintenance, and a missed alarm yields system failure and the need for corrective maintenance. Mathematically, they can be formulated as conditional probabilities, as shown below.

$$FA = \Pr\left(\mathrm{E}_{\mathrm{faulty}}^{\mathrm{esti}} \middle| \mathrm{E}_{\mathrm{healthy}}^{\mathrm{true}}\right) \tag{2.15}$$

$$MA = \Pr\left(\mathrm{E}_{\mathrm{healthy}}^{\mathrm{esti}} \middle| \mathrm{E}_{\mathrm{faulty}}^{\mathrm{true}}\right) \tag{2.16}$$

where FA and MA are false and missed alarm rates respectively; $\mathrm{E}_{\mathrm{healthy}}^{\mathrm{true}}$ and $\mathrm{E}_{\mathrm{faulty}}^{\mathrm{true}}$ are the events in which the true health state of an engineered system is healthy and faulty, respectively; and $\mathrm{E}_{\mathrm{healthy}}^{\mathrm{esti}}$ and $\mathrm{E}_{\mathrm{faulty}}^{\mathrm{esti}}$ are the events where the health state of an engineered system is estimated to be healthy and faulty, respectively. Table 2-2 summarizes the descriptions above.

Table 2-2 False alarms in PHM

Type	Health state		Result	Formulation
	True	Esti.		
False alarm	Healthy	Faulty	Unnecessary shutdown & maintenance	$FA = \Pr\left(\mathrm{E}_{\mathrm{faulty}}^{\mathrm{esti}} \middle| \mathrm{E}_{\mathrm{healthy}}^{\mathrm{true}}\right)$
Missed alarm	Faulty	Healthy	System failure & corrective maintenance	$MA = \Pr\left(\mathrm{E}_{\mathrm{healthy}}^{\mathrm{esti}} \middle| \mathrm{E}_{\mathrm{faulty}}^{\mathrm{true}}\right)$

Figure 2-10 and Figure 2-11 show examples of a false alarm and a missed alarm, respectively, due to the imperfect PHM model; this is the major concern in PHM design. These examples use one dimensional (i) health feature and (ii) threshold-based health diagnostics. First, the health feature (HF) is a quantitative metric relevant to the health state of an engineered system; it changes as health degrades. The health feature has randomness due to uncertainty factors, such as variant operating conditions and measurement noise. PHM utilizes the health feature to estimate the health state of an engineered system. The examples of a health feature are the directionality metric of the vibration spectral response in journal bearing systems [57], the directional Mahalanobis distance of capacitance for water-cooled power generators [60], impedance spectrum parameters for proton exchange membrane (PEM) fuel cells [61], and the generalized damage parameter (GDP) for gas turbine discs [84]. Second, threshold-based health diagnostics estimates the health state of an engineered system by comparing the health feature of an engineered system to a health state criterion [87, 88]. The health state criterion (c_{esti}) is designed or estimated to be located between healthy systems and faulty systems. For the case of Figure 2-10 and Figure 2-11,

if the health feature is smaller than c_{esti}, the system is estimated to be healthy ($E^{esti}_{healthy}$); otherwise, it is determined to be faulty (E^{esti}_{faulty}). However, this estimated health state criterion c_{esti} can differ from the true health state criterion c_{true}, which is the true boundary between the events of a system's true health state of healthy ($E^{true}_{healthy}$) and faulty (E^{true}_{faulty}). For a real engineered system, the explicit true health state model such as c_{true} is usually not available. But here, it is assumed to be available to explain the concept of false and missed alarms. Discrepancies between c_{esti} and c_{true} are possible due to insufficient data, data uncertainty (e.g., measurement noise, variant operating conditions), improper PHM algorithm selection, inadequate parameters, and so on. As a result, a system in which the health feature is located between the two health criteria c_{esti} and c_{true} (gray areas in Figure 2-10 and Figure 2-11) will have false and missed alarm problems.

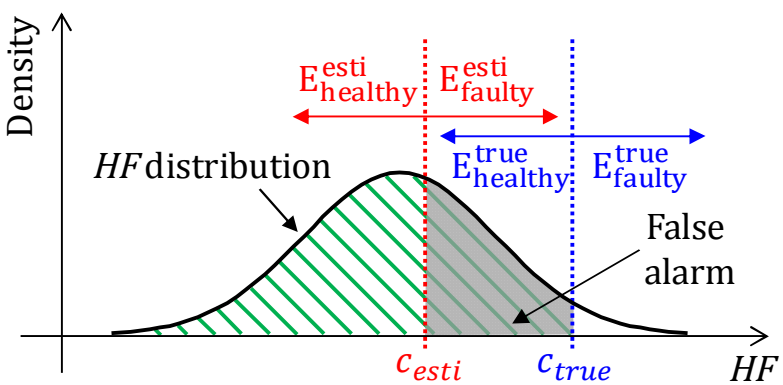


Figure 2-10 Example of a false alarm

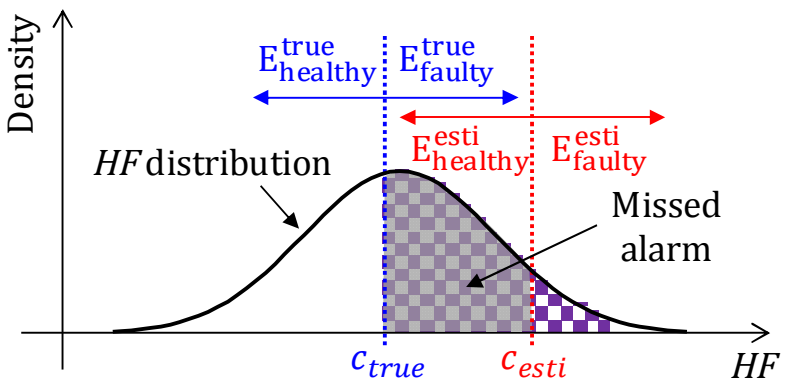


Figure 2-11 Example of a missed alarm

According to Eqs. (2.15) and (2.16), the probabilities of false alarm and missed alarm are quantified as shown below in Eqs. (2.17) and (2.18). They correspond to the ratio of the gray area to the diagonal-lined area in Figure 2-10 and the gray area to the square-patterned area in Figure 2-11, respectively.

$$FA = \Pr\left(E^{esti}_{faulty} \middle| E^{true}_{healthy}\right) = \Pr(HF \geq c_{esti} | HF < c_{true}) = \frac{\Pr(HF \geq c_{esti} \cap HF < c_{true})}{\Pr(HF < c_{true})} \tag{2.17}$$

$$MA = \Pr\left(E^{esti}_{healthy} \middle| E^{true}_{faulty}\right) = \Pr(HF < c_{esti} | HF \geq c_{true}) = \frac{\Pr(HF < c_{esti} \cap HF \geq c_{true})}{\Pr(HF \geq c_{true})} \tag{2.18}$$

In order to address false and missed alarm problems in PHM, some researches have been conducted. Tian et al. [89] analyzed the causes and mechanisms of false and missed alarms and suggested possible solutions to reduce them in aircraft hydraulic systems. Kim et al. [90] proposed a power spectrum analysis-

based fault indicator for induction motor rotor fault detection. The proposed indicator is physically immune to false alarms due to the magnetic asymmetry in the rotor and its low frequency load torque oscillations. Yang et al. [91] proposed a rotor fault frequency component produced by space harmonic waves for induction motor rotor cage fault detection. This component does not penetrate into the rotor yoke to reach axial ducts; thus, it is physically free from false fault alarms. Cui et al. [92] suggested a condition-based multistage false alarm detection and reduction method. The false alarm evolution process is divided into three stages and then the dynamic Bayesian network inference model is developed to detect and suppress any false alarms for each stage. The proposed framework was demonstrated with experimental data from a milling machine.

Meanwhile, the assumption that maintenance actions are solely determined by the health estimation result is not guaranteed for real engineering systems; the decision of a maintenance action or strategy is determined considering not only health estimation result but also various factors. First thing to consider is various health-relevant information such as operating conditions, past inspection records, sensory signals, and experts' opinion. Referring the information, a system operator interprets health estimation result whether it is correct or not. If a system operator fails to interpret false and missed alarms correctly, they yield unnecessary maintenance and corrective maintenance, respectively. Second, the consequence of system failures should be considered. For a system with severe losses of capital, human, reputation, and so on in the event of failure, its maintenance is determined in a conservative manner with frequent inspections. Additionally, its decision takes into consideration maintenance resources (e.g.,

labor, spares, and equipment) and regulation of a maintenance standard, template or guidance provided by system suppliers. As this paper concerns the analysis on life-cycle maintenance cost for fault diagnosis design, the factors except health estimation result by fault diagnosis are not considered. For the details regarding maintenance decisions, please refer the references of [93, 94].

2.2.2 Quantification of False and Missed Alarms

In order to calculate the probabilities of Eqs. (2.15) and (2.16), this study employs a health estimation matrix [27, 28]. This is a square matrix in which the rows and columns are the true health state and the estimated health state, respectively. Its element $N_{\alpha\hat{\beta}}$ is the number of samples estimated to be β health state given the true α health state. Considering binary health states, healthy (H) and faulty (F), there are four conditional health state estimation events (true healthy, false healthy, true faulty, and false faulty), as shown in Table 2-3. In order to estimate the health estimation matrix, Monte Carlo simulation (MCS) is used of its high accuracy and general applicability for various problems [19]. MCS randomly generates health feature samples based upon the uncertainties, such as the degree of health degradation and operating conditions. According to the true and estimated health state using a given PHM model, the number of samples in true α health state and estimated β health state is allocated to $N_{\alpha\hat{\beta}}$, and false and missed alarm rates can be quantified as Eqs. (2.19) and (2.20).

Table 2-3 Health estimation matrix of two health states

Health estimation matrix		**Estimated health state**	
		Healthy ($\widehat{\mathrm{H}}$)	Faulty ($\widehat{\mathrm{F}}$)
True health state	Healthy (H)	$N_{\mathrm{H}\widehat{\mathrm{H}}}$	$N_{\mathrm{H}\widehat{\mathrm{F}}}$
	Faulty (F)	$N_{\mathrm{F}\widehat{\mathrm{H}}}$	$N_{\mathrm{F}\widehat{\mathrm{F}}}$

$$FA = \frac{N_{\mathrm{H}\widehat{\mathrm{F}}}}{N_{\mathrm{H}\widehat{\mathrm{H}}} + N_{\mathrm{H}\widehat{\mathrm{F}}}} \tag{2.19}$$

$$MA = \frac{N_{\mathrm{F}\widehat{\mathrm{H}}}}{N_{\mathrm{F}\widehat{\mathrm{H}}} + N_{\mathrm{F}\widehat{\mathrm{F}}}} \tag{2.20}$$

For a system of multiple health states, including healthy (H) and n failure modes (F_i for $i = 1, \ldots, n$), the health estimation matrix is a $(1+n)$-by-$(1+n)$ matrix as shown in Table 2-4.

Table 2-4 Health estimation matrix of multiple health states

Health estimation matrix			**Estimated health state**			
			Healthy ($\widehat{\mathrm{H}}$)	Faulty		
				$\widehat{\mathrm{F}}_1$	…	$\widehat{\mathrm{F}}_n$
True health state	Healthy (H)		$N^{\mathrm{multi}}_{\mathrm{H}\widehat{\mathrm{H}}}$	$N^{\mathrm{multi}}_{\mathrm{H}\widehat{\mathrm{F}}_1}$	…	$N^{\mathrm{multi}}_{\mathrm{H}\widehat{\mathrm{F}}_n}$
	Faulty	F_1	$N^{\mathrm{multi}}_{\mathrm{F}_1\widehat{\mathrm{H}}}$	$N^{\mathrm{multi}}_{\mathrm{F}_1\widehat{\mathrm{F}}_1}$	…	$N^{\mathrm{multi}}_{\mathrm{F}_1\widehat{\mathrm{F}}_n}$
		⋮	⋮	⋮	⋱	⋮
		F_n	$N^{\mathrm{multi}}_{\mathrm{F}_n\widehat{\mathrm{H}}}$	$N^{\mathrm{multi}}_{\mathrm{F}_n\widehat{\mathrm{F}}_1}$	…	$N^{\mathrm{multi}}_{\mathrm{F}_n\widehat{\mathrm{F}}_n}$

In order to apply the above quantification approach, this matrix can be converted into a binary 2-by-2 health estimation matrix by summing elements as shown below.

$$N_{\mathrm{H}\widehat{\mathrm{H}}} = N_{\mathrm{H}\widehat{\mathrm{H}}}^{\mathrm{multi}} \tag{2.21}$$

$$N_{\mathrm{H}\widehat{\mathrm{F}}} = \sum\nolimits_{i=1}^{n} N_{\mathrm{H}\widehat{\mathrm{F}}_i}^{\mathrm{multi}} \tag{2.22}$$

$$N_{\mathrm{F}\widehat{\mathrm{H}}} = \sum\nolimits_{i=1}^{n} N_{F_i\widehat{\mathrm{H}}}^{\mathrm{multi}} \tag{2.23}$$

$$N_{\mathrm{F}\widehat{\mathrm{F}}} = \sum\nolimits_{i=1}^{n} \sum\nolimits_{j=1}^{n} N_{F_i\widehat{F}_j}^{\mathrm{multi}} \tag{2.24}$$

where $N_{\alpha\widehat{\beta}}^{\mathrm{multi}}$ is the number of samples estimated to be β health state given the true α health state in the multiple health state health estimation matrix.

In practice, false and missed alarms could hurt the accuracy of the health state estimation. One possible approach to correctly estimate the health state under false and missed alarms is through Bayesian inference [95]. System operators are interested in whether a system is really healthy (H) when the PHM solution estimates the system health state to be healthy ($\widehat{\mathrm{H}}$). According to Bayes' theorem, the following equation can be employed.

$$\frac{\Pr\left(\mathrm{H}\middle|\widehat{\mathrm{H}}\right)}{\Pr\left(\mathrm{F}\middle|\widehat{\mathrm{H}}\right)} = \frac{\Pr\left(\widehat{\mathrm{H}}\middle|\mathrm{H}\right)}{\Pr\left(\widehat{\mathrm{H}}\middle|\mathrm{F}\right)} \cdot \frac{\Pr(\mathrm{H})}{\Pr(\mathrm{F})} = \frac{1-\mathrm{FA}_I}{\mathrm{FA}_{II}} \cdot \frac{R}{1-R} = \mathrm{BF}_{\mathrm{HF}}^{\widehat{\mathrm{H}}} \cdot \frac{R}{1-R} \tag{2.25}$$

where $\mathrm{BF}_{\mathrm{HF}}^{\widehat{\mathrm{H}}}$ is a Bayes factor indicating the ratio of the healthy health state detection rate to the missed alarm rate. Here, the left-hand side probabilities $\Pr\left(\mathrm{H}\middle|\widehat{\mathrm{H}}\right)$ and $\Pr\left(\mathrm{F}\middle|\widehat{\mathrm{H}}\right)$ indicate the probability that a system is truly healthy and faulty, respectively, when the PHM solution estimates the system health state to

be healthy. Similarly, Bayesian inference for faulty health state estimation ($\hat{\mathrm{F}}$) can be formulated as below.

$$\frac{\Pr(\mathrm{F}|\hat{\mathrm{F}})}{\Pr(\mathrm{H}|\hat{\mathrm{F}})} = \frac{\Pr(\hat{\mathrm{F}}|\mathrm{F})}{\Pr(\hat{\mathrm{F}}|\mathrm{H})} \cdot \frac{\Pr(\mathrm{F})}{\Pr(\mathrm{H})} = \frac{1-\mathrm{FA}_{II}}{\mathrm{FA}_{I}} \cdot \frac{1-R}{R} = \mathrm{BF}_{\mathrm{FH}}^{\hat{\mathrm{F}}} \cdot \frac{1-R}{R} \tag{2.26}$$

where $\mathrm{BF}_{\mathrm{FH}}^{\hat{\mathrm{F}}}$ is a Bayes factor indicating the ratio of the faulty health state detection rate to the false alarm rate.

2.3 Summary and Discussion

Resilience engineering is a novel and innovative discipline considering resilience, the ability of an engineered system to maintain its functionality by resisting and recovering against adverse events. This is based on a resilience measure which integrates two health-related measures: reliability, which focuses on resisting against adverse events, and prognostics and health management (PHM) efficiency, which focuses on recovering from adverse events. Utilizing a resilience measure can helps to analyze system failure probability and corresponding risk, and determine operation actions (e.g., maintenance and design modification) to maintain system performance.

In conventional design approaches such as reliability-based design optimization (RBDO) and PHM, the two properties of resilience, resisting and recovering, are considered separately. However, two are properties are complementary to each other in terms of preventing failures as shown in Figure 2-12. Thus, the conventional design approaches without considering their interaction can yield conservative or failure-prone system design with high life-

cycle cost. Whereas resilience-driven system design, which considers two properties cohesively, enables engineering design that prevents over-designed and/or fault-prone systems and assures system availability while minimizing life-cycle cost.

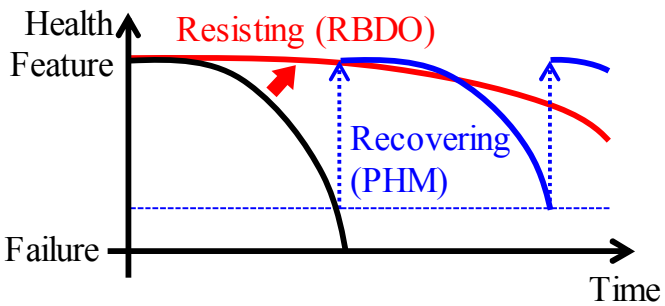


Figure 2-12 Resisting and recovering actions to maintain system functionality

Meanwhile, the one of challenge in PHM, as well as in RDSD, is false and missed alarms. The false and missed alarms, estimating a healthy system as faulty one or a faulty system as healthy one, can severely reduce the system availability, sustainability and reliability. The presence of false and missed alarms makes PHM and RDSD unreliable and hinders its application especially for the high risky engineered systems such as nuclear power plants. Although both alarms affect system availability, current resilience engineering considers missed alarms only. Therefore, false alarms should be considered for the sake of successful implementation of RDSD.

Chapter 3. Resilience Analysis Considering False Alarms

Considering the importance of false alarms reviewed in Chapter 1.1 , this Chapter aims at refining engineering resilience measure, which currently does not consider false alarms, to address false alarms. As the resilience measure is a key factor in resilience analysis as well as resilience-driven system design (RDSD), the system design outcome of RDSD is highly dependent on the formulation of the resilience measure. That is, if false alarms are not considered in the resilience measure, engineered systems can be prone to false alarm issues. The Chapter is organized as follows: Chapter 3.1 proposes the new formulation of a resilience measure that considers false alarms. Case studies described in Chapter 3.2 show the importance of addressing false alarms by comparing the original and the proposed resilience measures. Summary and discussion are discussed in Chapter 3.3.

3.1 Resilience Measure Considering False Alarms

This Chapter proposes a new resilience measure that considers false alarms. Consideration of false alarms results in a significant difference in the resilience measure. To verify the proposed measure, the existing and newly proposed resilience measures are compared based upon the resilience scenarios shown in Figure 3-1 and Figure 3-2. Here, the symbols of the events of true health state ($E^{true}_{healthy}$ and E^{true}_{faulty}) and estimated health state ($E^{esti}_{healthy}$ and E^{esti}_{faulty}) are changed into H, F, $\widehat{H}$, and $\widehat{F}$ respectively to provide a better description.

For a system with a healthy health state with probability R, it can be

evaluated as healthy or faulty by the PHM solution. Correct health estimation (e.g., a healthy system determined to be healthy) results in the system operating normally (#N-1 in Figure 3-2). An incorrect health estimation (e.g., a healthy system described as faulty) results in unnecessary maintenance actions (#N-2). The existing approach disregards the presence of the false alarm, and formulates an incorrect measure that does not consider the false alarm rate FA (#E-1 in Figure 3-1). In contrast, the new approach, which considers false alarms, formulates the correct measure (#N-1). As a result, the probabilities of "system normal" operation are different, R (#E-1) and $(1 - FA_I) \cdot R$ (#N-1). Furthermore, the new approach can quantify the probability of unnecessary maintenance action due to a false alarm, specifically $FA \cdot R$ (#N-2). Correspondingly, the new cost term related to unnecessary maintenance actions should be included in resilience-driven system design.

For a system that has a faulty health state with a probability $1 - R$, the existing (#E-2, #E-3) and new approaches (#N-3, #N-4) have the same formulations except the PHM efficiency terms, Λ and Λ_{FA}. The differences between the PHM efficiencies determined by the two approaches are two-fold: data employment and calculation method. First, the existing measure employs data from healthy and faulty systems to quantify the PHM efficiency, which is not rigorous, and thus prone to error. This is because PHM efficiency ($\Lambda = \Pr(\hat{\mathrm{F}}|\mathrm{F})$) is the conditional probability of the correct health estimation event given a faulty system event (F), not whole systems (F ∪ H). In contrast, the new measure employs only data from faulty systems to calculate PHM efficiency, as in Eqs. (2.19) and (2.20). Second, the existing measure calculates PHM

efficiency Λ by multiplying the correct prognosis probability Λ_P and the correct diagnosis probability Λ_D ($\Lambda = \Lambda_P \cdot \Lambda_D$). Decoupling of Λ into Λ_P and Λ_D transforms the PHM design problem into a hierarchical two-step problem, specifically, the SN design (hardware) and the prognostic algorithm design (software) [11]. Although this approach facilitates the PHM design problem, there are still challenges, such as decision making on the target correct diagnosis probability. In addition, this approach is not applicable to resilience analysis for systems in operation. Systems in operation have historical PHM data, including estimated health states from the PHM solution and true health states determined by field engineers' inspections, as shown in Table 2-3 and Table 2-4. Thus, the two probabilities Λ_D and Λ_P cannot be inversely calculated based on this historical PHM data. However, the new measure can analyze the resilience of the system in operation using $\Lambda_{\mathrm{FA}} = 1 - MA$ (#N-4) and Eq. (2.20). In addition, it is applicable to the PHM design problem with the use of (meta) heuristic algorithms [44] such as Monte Carlo simulation, simulated annealing, and the genetic algorithm.

#	True HS	Esti. HS	Result	Formulation	Avail.
E-1	Healthy R		Normal Operation	$\Pr(\mathrm{H}) = R$	O
E-2	Faulty $1-R$	Healthy $1-\Lambda$	System Failure	$\Pr(\hat{\mathrm{H}}\mathrm{F}) = \Pr(\hat{\mathrm{H}}\|\mathrm{F}) \cdot \Pr(\mathrm{F})$ $= (1-\Lambda) \cdot (1-R)$	X
E-3		Faulty Λ	Restoration κ	$\Pr(\mathrm{E}_{mr}\hat{\mathrm{F}}\mathrm{F}) = \kappa \cdot \Lambda \cdot (1-R)$ $\Lambda = \Pr(\hat{\mathrm{F}}\|\mathrm{F}) = \Lambda_P \cdot \Lambda_D$	O

Figure 3-1 Resilience scenario using the existing resilience measure [11]

#	True HS	Esti. HS	Result	Formulation	Avail.
N-1	Healthy R	Healthy $1-FA$	Normal Operation	$\Pr(\hat{\mathrm{H}}\mathrm{H}) = \Pr(\hat{\mathrm{H}}\|\mathrm{H}) \cdot \Pr(\mathrm{H}) = (1-FA) \cdot R$	O
N-2		Faulty FA	Unnecessary Maintenance	$\Pr(\hat{\mathrm{F}}\mathrm{H}) = \Pr(\hat{\mathrm{F}}\|\mathrm{H}) \cdot \Pr(\mathrm{H}) = FA \cdot R$	X
N-3	Faulty $1-R$	Healthy MA	System Failure	$\Pr(\hat{\mathrm{H}}\mathrm{F}) = \Pr(\hat{\mathrm{H}}\|\mathrm{F}) \cdot \Pr(\mathrm{F}) = MA \cdot (1-R)$	X
N-4		Faulty $1-MA$	Restoration κ	$\Pr(\mathrm{E}_{mr}\hat{\mathrm{F}}\mathrm{F}) = \Pr(\mathrm{E}_{mr}\|\hat{\mathrm{F}}\mathrm{F}) \cdot \Pr(\hat{\mathrm{F}}\mathrm{F}) = \kappa \cdot (1-MA) \cdot (1-R)$	O

Figure 3-2 Resilience scenario considers false alarms

The resilience measure is formulated as the summation of conditional probabilities of maintaining the system's availability. According to Figure 3-1 and Figure 3-2, the existing resilience measure is the summation of #E-1 and #E-3, which is equal to Eq. (2.4) in Chapter 2.1.1.3. The proposed resilience measure that considers false alarms is the summation of #N-1 and #N-4 as

$$\begin{aligned}\Psi_{\mathrm{FA}} &= \Pr(\hat{\mathrm{H}}\mathrm{H}) + \Pr(\mathrm{E}_{mr}\hat{\mathrm{F}}\mathrm{F}) \\ &= (1-FA)\cdot R + \kappa\cdot(1-MA)\cdot(1-R) \\ &= (1-FA)\cdot R + \kappa\cdot\Lambda_{\mathrm{FA}}\cdot(1-R)\end{aligned} \tag{3.1}$$

In the same way as the existing measure, the proposed measure is formulated in a probabilistic manner, ranging from 0 to 1. The existing measure is proportional to the reliability R, of which the weight factor $(1-\varepsilon_\rho)$ is always positive (Figure 2-3). For the new measure, the reliability weight factor ($(1-FA)-\kappa\cdot(1-MA) = MA-FA$ for $\kappa=1$) can be negative for a large FA case as compared to MA. This means that the system resilience would decrease, along with the reliability increment, due to a false alarm. It does not

mean that the reliability should be lowered to maximize resilience. Reliability should be decided to minimize the life-cycle cost (LCC) considering the tradeoff between the unnecessary maintenance action rate $FA \cdot R$ (#N-2), the system failure rate $MA \cdot (1-R)$ (#N-3), the system restoration rate $(1-MA) \cdot (1-R)$ (#N-4), and corresponding costs. The life-cycle cost includes estimated unnecessary maintenance cost $C^{\mathrm{UM}} = c^{\mathrm{UM}} \cdot FA \cdot R$, estimated system failure cost $C^{\mathrm{CM}} = c^{\mathrm{CM}} \cdot MA \cdot (1-R)$, estimated predictive maintenance cost $C^{\mathrm{PM}} = c^{\mathrm{PM}} \cdot (1-MA) \cdot (1-R)$, and so on, where c^{UM}, c^{CM} and c^{PM} are the unnecessary maintenance cost, the corrective maintenance cost, and the predictive maintenance cost, respectively. For additional information about the systematic approach to optimizing the reliability by minimizing the life-cycle cost, please refer to Chapter 2.1.2.

No consideration of the false alarm leads to the error in the resilience calculation as

$$\mathrm{Err}_{\Psi} = \Psi - \Psi_{\mathrm{FA}} = FA \cdot R + \kappa \cdot (\Lambda - \Lambda_{\mathrm{FA}}) \cdot (1-R) \tag{3.2}$$

where the first error term $(FA \cdot R)$ comes from not considering the false alarm, and the second error term $\kappa \cdot (\Lambda - \Lambda_{\mathrm{FA}}) \cdot (1-R)$ comes from the difference in the method of calculating the PHM efficiency. The first term is relatively greater than the second term, making the resilience error Err_{Ψ} have positive value $(\Psi > \Psi_{\mathrm{FA}})$. This means that the existing resilience measure Ψ overestimates the system as more resilient than it actually is (Ψ_{FA}); therefore, a system designed with the existing measure Ψ would fail to satisfy the expected target resilience level.

3.2 Case Studies

This Chapter aims to demonstrate the importance of considering false alarms in the resilience measure. For this purpose, two case studies are employed. The first examines numerical examples and the second studies an electro-hydrostatic actuator (EHA). The existing and the new resilience measures are compared for each case study.

3.2.1 Numerical Example

This Chapter presents numerical examples using sample health estimation matrices as shown in Table 3-1 (a) and (b). Both health estimation matrices have one hundred samples with equal reliability but different false and missed alarm rates. According to the predefined equations, Table 3-1 (a) has a system reliability R of $(80+10)/(80+10+2+8) = 90/100 = 90\%$, a false alarm rate FA of $10/(80+10) = 11\%$, and a missed alarm rate MA of $3/(3+7) = 30\%$. Likewise, Table 3-1 (b) has R of 90%, FA of 2%, and MA of 10%. As discussed in Chapter 2.1.1.4, it is hard to calculate the PHM efficiency of the existing measure with the health estimation matrix; thus, it is assumed to be the same as that of the new measure ($\Lambda \coloneqq \Lambda_{\mathrm{FA}} = 1 - MA$). Assuming the maintenance success rate κ to be unity (as discussed in Chapter 2.1.1.2), the resilience measures are calculated using Eqs. (2.4) and (3.1). Table 3-2 lists their values, with the resilience of a non-restorative system without a PHM solution ($\Psi_{\mathrm{w/o\ PHM}} = R = 90\%$). For the case with the high false and missed alarm rates (a), the two measures have significant discrepancy

(97%−87%=10%), and would make different decisions on system design and operation issues. Regarding the PHM implementation issue, for example, analysis with the existing measure Ψ suggests implementing the PHM solution because it increases resilience from 90% to 97%. However, this is not a correct decision because false alarms are not considered. Analysis with the new measure Ψ_{FA} that considers false alarms suggests *exclusion* of the PHM solution, because it decreases resilience from 90% to 87%. More systematically, the decision about PHM implementation must be determined by solving a life-cycle cost (LCC) problem. In this case study, although PHM decreases the system resilience and yields unnecessary maintenance costs, it can prevent system failure with 70% probability $(1 - MA)$. Thus, if the system is highly risky and its failure cost is dominant compared to any unnecessary maintenance costs, then the PHM should not be excluded. For the case with the low false and missed alarm rates (b), the two measures are comparable and the difference is relatively small (99%−97%=2%). Although the difference is small, the resulting difference in life-cycle cost can be enormous depending on system failure consequences (e.g., human loss and/or significant capital loss).

Table 3-1 Health estimation matrix of sample case study data

(a) High FMA Rates		**Estimated HS**	
		Healthy	Faulty
True HS	Healthy	80	10
	Faulty	3	7

(b) Low FMA Rates		**Estimated HS**	
		Healthy	Faulty
True HS	Healthy	88	2
	Faulty	1	9

*FMA: false and missed alarms; HS: health state;

Table 3-2 Resilience measure calculation of numerical examples

Resilience Measure		Mathematical Formulation	FMA Rates	
			(a) High	(b) Low
w/ PHM	Existing	$\Psi = R + \kappa \cdot \Lambda \cdot (1 - R)$	97%	99%
	Proposed	$\Psi_{\mathrm{FA}} = (1 - FA) \cdot R + \kappa \cdot (1 - MA) \cdot (1 - R)$	87%	97%
w/o PHM		$\Psi_{\mathrm{w/o\ PHM}} = R$	90%	

*FMA: false and missed alarms;

In the resilient system design framework in Chapter 2.1.2, the system is designed to satisfy a target resilience level, while minimizing life-cycle cost. If the evaluation of the system's resilience is not accurate due to the ignorance of false alarms, the system will not satisfy the intended target resilience level and will be prone to the false alarm problems. Let us consider a resilient system design problem targeting a 97% resilience level. As shown in Table 3-2, the existing measure Ψ evaluates the system resilience level non-conservatively (i.e., 97% for the system with high false and missed alarm rates); whereas, the proposed measure Ψ_{FA} evaluates correctly (i.e., 87% for the system with high false and missed alarm rates). In summary, the proposed resilience measure enables a system design with a lower false and missed alarm rates than is possible through use of the existing measure. The proposed measure thus allows the system design to satisfy a target resilience level (i.e., 97% in Table 3-2 (b)).

3.2.2 Electro-Hydrostatic Actuator (EHA)

An electro-hydrostatic actuator (EHA) is a device that controls the position or velocity of a cylinder rod. Its compact size, high energy efficiency, and redundant design possibility facilitates wide applications, including aircraft, excavators, robotics, active dampers, and automobiles [96]. For EHA simulation, a multi-domain system modeling and simulation platform (LMS Imagine.Lab AMESim) was employed in this study [97]. The schematic diagram of an EHA simulation model is shown in Figure 3-3. Its main components are a controller, a servomotor (SM), a bi-directional pump (PMP), an accumulator (ACC), check valves (CHK), relief valves (RLF), and a hydraulic cylinder (CYL). For cylinder rod position control feedback and system monitoring, four sensors were implemented: a servomotor temperature sensor (T), a servomotor rotary speed sensor (R), a pressure sensor (P), and a cylinder rod displacement sensor (D). In order to control the piston position as requested, the controller generated electrical signals to the servomotor considering the feedback signals of rotary speed and rod displacement. Then, the servomotor produced rotational motion, and the connected pump imposed fluid movement. Depending on the direction of the fluid movement, the rod in the cylinder moved inward or outward. For system safety, the check valves and the accumulator were able to prevent cavitation, and the relief valves relieved limit-over pressure.

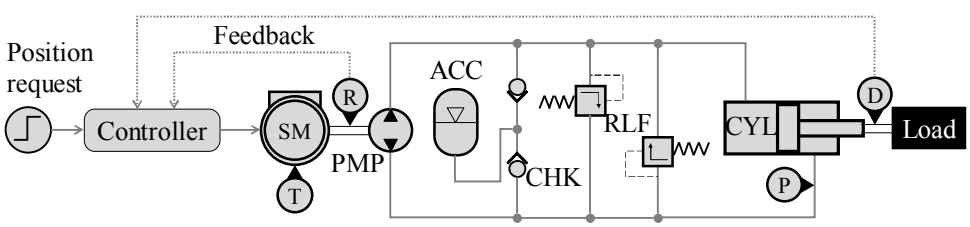


Figure 3-3 Schematic diagram of an electro-hydrostatic actuator (EHA)

simulation model

Two failure modes were considered in this study: cylinder cross-line leakage and servomotor lubricant deterioration. The actuator cross-line leakage was mainly caused by wear of a piston seal and/or a ring, and resulted in response delay and actuator force reduction [98]. The servomotor lubricant deterioration was due to contamination (particle, water), oxidation, and harsh operating conditions (temperature, pressure); it degraded performance of friction reduction, wear prevention, component cooling, and corrosion protection [79]. In the EHA model, two health-related parameters, the leakage coefficient of the cylinder and the viscous friction coefficient of the servomotor, were used to simulate the two failures, respectively. The parameter values of a faulty system were assumed to be five times those of a healthy system. This study considers three noise parameters (cylinder viscous friction coefficient, external loading torque, and servomotor temperature), which are relevant to system response. A total of five parameters were assumed to follow a normal distribution; their statistics are tabulated in Table 3-3.

Table 3-3 Statistics of EHA simulation model parameters

Category	**Component**	**Parameter**	**Unit**	**Mean**	**CoV***
Health-related (healthy)	Cylinder	Leakage coeff.	mL/min/bar	1.2	10%
	Servomotor	Viscous fric. coeff.	Nm/(rev/min)	1E–4	10%
Noise-	Cylinder	Viscous fric. coeff.	N/(m/s)	5000	5%

related	Load	Loading @ 2 sec	Nm	2000	30%
	Servomotor	Temperature	℃	25	50%

*CoV: coefficient of variation

Figure 3-4 shows the example of sensory signals from the rod displacement sensor (D) and the rotary speed sensor (R). The EHA model was requested to control the rod displacement to be 1 cm at 0.5 sec, and loading torque disturbance by the external load occurred at 2.0 sec. In this figure, the parameters' uncertainty is not considered, and the plot lines of the system responses do not disperse. Based on the health states, the system behaved in different ways, and correspondingly the health features for health state estimation were different. For example, servomotor (SM) lubricant failure does not affect the displacement signal (Figure 3-4 (a)), which cannot detect the SM failure. However, the rotary speed signal after the position request at 0.5 sec (Figure 3-4 (b)) is affected by SM failure; thus, it is appropriate for SM failure detection. This is because the servomotor, which operates at rated power to increase the cylinder pressure, has a low angular speed due to the excessive friction force resulting from the lubricant failure. Through the analysis of the sensory signals, five health features were defined from four sensors, as listed in Table 3-4. The rotary speed sensor (R) has two health features; the others have one health feature.

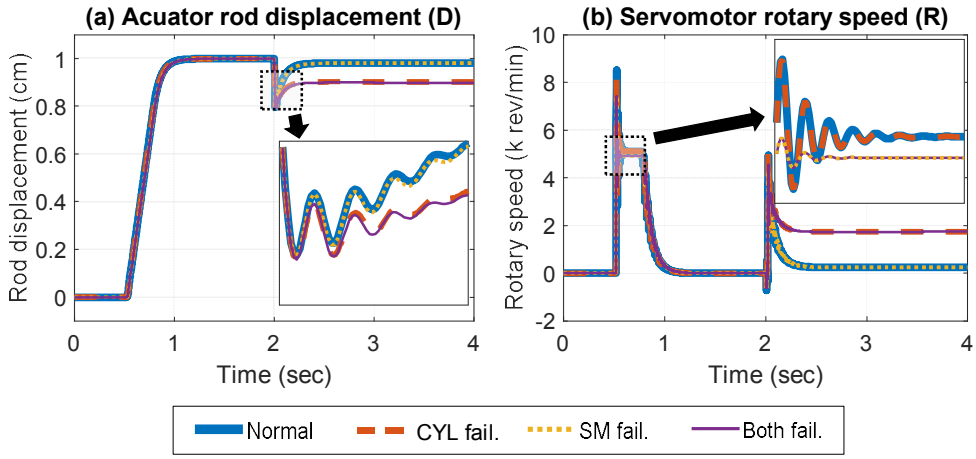


Figure 3-4 Sensory signals of EHA in four health states

Table 3-4 Extracted health features for EHA health state estimation

#	Sensor	System State	Health Feature
1	Rotary speed (R)	Position request (0.5 sec)	Max. peak-to-peak
2		After disturbance (2.0 sec)	Converged value
3	Rod displacement (D)	After disturbance (2.0 sec)	Converged value
4	Pressure (P)	After disturbance (2.0 sec)	Max. peak-to-peak
5	Motor temperature (T)	Whole	Mean value

In order to train the PHM model and test its performance (PHM efficiency), 400 sensory signal datasets were generated respectively (totally 400+400=800 datasets). The datasets include four health states (normal, cylinder failure, servomotor failure, and failure of both) evenly represented, i.e. 100 samples for each health state. They were simulated with randomly generated model input parameters following the statistics in Table 3-3. In order to reduce the EHA simulation time, the multi-dimensional spline interpolation method with a five-level full factorial design of experiment (DOE) was used. To represent

measurement noise, white Gaussian noise was added to the generated sensory signals. The health features in Table 3-4 were extracted and plotted in Figure 3-5. Each health feature was affected by different failure modes and had a different correlation with other health features. Therefore, the selection or combination of them was significant in the health state classification. For example, health features #1 and #2 from the R sensor can classify the servomotor and the cylinder failure modes, respectively. Thus, their combination would classify four data groups (Figure 3-5 (a)). Whereas, health features #4 and #5 were not affected by the failure modes and thus those four data groups were not distinguishable at all (Figure 3-5 (b)). They were affected by uncertainty factors of the cylinder viscous friction coefficient, the external disturbance loading, and the servomotor temperature in Table 3-3. Hence, these two features were able to help analyze the change of other health features from the two uncertainty factors, and indirectly increased data classification accuracy. In Figure 3-5 (c), for example, the sole health feature #4 cannot classify the data groups directly, but it can perfectly classify group 1 (normal) and group 2 (cylinder failure) if used with health feature #2. Likewise, health feature #5 in Figure 3-5 (d) can analyze the uncertainty of health feature #1, servomotor temperature. This increased the discrepancy between group 1 (normal) and group 3 (servomotor failure). Health features #2 and #3 are highly correlated (Pearson correlation coefficient $\rho_{\text{Pearson}}=-0.9910$), and interchangeable with each other (Figure 3-5 (e)).

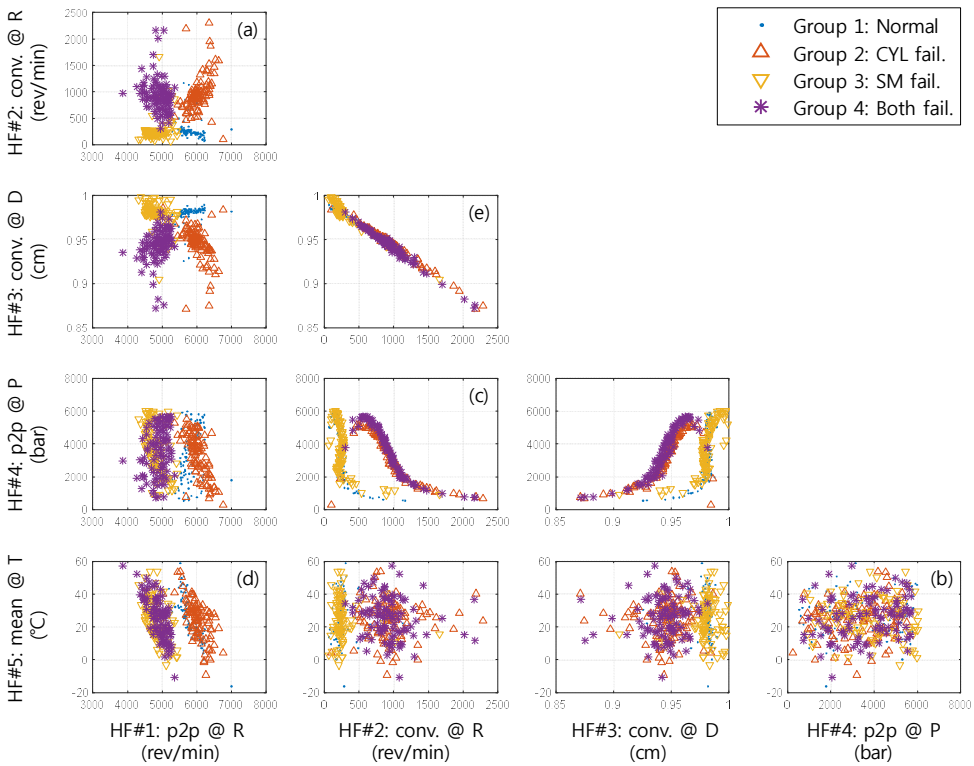


Figure 3-5 Health features of randomly generated datasets

For health state estimation, a linear discriminant analysis (LDA) classifier was employed; this is a widely used supervised classifier and appropriate for low-dimensional data with low nonlinearity. It explicitly models a linear boundary between multiclass data by maximizing their separation [99]. Table 3-5 shows the health estimation matrix of a multi-health state using the trained LDA classifier when all sensors and health features were employed. This matrix was converted into the health estimation matrix of a bi-health state, as shown in Table 3-6. The corresponding false and missed alarm rates were 5.0% and 6.3%, as determined from Eqs. (2.19) and (2.20).

Table 3-5 EHA health estimation matrix of multi-health state

Health Estimation Matrix			Estimated HS			
			Healthy	Faulty		
				CYL	SM	Both
True HS	Healthy		95	1	4	0
	Faulty	CYL	14	86	0	0
		SM	5	2	90	3
		Both	0	0	2	98

Table 3-6 EHA health estimation matrix of bi-health state

Health Estimation Matrix		Estimated HS	
		Healthy	Faulty
True HS	Healthy	95	5
	Faulty	19	281

Because the false alarm rates were calculated using the training and testing datasets, which were randomly generated, they also have uncertainty. Figure 3-6 shows their uncertainty as an error bar of one standard deviation for the different number of sensors (N_s). The false alarm rates were significantly reduced when the R sensor was employed. The R sensor has two health features that are sensitive to both failures. The false alarm rates were not further decreased from $N_s = 3$; thus, three sensors (R, P, and T) were chosen based on these findings. The corresponding false and missed alarm rates have means of $E(FA) = 3.75\%$ and $E(MA) = 1.37\%$; standard deviations were $\sigma(FA) = 2.50\%$ and

$\sigma(MA) = 1.29\%$.

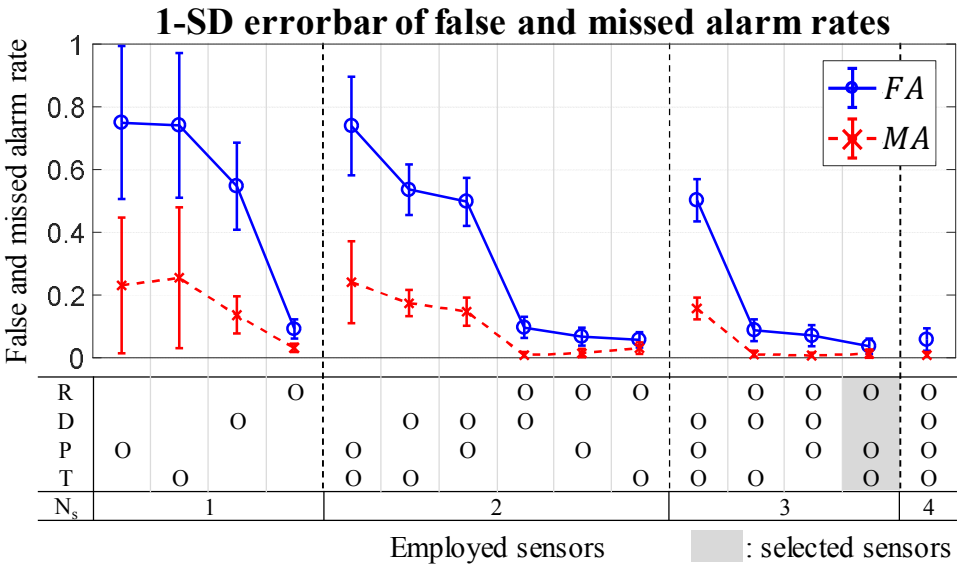


Figure 3-6 Evaluated EHA false alarm rates with different sensors

Lastly, the resilience measures of the EHA can be calculated using the estimated false alarm rates. Their mean values are from Eqs. (2.4) and (3.1) and their standard deviations are from Eqs. (3.3) and (3.4) (below) using the formula $\sigma(aX + bY) = \sqrt{a^2\sigma_X^2 + b^2\sigma_Y^2 + 2a^2b^2 \cdot \mathrm{cov}(X,Y)}$. Here, X and Y are random variables, a and b are coefficients, $\sigma_X = \sigma(X)$ is the standard deviation of X, and $\mathrm{cov}(X,Y)$ is a covariance between X and Y. The covariance between two false alarm rates is arbitrary and dependent on the design of the PHM solution.

$$\sigma(\Psi) = \kappa \cdot \sigma(MA) \cdot (1 - R) \tag{3.3}$$

$$\sigma(\Psi_{\mathrm{FA}}) = \sqrt{\begin{matrix}[\sigma(FA)\cdot R]^2 + [\kappa\cdot\sigma(\mathrm{MA})\cdot(1-R)]^2 \\ +2\cdot\kappa^2\cdot R^2\cdot(1-R)^2\cdot\mathrm{cov}(FA,MA)\end{matrix}} \tag{3.4}$$

Figure 3-7 shows the one standard deviation error bar of calculated resilience measures in terms of EHA reliability. The existing measure overestimates the EHA resilience, estimating it to be greater than the actual (Ψ_{FA}), by omitting false alarms. The mean of the proposed measure decreases as EHA reliability increases because FA is larger than MA; these are the weight of $(1-R)$ and R, respectively. As discussed in Chapter 3.1, this does not imply that the reliability should be minimized to increase the resilience and reduce the unnecessary maintenance action rate $FA\cdot R$ because that would also increase the system failure rate, $MA\cdot(1-R)$ (see Figure 3-2). With regard to the resilience measures' uncertainty (standard deviation), the difference between the two measures is significant, especially for high reliability systems. This difference is primarily due to the term $\sigma(FA)\cdot R$. As a result, the existing measure, which does not consider false alarms, incorrectly evaluates the resilience in terms of the standard deviation as well as the mean.

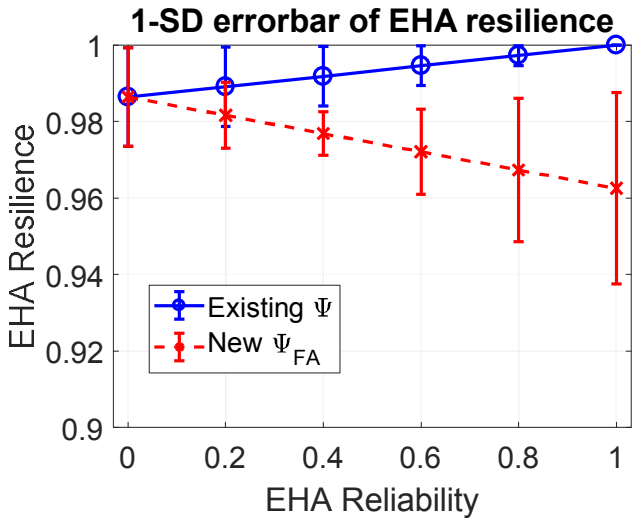


Figure 3-7 EHA resilience, as evaluated by two resilience measures

3.3 Summary and Discussion

An engineering resilience measure is a novel and innovative measure that describes the ability of an engineered system to maintain its functionality by resisting and recovering against adverse events. This measure cohesively integrates two widely used health-related measures: reliability, which focuses on resisting adverse events, and PHM efficiency, which focuses on recovering from adverse events. Compared to design approaches which consider these two conventional measures separately, resilience-driven system design enables engineering design that prevents over-designed and/or fault-prone systems and assures system availability while minimizing life-cycle cost.

This chapter proposed a new formulation of the resilience measure that, for the first time, considers false alarms. A false alarm as well as a missed alarm are one of challenging issues in PHM; these occur when PHM falsely evaluates the

health state of the engineered system, i.e., describing a truly healthy system as faulty or vice-versa. Because any false and missed alarm can critically reduce system availability, the degree of system resilience should be evaluated with consideration of two alarms. The conventional resilience measure does not consider false alarms; this makes it problematic to estimate the true degree of resilience of a system. The existing measure Ψ evaluates the system resilience level non-conservatively, whereas the proposed measure Ψ_{FA} evaluates correctly. In summary, the proposed resilience measure enables a system design with a lower false alarm rate than is possible through use of the existing measure. The proposed resilience measure thus enables a system design to satisfy a target resilience level.

In order to formulate the new resilience measure, false alarms were discussed in terms causes, effects and probabilistic formulations. Based upon analysis of the resilience scenarios, a new formulation of the resilience measure is proposed in this chapter that allows false alarms to be considered. Compared to the conventional resilience measure, the newly proposed one can more accurately estimate system resilience. In addition, the new measure facilitates resilience analysis of on-site operating systems while still being applicable to the design of new resilient systems with minimized life-cycle cost. The significance of false alarms in resilience, and the differences between the conventional and new resilience measures were demonstrated via numerical and electro-hydrostatic actuator (EHA) case studies.

Chapter 4. Resilience-Driven System Design Considering False Alarms (RDSD-FA)

Resilience-Driven System Design (RDSD) optimizes the designs of an engineered system and a PHM unit to satisfy target resilience level, and thus the resulted design is highly dependent on the estimation of resilience. If the resilience estimation is inaccurate, the design would not satisfy the intended resilience level, resulting low system availability with high life-cycle cost. In RDSD by Youn et al [11], the resilience estimation is not accurate due to inconsideration of false alarms. This chapter proposed the revised RDSD framework based upon the newly proposed resilience measure considering false alarms in Chapter 3. The key idea is to incorporate false alarms as well as missed alarms within RDSD cohesively. The detail of RDSD considering false alarms, RDSD-FA, is presented, and then the case study comparing RDSD-FA with RDSD will be followed.

4.1 Overview of RDSD-FA Framework

The overall framework of RDSD-FA is based upon that of RDSD reviewed in Chapter 2.1.2. It consists of three hierarchical steps: resilience allocation problem (RAP), reliability-based design optimization (RBDO), and prognostics and health management (PHM) design. The key difference between two frameworks is the allocation of a false alarm rate to PHM design problem. In the conventional RDSD framework shown in Figure 2-4, it considers PHM efficiency and allocates its target value to PHM design problem. PHM efficiency is the probability of estimating that a faulty system is faulty, which corresponds to

missed alarm rate. Thus, false alarm rate is not considered in RDSD. As discussed in Chapter 2.2 and Chapter 3, a false alarm results in unnecessary maintenance cost and decreases system resilience, it should be considered for designing a resilient engineered system. In order to handle this issue, RDSD-FA considers both false and missed alarm rates instead of PHM efficiency as shown in Figure 4-1. This helps to design PHM unit more specifically to minimize life-cycle cost (LCC) and realize system resilience as intended. The details of revised RDSD-FA are described below.

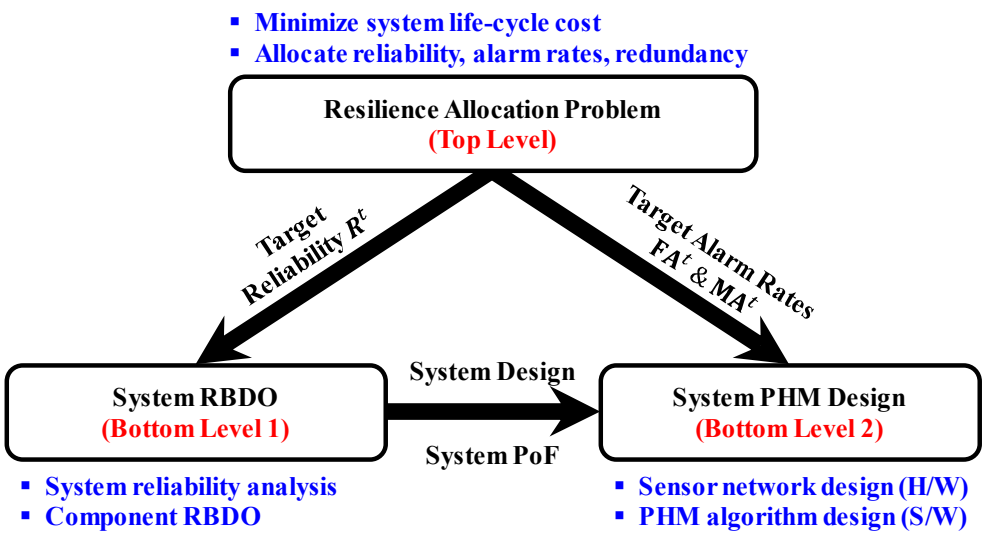


Figure 4-1 Hierarchical resilience-driven system design framework considering false alarms

4.2 Resilience Allocation Problem Considering False Alarms

Resilience allocation problem (RAP) allocates target reliability, target false and missed alarm rates, and redundancy levels to satisfy target resilience level while

minimizing life-cycle cost. In order to incorporate false alarm, the formulations of optimization problem are refined as below.

$$\begin{aligned} &\text{minimize}_{\mathbf{r}^t,\mathbf{FA}_I^t,\mathbf{FA}_{II}^t,\mathbf{m}} \quad LCC_{\mathrm{FA}}(\mathbf{r}^t,\mathbf{FA}^t,\mathbf{MA}^t,\mathbf{m}) \\ &\text{subject to} \quad \Psi_{\mathrm{FA}}^{\mathrm{SYS}}(\mathbf{r}^t,\mathbf{FA}^t,\mathbf{MA}^t,\mathbf{m}) \geq \Psi^t \\ &\qquad\qquad \mathbf{0} \leq \mathbf{r}^t,\mathbf{FA}^t,\mathbf{MA}^t \leq \mathbf{1} \\ &\qquad\qquad 1 \leq m_j \leq m_j^U \ (j = 1,\dots,N) \end{aligned} \tag{4.1}$$

where $\mathbf{FA}^t$ and $\mathbf{MA}^t$ are the vector of target false and missed alarm rates for N subsystems. As false and missed alarm rates are quantified as probabilities, they are bounded between zero and one as target reliability. Based upon the resilience measure considering false alarms in Chapter 3.1, the resilience of a series-parallel system $\Psi_{\mathrm{FA}}^{\mathrm{SYS}}$ can be calculated as below.

$$\Psi_{\mathrm{FA}}^{\mathrm{SYS}}(\mathbf{r}^t,\mathbf{FA}^t,\mathbf{MA}^t,\mathbf{m}) = \prod_{j=1}^{N} \psi_{\mathrm{FA},j}\left(r_j^t, FA_j^t, MA_j^t, m_j\right) \tag{4.2}$$

$$\psi_{\mathrm{FA},j} = 1 - \left[FA_j^t \cdot r_j^t + MA_j^t \cdot \left(1 - r_j^t\right)\right]^{m_j} \tag{4.3}$$

where $\psi_{\mathrm{FA},j}$ is the resilience measure of j-th subsystem considering false alarms; FA_j^t and MA_j^t are target false and missed alarm rates for j-th subsystem respectively. The Eq. (4.3) is based upon the same assumption in Chapter 2.1.2.2 that the probability of successful mitigation and recovery κ is one, and the reliability and PHM efficiency of components in each subsystem are identical.

The life-cycle cost of RDSD-FA, LCC_{FA}, is defined as a sum of initial development cost ($C_{\mathrm{FA}}^{\mathrm{I}}$), PHM development cost ($C_{\mathrm{FA}}^{\mathrm{PHM}}$), and unnecessary, predictive and corrective maintenance costs ($C_{\mathrm{FA}}^{\mathrm{UM}}$, $C_{\mathrm{FA}}^{\mathrm{PM}}$ and $C_{\mathrm{FA}}^{\mathrm{CM}}$) considering

false alarms. They are based upon the costs in Chapter 2.1.2.2, and the costs related with false alarm rates ($C_{\mathrm{FA}}^{\mathrm{PHM}}$, $C_{\mathrm{FA}}^{\mathrm{UM}}$, $C_{\mathrm{FA}}^{\mathrm{PM}}$ and C_{FA}^{CM}) are refined as below.

$$LCC_{\mathrm{FA}} = C_{\mathrm{FA}}^{\mathrm{I}} + C_{\mathrm{FA}}^{\mathrm{PHM}} + C_{\mathrm{FA}}^{\mathrm{M}} \tag{4.4}$$

$$C_{\mathrm{FA}}^{\mathrm{I}} = C^{\mathrm{I}} = \sum_{j=1}^{N} \alpha_j^{\mathrm{I}} \cdot \left(-\frac{T}{\ln\left(r_j^t\right)}\right)^{\beta_j^{\mathrm{I}}} \cdot \left[m_j + \exp\left(\frac{m_j}{4}\right)\right] \tag{4.5}$$

$$C_{\mathrm{FA}}^{\mathrm{PHM}} = \sum_{j=1}^{N} \alpha_j^{\mathrm{PHM}} \cdot \left(-\frac{T}{\ln\left(1-(FA_j^t + MA_j^t)/2\right)}\right)^{\beta_j^{\mathrm{PHM}}} \cdot m_j \tag{4.6}$$

$$C_{\mathrm{FA}}^{\mathrm{M}} = C_{\mathrm{FA}}^{\mathrm{UM}} + C_{\mathrm{FA}}^{\mathrm{PM}} + C_{\mathrm{FA}}^{\mathrm{CM}} \tag{4.7}$$

$$C_{\mathrm{FA}}^{\mathrm{UM}} = \sum_{j=1}^{N} m_j \cdot FA_j^t \cdot r_j^t \cdot c_j^{\mathrm{UM}} \tag{4.8}$$

$$C_{\mathrm{FA}}^{\mathrm{PM}} = \sum_{j=1}^{N} m_j \cdot \left(1 - MA_j^t\right) \cdot \left(1 - r_j^t\right) \cdot c_j^{\mathrm{PM}} \tag{4.9}$$

$$C_{\mathrm{FA}}^{\mathrm{CM}} = \sum_{j=1}^{N} m_j \cdot MA_j^t \cdot \left(1 - r_j^t\right) \cdot c_j^{\mathrm{CM}} \tag{4.10}$$

where c_j^{UM} denotes the unnecessary maintenance cost of each component in the j-th subsystem; $C_{\mathrm{FA}}^{\mathrm{M}}$ is the total maintenance cost including $C_{\mathrm{FA}}^{\mathrm{UM}}$, $C_{\mathrm{FA}}^{\mathrm{PM}}$, and $C_{\mathrm{FA}}^{\mathrm{CM}}$. $C_{\mathrm{FA}}^{\mathrm{PHM}}$ is refined to be function of two false alarm rates instead of PHM efficiency based upon the Eq. (2.10). The newly added cost term, unnecessary maintenance cost $C_{\mathrm{FA}}^{\mathrm{UM}}$, is incurred when PHM unit estimates a healthy engineered system to be faulty (i.e., false alarms). Its probability is $FA_j^t \cdot r_j^t$, and it includes the costs of system shutdown, inspection, and repair or replacement cost in case of incorrect inspection. $C_{\mathrm{FA}}^{\mathrm{PM}}$ and $C_{\mathrm{FA}}^{\mathrm{CM}}$ are refined to be a function

of missed alarm rate MA_j^t instead of PHM efficiency Λ.

Figure 4-2 shows the example of resilience allocation result by RDSD-FA. The 1st subsystem is without PHM and thus a healthy component is always available without false alarm problems (i.e., $FA = 0\%$), and a faulty system leads to system failure without failure prevention (i.e., $MA = 100\%$). The resulted resilience considering false alarms $\Psi_{\mathrm{FA}}^{\mathrm{SYS}}$ is 98.71% according to Eq. (4.2).

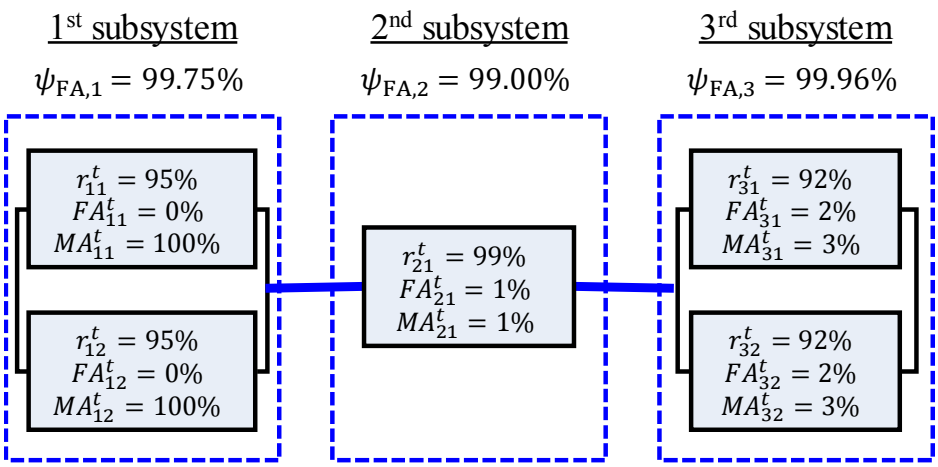


Figure 4-2 Example of resilience allocation result for a series-parallel system considering false alarms

The solutions of resilience problem in Eq. (4.1), target reliability, target false alarm rate, and target missed alarm rate, are transferred to RBDO problem and PHM design problem respectively as shown in Figure 4-1. Regarding RBDO problem which is not related with false alarms and thus not refined, please refer Chapter 2.1.2.3. The PHM design considering false alarms is presented below.

4.3 Prognostics and Health Management (PHM) Design Considering False Alarms

This chapter refines the PHM design framework in Chapter 2.1.2.4 considering false alarms. In order to incorporate false alarms, the PHM design problem for *j*-th subsystem component is formulated as below.

$$\begin{aligned} &\text{minimize}_{\mathbf{d}_j^{PHM}} \; C_j^{\mathrm{PHM}}(\mathbf{d}_j^{\mathrm{PHM}}) + C_j^{\mathrm{M}}(\mathbf{d}_j^{\mathrm{PHM}}) \\ &\text{subject to } FA_j(\mathbf{d}_j^{\mathrm{PHM}}) \le FA_j^t \\ &\qquad MA_j(\mathbf{d}_j^{\mathrm{PHM}}) \le MA_j^t \\ &\qquad \mathbf{d}_j^{\mathrm{PHM,L}} \le \mathbf{d}_j^{\mathrm{PHM}} \le \mathbf{d}_j^{\mathrm{PHM,U}} \end{aligned} \tag{4.11}$$

where C_j^{PHM} is PHM development cost for *j*-th subsystem component; C_j^{M} is the total maintenance cost of *j*-th subsystem; FA_j and MA_j are false and missed alarm rates of *j*-th subsystem component respectively. The new cost term C_j^{M} includes unnecessary, corrective, and predictive maintenance costs. As PHM design is related with not only C_j^{PHM} but also C_j^{M}, and the introduction of C_j^{M} makes the PHM design more rigorous. Thus, this results in better PHM design compared to the previous one in Chapter 2.1.2.4 which does not consider C_j^{M}. C_j^{M} is formulated as below.

$$C_j^{\mathrm{M}} = C_j^{\mathrm{UM}}(\mathbf{d}_j^{\mathrm{PHM}}) + C_j^{\mathrm{PM}}(\mathbf{d}_j^{\mathrm{PHM}}) + C_j^{\mathrm{CM}}(\mathbf{d}_j^{\mathrm{PHM}}) \tag{4.12}$$

$$C_j^{\mathrm{UM}}(\mathbf{d}_j^{\mathrm{PHM}}) = m_j \cdot FA_j(\mathbf{d}_j^{\mathrm{PHM}}) \cdot r_j \cdot c_j^{\mathrm{UM}} \tag{4.13}$$

$$C_j^{\mathrm{PM}}(\mathbf{d}_j^{\mathrm{PHM}}) = m_j \cdot \left(1 - MA_j(\mathbf{d}_j^{\mathrm{PHM}})\right) \cdot (1 - r_j) \cdot c_j^{\mathrm{PM}} \tag{4.14}$$

$$C_j^{\mathrm{CM}}\left(\mathbf{d}_j^{\mathrm{PHM}}\right) = m_j \cdot MA_j\left(\mathbf{d}_j^{\mathrm{PHM}}\right) \cdot \left(1 - r_j\right) \cdot c_j^{\mathrm{CM}} \tag{4.15}$$

where C_j^{UM}, C_j^{PM}, and C_j^{CM} are unnecessary, predictive, and corrective maintenance costs of j-th subsystem; r_j is the resulted reliability of j-th subsystem component through RBDO in Chapter 2.1.2.3. The resulted r_j, FA_j, and MA_j can differ from their target values (i.e., r_j^t, FA_j^t, and MA_j^t). Thus, the resulted total maintenance cost C_j^{M} also can differ from the expected total maintenance cost $C_{\mathrm{FA}}^{\mathrm{M}}$ in the resilience allocation problem.

4.4 Case study: Electro-Hydrostatic Actuator (EHA)

In this case study, an electro-hydrostatic actuator (EHA) introduced in 3.2.2 was employed to demonstrate the proposed RDSD-FA. Its high energy efficiency and compactness have led to the wide use of EHA in many applications such as aircraft, excavators, robotics, active dampers, and automobiles. As the failure of EHA can result in catastrophic consequences, high redundancy level is introduced to satisfy high reliability with high life-cycle cost (e.g., a triplex redundant flight control system) [100]. In order to reduce the life-cycle cost while satisfying the required resilience level, RDSD-FA framework can be applied. The design results of RDSD-FA is compared with that of RDSD. The details are shown below.

4.4.1 Step 1: Resilience Allocation Considering False Alarms

As shown in Figure 4-3, EHA mainly consists of four subsystems: electro-controller (EC), servomotor (SM), hydraulic pump (PMP), and hydraulic cylinder (CYL). This step allocated target reliability, redundancy, target false alarm rate, and target missed alarm rate to four subsystems so as to minimize life-cycle cost

while satisfying target resilience level. The corresponding optimization problem is given as Eq. (4.16).

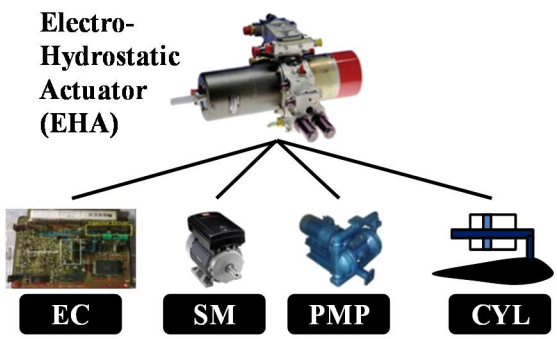


Figure 4-3 Electro-hydrostatic actuator system and its subsystems

$$
\begin{aligned}
&\text{find} && r_j^t, m_j, FA_j^t, MA_j^t \text{ for } j = 1, \dots, 4 \\
&\text{minimize} && LCC_{\mathrm{FA}} = C_{\mathrm{FA}}^{\mathrm{I}} + C_{\mathrm{FA}}^{\mathrm{PHM}} + C_{\mathrm{FA}}^{\mathrm{UM}} + C_{\mathrm{FA}}^{\mathrm{PM}} + C_{\mathrm{FA}}^{\mathrm{CM}} \\
&\text{subject to} && \Psi_{\mathrm{FA}}^{\mathrm{SYS}} = \prod_{j=1}^{4} \psi_{\mathrm{FA},j} \geq \Psi^t = 0.9500 \\
& && 0 \leq r_j^t, FA_j^t, MA_j^t \leq 1 \\
& && 1 \leq m_j \leq 5
\end{aligned}
\tag{4.16}
$$

In this study, the upper boundary of redundancy was set to five, and target resilience level was set to 95% ($\Psi^t = 0.95$). The parameters regarding LCC_{FA} are listed in Table 4-1. In order to solve this problem, a genetic algorithm (GA) was used which can handle both discrete design variables (i.e., redundancy) as well as continuous design variables (i.e., target reliability and target false and missed alarm rates). Table 4-2 shows the optimization results according to PHM implementation. Comparing two design results, PHM implementation resulted in 50.46% decrease of LCC_{FA} by reducing subsystem reliability r_j^t and

redundancy levels m_j as well as reducing missed rate MA_j^t to prevent system failures.

Table 4-1 Parameters of life-cycle cost model for resilience allocation problem

Cost	Para.	Subsystem			
		EC	SM	PMP	CYL
$C_{\mathrm{FA}}^{\mathrm{I}}$	α_j^C	5.0e-5	0.8e-5	1.0e-5	0.7e-5
	β_j^C	1.3			
	T	1000			
$C_{\mathrm{FA}}^{\mathrm{PHM}}$	α_j^{PHM}	3.3E-06	5.3E-06	6.7E-06	4.7E-06
	β_j^{PHM}	1.15			
$C_{\mathrm{FA}}^{\mathrm{M}}$	c_j^{UM}	0.5	0.8	1.2	1.5
	c_j^{PM}	1.5	2.4	3.6	4.5
	c_j^{CM}	5	8	12	15

Table 4-2 Resilience allocation results according to PHM implementation

Design variable		Subsystem				Cost	
		EC	SM	PMP	CYL		
w/o PHM	r_j^t	0.8916	0.8763	0.8786	0.9004	$C_{\mathrm{FA}}^{\mathrm{I}}$	13.5792
	m_j	2	2	2	2	$C_{\mathrm{FA}}^{\mathrm{PHM}}$	0
	FA_j^t	0.0000	0.0000	0.0000	0.0000	$C_{\mathrm{FA}}^{\mathrm{M}}$	8.9651
	MA_j^t	1.0000	1.0000	1.0000	1.0000	$\boldsymbol{LCC_{\mathrm{FA}}}$	**22.5443**
	$\psi_{\mathrm{FA},j}^t$	0.9882	0.9847	0.9853	0.9901		
w/ PHM	r_j^t	0.7588	0.7636	0.7263	0.8166	$C_{\mathrm{FA}}^{\mathrm{I}}$	3.8559
	m_j	2	2	1	1	$C_{\mathrm{FA}}^{\mathrm{PHM}}$	2.9378

	FA_j^t	0.0353	0.0698	0.0117	0.0123	$C_{\mathrm{FA}}^{\mathrm{M}}$	4.3746
	MA_j^t	0.1317	0.0482	0.0355	0.0705	$\boldsymbol{LCC_{\mathrm{FA}}}$	**11.1683**
	$\psi_{\mathrm{FA},j}^t$	0.9966	0.9958	0.9818	0.9770		

After solving this top-level problem, two bottom-level problems, i.e., RBDO and PHM design, are sequentially conducted for four subsystems to satisfy the allocated performance levels in Table 4-2. Among four subsystems, the hydraulic cylinder was selected in this case study to demonstrate the proposed RDSD-FA framework. In order to explore the performance of different hydraulic cylinder and PHM designs, the EHA simulation model of LMS Imagine.Lab AMESim in Chapter 3.2.2 was used.

4.4.2 Step 2: Reliability-Based Design Optimization

The first bottom level-problem performed RBDO for the hydraulic cylinder to satisfy the allocated target reliability level from the top-level resilience allocation problem in Chapter 4.4.1. Specifically, this aimed to optimize two design variables, the mean of piston diameter μ_{d_p}, and the mean of cylinder rod diameter μ_{d_r} to satisfy the allocated target reliability of 0.8166 and minimize the cylinder volume regarded as the initial development cost. For cylinder reliability, five performance constraints were considered shown in Figure 4-4 [11]. The EHA was requested to control the rod displacement to be 1cm at 0.5 sec, and disturbed by external loading at 2.0 sec. Under this operating condition, G_1 and G_2 are timeliness-relevant constrains, and G_3 and G_4 are robustness-relevant constrains. G_5 is to ensure the structural strength of the rod relative to the piston.

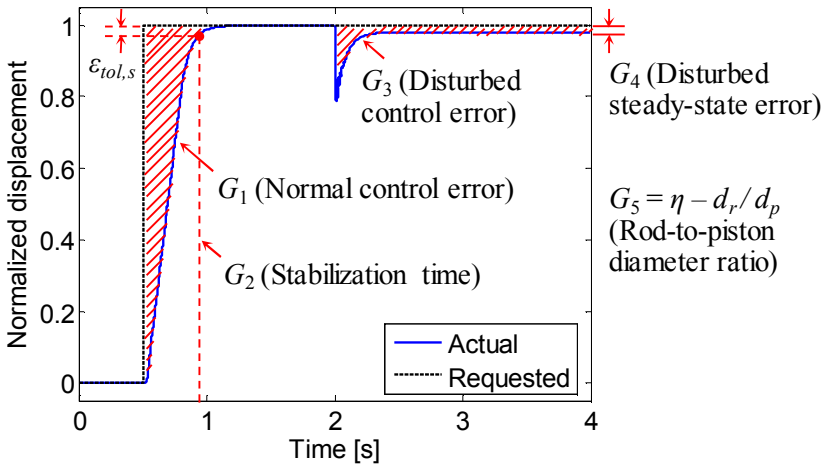


Figure 4-4 Five performance constraints of hydraulic cylinder

The RBDO problem corresponding to above description can be formulated as follow.

$$\begin{aligned}
&\underset{\mathbf{d}=(\mu_{d_p},\mu_{d_r})}{\text{minimize}} \quad C\left(\mu_{d_p},\mu_{d_r}\right) = \omega \cdot V_s\left(\mu_{d_p}\right) + (1-\omega)\cdot V_r(\mu_{d_r}) \\
&\text{where} \qquad \omega = 0.098,\ V_s = l_s \cdot \pi\left(\mu_{d_p}/2\right)^2, V_r = l_s \cdot \pi\left(\mu_{d_r}/2\right)^2 \\
&\text{subject to} \quad r = \Pr\left(\cap_{i=1}^{5} G_i(\mathbf{d}) \le 0\right) \ge r^t = 0.8166; \\
&\qquad\qquad \mathbf{d}^{\mathrm{L}} \le \mathbf{d} \le \mathbf{d}^{\mathrm{U}};\ \mathbf{d}^{\mathrm{L}} = (55.0\ 10.0);\ \mathbf{d}^{\mathrm{U}} = (75.0\ 30.0); \\
&\text{where} \qquad G_1 = \int_0^2 \left|Y(t) - Y_{req}(t)\right| dt - e_{nc} \qquad (4.17) \\
&\qquad\qquad G_2 = \underset{t\in[0.5,2]}{\operatorname{argmin}}\left\{\left|Y(t) - Y_{req}(t)\right| \le \varepsilon_{tol,s}\right\} - \tau_s \\
&\qquad\qquad G_3 = \int_2^4 \left|Y(t) - Y_{req}(t)\right| dt - e_{dc} \\
&\qquad\qquad G_4 = \min_{t\in[2,4]}\left\{\left|Y(t) - Y_{req}(t)\right|\right\} - e_{dss} \\
&\qquad\qquad G_5 = \eta - d_r/d_p
\end{aligned}$$

where ω is weight factor of stroke volume; V_s and V_l are the volume of stroke and rod respectively; l_s is stroke length; $\mathbf{d}^{\mathrm{L}}$ and $\mathbf{d}^{\mathrm{U}}$ are the lower and upper boundary of design variables $\mathbf{d} = \left(\mu_{d_p}, \mu_{d_r}\right)$ respectively; $Y(t)$ and $Y_{req}(t)$ are the actual and requested response at time t; e_{nc} is the critical normal control error; $\varepsilon_{tol,s}$ is the stabilization time criterion; τ_s is the critical stabilization time; e_{dc} is the critical disturbance control error; e_{dss} is the critical disturbed steady-state error; η is the critical rod-to-piston diameter ratio ($\eta = 1/3$); d_p and d_r are the diameters of piston and cylinder rod respectively. In EHA simulation, additional two random noise variables, the cylinder leakage coefficient β_{CYL} and the viscous friction coefficient ν_{CYL}, were considered. The parameter values and the information of random variables are listed in Table 4-3 and Table 4-4 respectively.

Table 4-3 RBDO problem parameters

Parameter	e_{nc}	$\varepsilon_{tol,s}$	τ_s	e_{dc}	e_{dss}	η
Unit	cm · sec	cm	sec	cm · sec	cm	-
Value	0.25	0.03	1.05	0.06	0.02	1/3

Table 4-4 RBDO problem random variables

Random variables		**Unit**	**Distribution**		
			Type	**Mean**	**Std. dev.***
Design -related	d_p	mm	Normal	μ_{d_p}	2.0
	d_r	mm	Normal	μ_{d_r}	1.0
Noise -related	l_s	mm	Normal	50.0	2.5
	β_{CYL}	L/min/Bar	Normal	1.2E-3	6.0E-5
	ν_{CYL}	N/(m/s)	Normal	5000	250

* Std. dev.: standard deviation

In order to solve RBDO problem of Eq. (4.17), interior point method and finite difference method with 0.1% perturbation level were used for optimization and sensitivity analysis of objective and constraint functions respectively. For the computational efficiency, the adaptive-sparse polynomial chaos expansion (PCE) method with univariate sampling method was employed [101]. Table 4-5 shows the initial and optimized design variables with their reliability and objective function. In the initial design, cylinder reliability was not satisfied due to the low reliability of G_3 and G_4. The optimization increased μ_{d_p}, which enlarged effective rod end area and cylinder volume. This resulted in reluctance against external disturbance, and thus the reliability of G_3 and G_4 were increased. The optimization increased μ_{d_r} as well to compensate the reliability loss of G_5 due to the increase of μ_{d_p}. As a result, the cylinder reliability was enhanced to satisfy the target reliability allocated from Chapter 4.4.1 ($r^t = 0.8166$) with 13.14% increased initial development cost. For the verification of the design result, Monte Carlo simulation (MCS) with 10,000 samples was used resulting hydraulic cylinder reliability 0.8110 with five probabilistic constraints of 0.9920, 0.9913, 0.9975, 0.8990, and 0.9197.

Table 4-5 Initial and optimal design of hydraulic cylinder

Design	μ_{d_p} (mm)	μ_{d_r} (mm)	$\Pr(G_i \leq 0)$					r	C
			G_1	G_2	G_3	G_4	G_5		
Initial	62.0000	22.0000	1.0000	1.0000	0.8220	0.2975	0.8639	0.1970	3.1981E4
Optimal	66.5695	23.8573	0.9936	0.9926	0.9975	0.9026	0.9158	0.8166	3.7257E4

4.4.3 Step 3: PHM Design Considering False Alarms

The second bottom-level problem designed a PHM unit for the hydraulic cylinder. Its objective it to optimizing PHM design variables to satisfy the target false and missed alarm rates while minimizing cylinder's PHM development cost and cylinder total maintenance cost. The target false and missed alarm rates were allocated from the resilience allocation problem in Chapter 4.4.1, and the cylinder's design was given from the RBDO in Chapter 4.4.2.

A PHM unit aims at preventing two failure modes: the lubricant deterioration of the servomotor and the cross-line leakage of the hydraulic cylinder. The former failure mode is possibly caused by contamination, oxidation, wear, and erosion, and the latter by piston seal wear. They were simulated by increasing a servomotor viscous friction coefficient and a cylinder leakage coefficient respectively. When those values exceeded five times initial healthy values, the hydraulic cylinder was defined to be failed.

In a rigorous manner, the failure modes in PHM design problem should be same with those in RBDO problem. This is because RDSD employs a PHM unit to detect and prevent failures that RBDO cannot resolve, so as to increase system resilience by $\kappa \cdot \Lambda_{\mathrm{FA}} \cdot (1 - R)$ as Eq. (3.1). However, the failure modes considered in RBDO are very easily diagnosed by a PHM unit, and thus not suitable to show various issues in PHM design problem. Therefore, this PHM design problem considers the lubricant deterioration and the cross-line leakage failure modes different from those considered in RBDO.

For the PHM design variable vector $\mathbf{d}^{\mathrm{PHM}}$, sensor selection vector $\mathbf{d}_{\mathrm{sensor}}^{\mathrm{PHM}}$, PHM algorithm selection vector $\mathbf{d}_{\mathrm{alg}}^{\mathrm{PHM}}$, and PHM algorithm parameter vector $\mathbf{d}_{\theta}^{\mathrm{PHM}}$ were considered. $\mathbf{d}_{\mathrm{sensor}}^{\mathrm{PHM}}$ and $\mathbf{d}_{\mathrm{alg}}^{\mathrm{PHM}}$ are logical vectors of which element I_k indicates whether the *k*-type sensor and the *k*-type PHM algorithm is used respectively. For the sensor selection, four sensors were considered as shown in Figure 3-3: a servomotor rotary speed sensor (R), a cylinder rod displacement sensor (D), a pressure sensor (P), and a servomotor temperature sensor (T). According to the sensor selection, the corresponding health features in Table 3-4 and Figure 3-5 were used for health assessment. For the PHM algorithm selection, three algorithms were considered: linear discriminant analysis (LDA) classifier [99, 102], support vector machine (SVM) with Gaussian kernel [99, 102], *k*-nearest neighbor (kNN) classifier with ten neighbors and Euclidean distance metric [99]. $\mathbf{d}_{\theta}^{\mathrm{PHM}}$ was defined to include the weights of false and missed alarms. False and missed alarm weights denote the significances of two false alarm rates, and a PHM model is trained differently according to their values. If false alarm weight increases, false alarm rate decreases and missed alarm rate may increase. This leads to the decrease of unnecessary maintenance cost from false alarms, and the increase of corrective maintenance cost from missed alarms. Thus, the optimization of false and missed alarm weights helps to decrease the total maintenance cost as well as life-cycle cost.

The PHM unit design problem corresponding to above descriptions can be formulated as below.

$$
\begin{aligned}
&\text{find} && \mathbf{d}^{\mathrm{PHM}} = \left\{\mathbf{d}_{\mathrm{sensor}}^{\mathrm{PHM}}, \mathbf{d}_{\mathrm{alg}}^{\mathrm{PHM}}, \mathbf{d}_{\theta}^{\mathrm{PHM}}\right\} \\
&\text{where} && \mathbf{d}_{\mathrm{sensor}}^{\mathrm{PHM}} = \{I_{\mathrm{R}}, I_{\mathrm{D}}, I_{\mathrm{P}}, I_{\mathrm{T}}\} \\
& && \mathbf{d}_{\mathrm{alg}}^{\mathrm{PHM}} = \{I_{\mathrm{LDA}}, I_{\mathrm{SVM}}, I_{\mathrm{kNN}}\} \\
& && \mathbf{d}_{\theta}^{\mathrm{PHM}} = \{w_{\mathrm{FA}}, w_{\mathrm{MA}}\} \\
&\text{minimize} && C^{\mathrm{PHM}}\left(\mathbf{d}_{\mathrm{sensor}}^{\mathrm{PHM}}\right) + C^{\mathrm{M}}\left(\mathbf{d}^{\mathrm{PHM}}\right) \\
&\text{where} && C^{\mathrm{PHM}} = c_{\mathrm{R}} \cdot I_{\mathrm{R}} + c_{\mathrm{D}} \cdot I_{\mathrm{D}} + c_{\mathrm{P}} \cdot I_{\mathrm{P}} + c_{\mathrm{T}} \cdot I_{\mathrm{T}} \\
& && c_{\mathrm{R}} = 0.7;\ c_{\mathrm{D}} = 0.5;\ c_{\mathrm{P}} = 0.4;\ c_{\mathrm{T}} = 0.2; \\
&\text{subject to} && FA\left(\mathbf{d}^{\mathrm{PHM}}\right) \le FA^{t} = 0.0123 \\
& && MA\left(\mathbf{d}^{\mathrm{PHM}}\right) \le MA^{t} = 0.0705 \\
& && 0 \le w_{\mathrm{FA}}, w_{\mathrm{MA}} \le 1
\end{aligned}
\tag{4.18}
$$

where I_k is an indicator function that is one if *k*-type sensor or algorithm is used or otherwise zero; w_{FA} and w_{MA} are the weights of false and missed alarm respectively; c_{R}, c_{D}, c_{P}, c_{T} are the costs of R, D, P, and T sensor respectively. The PHM development cost C^{PHM} was assumed to be the total cost of employed sensors. The total maintenance cost C^{M} was calculated using Eqs. (4.12)-(4.15) and the corresponding maintenance cost parameters in Table 4-1. False and missed alarm rates were evaluated using Eqs. (2.19)-(2.24). The information of random variables including additional three noise variables are tabulated in Table 4-6.

Table 4-6 Statistics of EHA simulation model parameters

Category	Component	Parameter	Unit	Mean	CoV*
Health-related (healthy)	Cylinder	Leakage coeff.	mL/min/bar	1.2	10%
	Servomotor	Viscous fric. coeff.	Nm/(rev/min)	1E–4	10%
Noise-related	Cylinder	Viscous fric. coeff.	N/(m/s)	5000	5%
	Load	Loading @ 2 sec	Nm	2000	20%

	Servomotor	Temperature	℃	25	50%

*CoV: coefficient of variation

In order to evaluate false and missed alarm rates according to different PHM designs, 400 sensory signal datasets were generated for training and testing of PHM model respectively (totally 400+400=800 datasets). The datasets include four health states (normal, cylinder failure, servomotor failure, and failure of both) evenly represented, i.e. 100 samples for each health state. Figure 4-5 shows the evaluated false and missed alarm rates according to different PHM algorithm selection $\mathbf{d}_{\text{alg}}^{\text{PHM}}$ and false alarm weights $\mathbf{d}_{\theta}^{\text{PHM}}$ when using only rod displacement sensor (D). There exists trade-off tendency between FA and MA according to the weights of false and missed alarms [103]. As false alarm weight w_{FA} increases or missed alarm weight w_{MA} decreases, false alarm rate FA decreases and missed alarm rate MA increases.

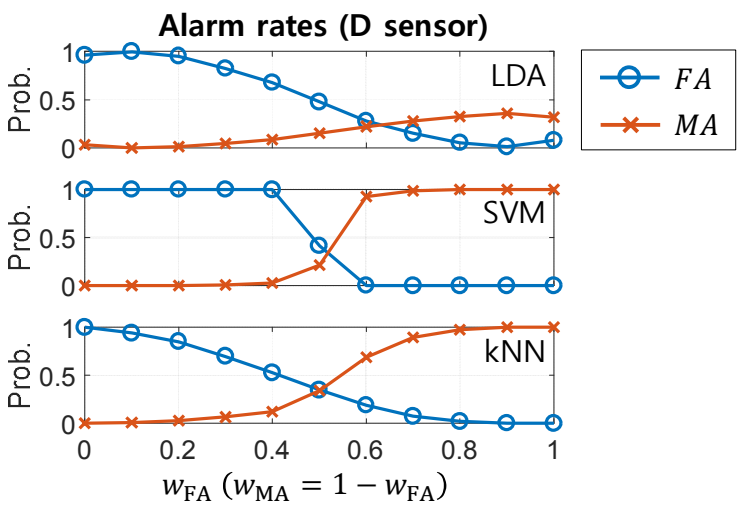


Figure 4-5 False and missed alarm rates with different weights and PHM algorithm

In order to solve the optimization problem of Eq. (4.18), a genetic algorithm

(GA) is used which can handle both discrete and continuous design variables. In order to find near-global minimum solution, the optimization was performed ten times repeatedly. Figure 4-6 shows the false and missed alarm rates of the optimized PHM designs with different PHM algorithms. Table 4-7 lists the details of the PHM designs. As false and missed alarm rates are variant because of the uncertainties in training and testing sample datasets, the evaluated false alarm rates are plotted with one standard deviation error bar. All three PHM designs satisfied the target false and missed alarm rates allocated from the top-level problem in Chapter 4.4.1 ($FA^t = 0.0123, MA^t = 0.0705$). They all use the rotary speed sensor (R) which has two health features classifying four health states (see Figure 3-5 (a)), and the pressure sensor (P) which can analyze the uncertainty of health features due to the noise random variables (see Figure 3-5 (c)). And they all have large w_{FA} over 0.8 to fulfill the constraint of the allocated target false alarm rate.

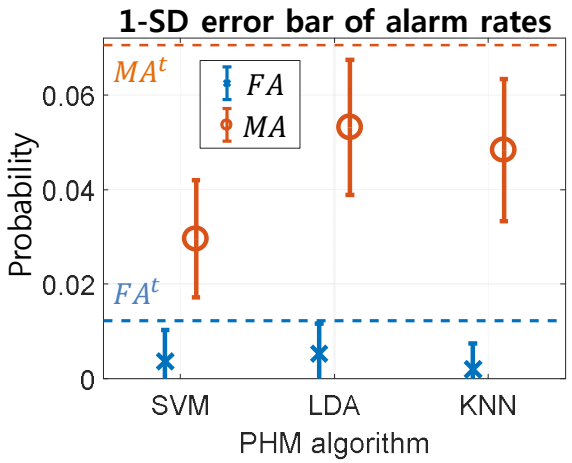


Figure 4-6 Error bar of false alarm and missed rates

Table 4-7 Optimal PHM designs of three PHM algorithm with their costs

#	$\mathbf{d}_{\text{sensor}}^{\text{PHM}}$				$\mathbf{d}_{\text{alg}}^{\text{PHM}}$			$\mathbf{d}_{\theta}^{\text{PHM}}$		Cost		
	I_{R}	I_{D}	I_{P}	I_{T}	I_{LDA}	I_{SVM}	I_{kNN}	w_{FA}	w_{MA}	C^{PHM}	C^{M}	$C^{\text{PHM}} + C^{\text{M}}$
1	1	0	1	0	1	0	0	0.9	0.1	1.1	0.9341	2.0341
2	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0.9**	**0.1**	1.1	0.8867	**1.9867**
3	1	0	1	1	0	0	1	0.8	0.2	1.3	0.9208	2.2208

Among three algorithms satisfying the allocated target false and missed alarm rates, the algorithm with the minimum sum of C^{PHM} and C^{M} was selected. For the calculation of C^{M} in Eqs. (4.12)-(4.15), the mean values of false and missed alarm rates were used. The selected algorithm was SVM, of which false and missed alarm rates were generally lower than those of the other algorithms. Its mean false and missed alarm rates are 0.0037 and 0.0296, resulting in the resilience of a hydraulic cylinder to be 0.9915 using Eq. (3.1). This is larger than the allocated resilience 0.9770 in Table 4-2.

4.4.4 Comparison of Design Results from RDSD and RDSD-FA

This chapter compares the design results from the RDSD by Youn et al. [11] and the proposed RDSD-FA. RDSD was performed through the framework described in Chapter 2.1.2, and the results are listed in Table 4-8 with those from RDSD-FA. In this table, PHM efficiency of RDSD is replaced with missed alarm rate of RDSD-FA ($MA \fallingdotseq 1 - \Lambda$) as discussed in Chapter 3.2.1.

In resilience allocation problem (RAP), the optimization problem formulations are different in terms of resilience measure, PHM development cost, and total maintenance cost as shown in Chapter 4.2. Thus, although target system resilience levels are equivalent as 95%, the allocated performance values are different. As the allocated target reliability R^t of RDSD is smaller than that of

RDSD-FA, initial development cost C^{I} of RDSD is smaller than that of RDSD-FA in RBDO. In PHM design, RDSD does not have the constraint on false alarm rate (see Eq. (2.14)), and thus has high false alarm rate FA resulting high unnecessary maintenance cost C^{UM}. RDSD-FA has high PHM development cost because it employed more sensors to satisfy the allocated target false and missed alarm rates. After the whole design, RDSD results in resilience of 0.8937 which does not satisfy the allocated target resilience Ψ^t of 0.9889. This is because RDSD does not consider false alarms in RAP, and allocates inadequate target performances. This dissatisfaction can cause unexpected system unavailability with social and capital loss. Whereas RDSD-FA, which considers false alarms, has the resilience Ψ_{FA} of 0.9915 satisfying the allocated target resilience Ψ^t of 0.9770. Through this comparison, it is demonstrated that false alarms have an important role in system resilience, and the proposed RDSD-FA can design an resilient engineered system successfully.

Table 4-8 Comparison of design results from RDSD and RDSD-FA

Hydraulic cylinder design		RDSD	RDSD-FA	Difference
RAP	R^t	0.7996	0.8166	2.13%
	m	1	1	0%
	FA^t	-	0.0123	-
	MA^t	0.0555	0.0705	27.03%
	Ψ^t	0.9889	0.9770	-1.20%
RBDO	C^{I}	3.6980E+4	3.7257E+4	0.75%
PHM Design	FA	0.1240	0.0037	-97.02%
	MA	0.0356	0.0296	-16.85%
	C^{PHM}	0.9	1.1	22.22%

C^{UM}	0.1487	0.0045	-96.97%
C^{PM}	0.8697	0.8009	-7.91%
C^{CM}	0.1069	0.0813	-23.95%
$C^{\mathrm{PHM}} + C^{\mathrm{M}}$	2.0253	1.9867	-1.91%
Ψ_{FA}	**0.8937**	**0.9915**	10.94%
$\Psi_{\mathrm{FA}} \geq \Psi^{t}$?	**No (-9.63%)**	**Yes (+1.48%)**	-

4.5 Summary and Discussion

Recent engineering systems are getting high capacity and exposed to harsh operating conditions in order to achieve superior performance. This makes engineering systems unreliable and risky, resulting in rapid performance degradation and abrupt system failure with substantial social expense. Up-to-date, many techniques have been developed to achieve the required reliability level of the system. Among them, the resilience-driven system design (RDSD) by Youn et al. [11] is the system design technique that minimizes life-cycle cost while satisfying target resilience level. This design framework cohesively incorporate two techniques in design stage and operation stage: reliability-based design optimization (RBDO) and prognostics and health management (PHM). Compared to conventional approaches implementing RBDO and PHM respectively, RDSD can design an engineered system to be resilient in a cost-effective manner by optimally allocating target performance levels to RBDO and PHM design problems. However, RDSD does not consider false alarms of PHM. This results in inaccurate resilience estimation and deficiency of performance allocation. The designed engineered system is prone to false alarms problems, and cannot maintain its required performance as a designer intended.

In order to handle to this issue, this chapter proposed RDSD considering false alarms (RDSD-FA). RDSD-FA includes three hierarchical tasks: resilience allocation problem (RAP), RBDO, and PHM design. In RAP, the engineering resilience measure considering false alarms proposed in Chapter 3 is employed. Regarding the estimation of life-cycle cost, PHM development cost and total maintenance costs are revised to include false alarm rates. The results of RAP, target reliability, redundancy level, and target false and missed alarm rates, are transferred to RBDO and PHM design problem. In RBDO, the subsystems are designed to satisfy the allocated target reliability while minimizing initial development cost. The optimal design of RBDO is delivered to PHM design problem. As RBDO is not related to false alarms, it is equivalent to that of RDSD. In PHM design, a PHM unit is designed to satisfy the target false and missed alarm rates allocated from RAP while minimizing PHM development cost and total maintenance cost. Compared to RDSD which does not consider false alarm rate, RDSD-FA can cope with false alarm problems and designs PHM more specifically to minimize life-cycle cost. In order to demonstrate RDSD-FA, the design problem of an Electro-hydrostatic actuator (EHA) is employed. The design from RDSD fails to satisfy the target resilience level whereas that of RDSD-FA satisfies successfully.

Chapter 5. Resilience-Driven System Design Considering Time-Dependent False Alarms (RDSD-TFA)

Resilience-driven system design considering false alarms (RDSD-FA) in Chapter 4 presents the systematic approach for assigning resilience to an engineered system in a cost effective way. This can design a resilient engineered system time-efficiently through three hierarchical tasks: resilience allocation problem (RAP), reliability-based design optimization (RBDO), and prognostics and health management (PHM) design. However, there are two limitations which should be handled for the maturing of RDSD-FA.

Limitation 1) Inconsideration of time-dependent variability of an engineered system

As an engineered system operates, its health state changes due to health degradation by adverse events and health recovery by maintenance actions. Correspondingly, its reliability, false and missed alarm rates, and resilience also change along with time. However, they are regarded as time-independent or static values in RDSD-FA. Although this regarding helps to design an engineered system to be resilient in a time-efficient manner, the estimation of resilience and life-cycle cost becomes inaccurate resulting unexpected loss. Thus in order to design a resilient engineered system in a rigorous and accurate manner, time-dependent variability of the system should be considered.

Limitation 2) Difficulty in determining target resilience level

In RDSD-FA, a system and PHM are designed to minimize life-cycle cost

while satisfying target resilience level. Regarding target resilience level, its determination is one of major issues because it affects system failure prevention rate (i.e. resilience) as well as life-cycle cost. For example, the designs satisfying $\Psi^t = 0.95$ and $\Psi^t = 0.99$ have life-cycle costs of 45.9357 and 55.0199 respectively [11]. However, there is no relevant study about deciding target resilience level in a systematic approach. Additionally, considering time-dependent variability of resilience, which is assumed to be static in RDSD-FA, its determination becomes more complicated.

In order to handle two limitations, this chapter proposes RDSD considering time-dependent false alarms (RDSD-TFA). In order to handle the first limitation, the concept and quantification method for time-dependent false and missed alarms are newly proposed. Regarding the other two variables, time-dependent reliability has been investigated by other researchers [104-107], and time-dependent resilience can be easily calculated based upon Eq. (3.1) if time-dependent reliability and time-dependent false alarm rates are quantified. The consideration of time-dependent probabilities enables the life-cycle simulation of an engineered system. This enables to analyze time-dependent maintenance probabilities and life-cycle cost more accurately and rigorously compared to RDSD-FA.

Regarding the second limitation, RDSD-TFA excludes the constraint of resilience, and thus the determination of target resilience level is not needed. In conventional design methodologies, objective function (e.g. total structural mass related to initial development cost) and constraint function (e.g. reliability related to maintenance costs) have different quantities which are exclusive to each other,

and thus they should be considered separately. However, in RDSD, the objective function, life-cycle cost, is related with resilience of constraint function. For example, higher target resilience increases initial development cost and PHM development cost, and decreases total maintenance cost. Therefore, the optimality of resilience constraint function can be evaluated in terms of life-cycle cost, and the constraint of resilience can be excluded. If target resilience level is lower than its optimum, system availability becomes lower, resulting excessive maintenance costs. If target resilience level is higher than its optimum, the system is conservatively designed with high initial development cost and PHM development cost. When LCC is minimized, the resulted resilience can be evaluated to be optimum.

This Chapter is organized as follows: Chapter 5.1 introduces the concept and quantification method of time-dependent false alarms. Chapter 5.2 presents RDSD-TFA in detail. The case studies of a numerical example and an electro-hydrostatic actuator (EHA) described in Chapter 5.3 demonstrates the feasibility and effectiveness of the proposed RDSD-TFA. Summary and discussion are discussed in Chapter 5.45.3.

5.1 Time-Dependent False and Missed Alarms in PHM

The health state of an engineered system changes throughout its operation time. Thus, its health feature distribution, which is shown to be static in Figure 2-10 and Figure 2-11, is time-dependent or time-variant. Figure 5-1 shows the example of time-dependent health feature HF distributions at three time steps (t_1, t_2, and t_3). It is assumed that the health feature distribution and its variance

change together as operation time increases. This assumption is relevant to real engineering problems such as a power transformer [59], a liquid damage indicator (LDI) [108], and an organic light-emitting diode (OLED) [109]. At the initial time of t_1, the health feature is distributed smaller than both estimated and true health state criteria (i.e., c_{esti} and c_{true}). Thus, the system is perfectly healthy and there is no false alarm. At time t_2, the health feature distribution is smaller than c_{true}; however, some portion of it exceeds c_{esti}. It results in a false alarm: the system is still utterly healthy, but a PHM unit estimates that system failure can occur. At time t_3, the health feature distribution exceeds c_{true} partially and c_{esti} totally. The system can be faulty and its false alarm rate becomes one according to Eq. (2.17). This means that the PHM unit will always estimate the healthy system to be faulty. Figure 5-2 shows the calculated time-dependent false alarm rate $FA(t)$ and reliability $R(t)$ of Figure 5-1. $R(t)$ is the probability that a system survives at time t, and this is formulated as Eq. (5.1). In this example, $R(t)$ is defined as $\Pr(HF(t) < c_{true})$.

$$R(t) = \Pr\left(\mathrm{E}_{\mathrm{healthy}}^{\mathrm{true}}(t)\right) \tag{5.1}$$

In Figure 5-2, false alarm rate $FA(t)$ cannot be estimated after the health feature distribution is totally beyond c_{true}. At this moment, the system is not healthy at all but totally faulty (i.e., $R(t) = 0$). Thus, it is impossible to evaluate the probability whether the healthy system is estimated to be healthy or faulty. Similarly, missed alarm rate is not quantifiable when an engineered system is totally healthy (i.e., $R(t) = 1$).

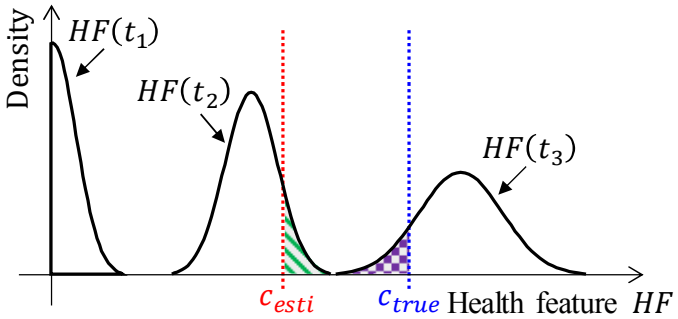


Figure 5-1 Example of time-dependent health feature distributions

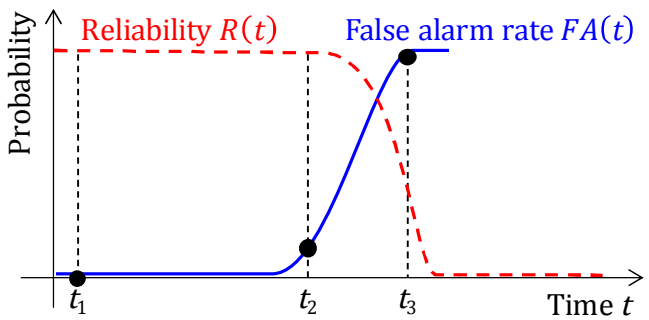


Figure 5-2 Example of calculated time-dependent false alarm rate and reliability

As shown in the example above, the false alarm rate as well as missed alarm rate are not static, as stated in the previous research [11, 110-114]; rather, they are time-dependent. Accordingly, the false and missed alarm rate formulations in Eqs. (2.15) and (2.16) need to incorporate time t, as shown below.

$$FA(t) = \Pr\left(\mathrm{E}_{\mathrm{faulty}}^{\mathrm{esti}}(t)\middle|\mathrm{E}_{\mathrm{healthy}}^{\mathrm{true}}(t)\right) \tag{5.2}$$

$$MA(t) = \Pr\left(\mathrm{E}_{\mathrm{healthy}}^{\mathrm{esti}}(t)\middle|\mathrm{E}_{\mathrm{faulty}}^{\mathrm{true}}(t)\right) \tag{5.3}$$

where $\mathrm{E}_{\mathrm{healthy}}^{\mathrm{true}}(t)$ and $\mathrm{E}_{\mathrm{faulty}}^{\mathrm{true}}(t)$ are events of a truly healthy system and a truly faulty system at time t, respectively. $\mathrm{E}_{\mathrm{healthy}}^{\mathrm{esti}}(t)$ and $\mathrm{E}_{\mathrm{faulty}}^{\mathrm{esti}}(t)$ are the

events where the system health state is estimated to be healthy and faulty at time t, respectively.

In order to calculate the probabilities of Eqs. (5.2) and (5.3), a health estimation matrix of Table 2-3 is modified into Table 5-1 to incorporate the time t. As described in Chapter 2.2.2, its element $N_{\alpha\hat{\beta}}$ is the number of samples estimated to be β health state by PHM model given the true α health state. To quantify Table 5-1, Monte Carlo simulation (MCS) can be employed which generates random health feature samples. The samples are allocated to four elements in Table 5-1 according to the true and estimated health state by PHM model . Time-dependent false and missed alarm rates can be quantified using Eqs. (5.4) and (5.5). In case of using MCS, time-dependent reliability can be estimated as Eq. (5.6) where $N_{\mathrm{H}}(t)$ and $N_{\mathrm{F}}(t)$ are the number of true healthy samples ($N_{\mathrm{H}}(t) = N_{\mathrm{H}\hat{\mathrm{H}}}(t) + N_{\mathrm{H}\hat{\mathrm{F}}}(t)$) and the number of true faulty samples ($N_{\mathrm{F}}(t) = N_{\mathrm{F}\hat{\mathrm{H}}}(t) + N_{\mathrm{F}\hat{\mathrm{F}}}(t)$) at time t respectively. Regarding the false and missed alarm rate quantification for multiple health states, including healthy and multi failure modes, please refer the approach described in Chapter 2.2.2.

Table 5-1 Health estimation matrix of two health states

Health estimation matrix		**Estimated health state**	
		Healthy ($\hat{\mathrm{H}}$)	Faulty ($\hat{\mathrm{F}}$)
True health state	Healthy (H)	$N_{\mathrm{H}\hat{\mathrm{H}}}(t)$	$N_{\mathrm{H}\hat{\mathrm{F}}}(t)$
	Faulty (F)	$N_{\mathrm{F}\hat{\mathrm{H}}}(t)$	$N_{\mathrm{F}\hat{\mathrm{F}}}(t)$

$$FA(t) = \frac{N_{\mathrm{H}\widehat{\mathrm{F}}}(t)}{N_{\mathrm{H}\widehat{\mathrm{H}}}(t) + N_{\mathrm{H}\widehat{\mathrm{F}}}(t)} \tag{5.4}$$

$$MA(t) = \frac{N_{\mathrm{F}\widehat{\mathrm{H}}}(t)}{N_{\mathrm{F}\widehat{\mathrm{H}}}(t) + N_{\mathrm{F}\widehat{\mathrm{F}}}(t)} \tag{5.5}$$

$$R(t) = \frac{N_{\mathrm{H}}(t)}{N_{\mathrm{H}}(t) + N_{\mathrm{F}}(t)} \tag{5.6}$$

5.2 Resilience-Driven System Design Considering Time-Dependent False Alarms (RDSD-TFA)

This chapter proposes resilience-driven system design considering time-dependent false alarms (RDSD-TFA). First, the overview of RDSD-TFA framework is presented, and then its details will be followed.

5.2.1 Overview of RDSD-TFA Framework

RDSD-TFA aims at designing a resilient engineered system to minimize its life-cycle cost. Its optimization problem can be formulated as below.

$$\begin{aligned} &\text{minimize}_{\mathbf{d}^{\text{SYS}},\mathbf{d}^{\text{PHM}}} \quad f_{obj}\left(LCC_{\text{TFA}}\left(\mathbf{d}^{\text{SYS}},\mathbf{d}^{\text{PHM}}\right)\right) \\ &\text{subject to} \quad \mathbf{d}^{\text{SYS,L}} \le \mathbf{d}^{\text{SYS}} \le \mathbf{d}^{\text{SYS,U}} \\ &\qquad\qquad \mathbf{d}^{\text{PHM,L}} \le \mathbf{d}^{\text{PHM}} \le \mathbf{d}^{\text{PHM,U}} \end{aligned} \tag{5.7}$$

where $f_{obj}(\cdot)$ is the objective function and has various forms, depending on the system designer's interest, such as mean value, maximum value, 95$^{\text{th}}$ percentile value, and the probability of exceeding an assigned budget. LCC_{TFA} is the life-cycle cost of RDSD-TFA and it is function of system design variable vector $\mathbf{d}^{\text{SYS}}$ and PHM design variable vector $\mathbf{d}^{\text{PHM}}$. $\mathbf{d}^{\text{SYS,L}}$ and $\mathbf{d}^{\text{SYS,U}}$ are lower and upper design boundaries of $\mathbf{d}^{\text{SYS}}$; $\mathbf{d}^{\text{PHM,L}}$ and $\mathbf{d}^{\text{PHM,U}}$ are lower and upper design boundaries of $\mathbf{d}^{\text{PHM}}$.

$\mathbf{d}^{\text{SYS}}$ and $\mathbf{d}^{\text{PHM}}$ are equivalent to $\mathbf{d}_j^{\text{C}}$ and $\mathbf{d}_j^{\text{PHM}}$ of RDSD-FA in Chapter 4, but only difference of target design scope. In RDSD-FA, the top-level resilience allocation problem (RAP) of Eq. (4.1) allocates target performance levels (i.e., reliability, false alarm rate, and missed alarm rate) to subsystem components.

Each subsystem component and PHM unit is designed considering its own $\mathbf{d}_j^{\mathrm{C}}$ and $\mathbf{d}_j^{\mathrm{PHM}}$ to satisfy the allocated target reliability and target false and missed alarm rates as shown in Eq. (4.11). Whereas RDSD-TFA, which is without resilience constraint, does not allocate target performance levels to subsystem components. Thus, it cannot design subsystem components one by one. Instead, it designs a whole system considering all design variables at once (i.e. $\mathbf{d}^{\mathrm{SYS}} = \{\mathbf{d}_j^{\mathrm{C}}: j = 1, \dots, N\}$ and $\mathbf{d}^{\mathrm{PHM}} = \{\mathbf{d}_j^{\mathrm{PHM}}: j = 1, \dots, N\}$). This may incur great computational cost, and possible solutions are surrogate modeling with adaptive sampling technique which reduces computational burden [115-117], and parallel and distributed computing which enables high performance computing [118].

LCC_{TFA} is formulated as a sum of initial development cost ($C_{\mathrm{TFA}}^{\mathrm{I}}$), PHM development cost ($C_{\mathrm{TFA}}^{\mathrm{PHM}}$), and total maintenance cost ($C_{\mathrm{TFA}}^{\mathrm{M}}$) considering time-dependent false alarms.

$$\begin{aligned} &LCC_{\mathrm{TFA}}\left(\mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}}\right) \\ &\quad = C_{\mathrm{TFA}}^{\mathrm{I}}\left(\mathbf{d}^{\mathrm{SYS}}\right) + C_{\mathrm{TFA}}^{\mathrm{PHM}}\left(\mathbf{d}^{\mathrm{PHM}}\right) + C_{\mathrm{TFA}}^{\mathrm{M}}\left(\mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}}\right) \end{aligned} \tag{5.8}$$

$C_{\mathrm{TFA}}^{\mathrm{I}}$ is total incurred system development cost including component production cost, assembly cost, quality control cost, and so on. $C_{\mathrm{TFA}}^{\mathrm{PHM}}$ includes hardware cost (e.g., sensor unit cost, signal processing unit cost, installation/maintenance cost) and software cost (e.g., algorithm training data acquisition cost, expert consulting fee, qualification cost). $C_{\mathrm{TFA}}^{\mathrm{M}}$ is total maintenance costs including unnecessary, corrective, and predictive maintenance costs. As discussed in Chapter 4.3, $C_{\mathrm{TFA}}^{\mathrm{M}}$ is affected by reliability, false alarm rate, and missed alarm rate, and thus it is a function of $\mathbf{d}^{\mathrm{SYS}}$ related to reliability and $\mathbf{d}^{\mathrm{PHM}}$ related to false and missed alarm rates.

Figure 5-3 shows the overall framework of RDSD-TFA and the relationship between key variables. This framework designs an engineered system resilient by optimizing $\mathbf{d}^{\mathrm{SYS}}$ and $\mathbf{d}^{\mathrm{PHM}}$ so as to minimize LCC_{TFA}. In order to estimate LCC_{TFA}, three tasks are required: system analysis for $C_{\mathrm{TFA}}^{\mathrm{I}}$, PHM analysis for $C_{\mathrm{TFA}}^{\mathrm{PHM}}$, and life-cycle simulation for $C_{\mathrm{TFA}}^{\mathrm{M}}$. Based upon the analysis of LCC_{TFA}, $\mathbf{d}^{\mathrm{SYS}}$ and $\mathbf{d}^{\mathrm{PHM}}$ are updated until convergence to minimal LCC_{TFA}, and this optimization is fourth task. The details of four tasks in RDSD-TFA are described below.

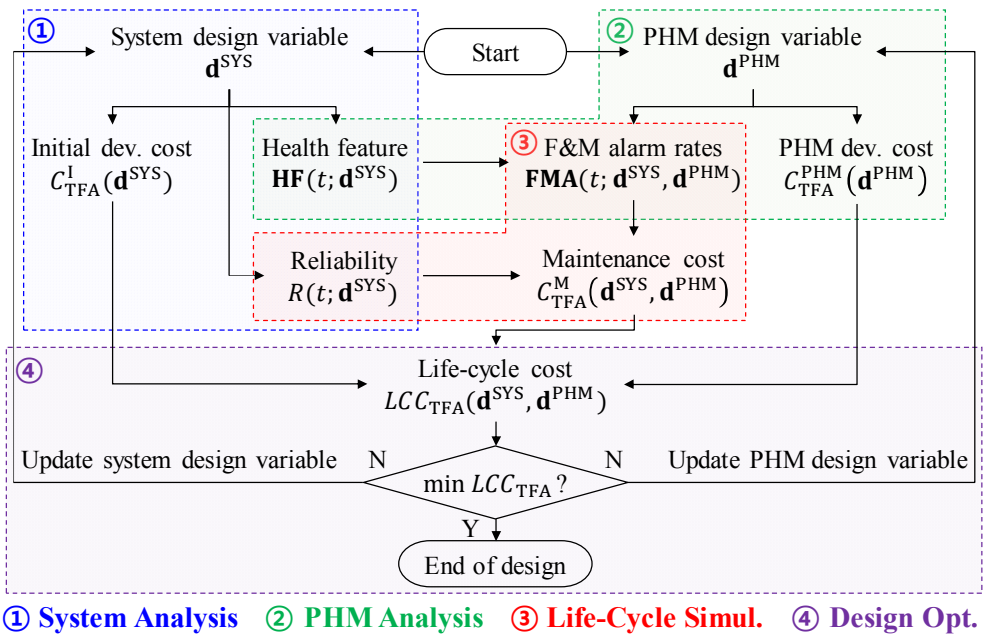


Figure 5-3 Overall framework of resilience-driven system design considering time-dependent false alarms

5.2.2 Task 1: System Analysis

This task analyzes initial development cost $C_{\mathrm{TFA}}^{\mathrm{I}}$, time-dependent health feature and time-dependent reliability according to given design variables. As an engineered system operates, its health degrades gradually due to adverse events. This makes the engineered system vulnerable to failure, and reliability gets lowered as well as health features changes. The change of reliability and health features are affected by design variables. For example, an airborne retractable mechanical system fails mainly due to the wear of its hinge. This wear can be detected the increase of vibration and hydraulic pressure. It is shown that its time-dependent reliability can be enhanced by adjusting the length, orientation, and radiuses of rods [107].

Initial development cost is a complex function of various factors such as material quantity, material quality, machining precision, geometry complexity, assembly cost, quality check. Thus, it is usually replaced by mass or volume of material in mechanical design problems [21, 56, 119-121]. In order to analyze time-dependent health features and time-dependent reliability, failure mode needs to be defined first. There are multiple failure modes in an engineered system, and it is complex and inefficient to consider all of them. Among many failure modes, critical failure mode is selected based upon analysis on their frequency, consequence, and risk [122-124]. Then, health degradation of an engineered system can be modeled by exploiting the physics of failure (PoF) of the selected failure mode [124, 125], a regression analysis, or a continuous process based upon the data from an experiment or a simulation model [126-128]. Lastly, time-dependent reliability and time-dependent health features are

estimated according to the constructed health degradation model. The time-dependent reliability can be quantified using the uncertainty propagation methods discussed in Chapter 2.1.1.1. The health features are defined to be capable of representing the health degradation as discussed in Chapter 2.2.1. For example, a water-cooled power generator fails mainly due to moisture absorption which can be detected by the increase of capacitance level on a stator bar surface [60]. A bearing of a rotating system deteriorates due to lubricant contamination, excessive load, and so on which can be diagnosed by statistical moments of vibration signals [129].

Figure 5-4 shows the example of time-dependent health feature and time-dependent reliability analysis for brushless direct current (BLDC) fan. Among various failure modes, the bearing seizure mainly occurred due to lubricant deterioration is selected based upon the failure modes and risk analysis [122]. It is known that the life of bearing due to lubricant deterioration is mainly determined by lubricant temperature, operating fan speed, and limiting fan speed [79]. Thus, the time-dependent reliability of BLDC fan can be modeled by estimating its life distribution. And this deterioration changes kinematic viscosity and dielectric constant, which can be used as health features[79]. As shown in Figure 5-4, the health features are affected by uncertainties in temperature, contamination material and their properties (i.e., viscosity and dielectric constant), and thus would be randomly distributed.

Brushless Direct Current (BLDC) Fan

Failure Mode	Bearing Seizure	Blade Crack	Motor Solder Crack
Failure Mechanism	Lubricant Deterioration	Fatigue	Fatigue
Freq.	5	3	2
Cons.	3	3	4
Risk	15	9	8

Physics of Failures

- 50% failure life $L_{50} = f_{L_{50}}(RPM, RPM_{max}, T)$
- Kinematic viscosity $V = f_V(t, P_{cont}, V_{cont}, T)$
- Dielectric constant $\varepsilon = f_\varepsilon(t, P_{cont}, \varepsilon_{cont}, T)$

RPM: fan speed T: temperature t: time
RPM_{max}: limiting RPM P: contamination percentage

Time-dependent Health Feature & Reliability

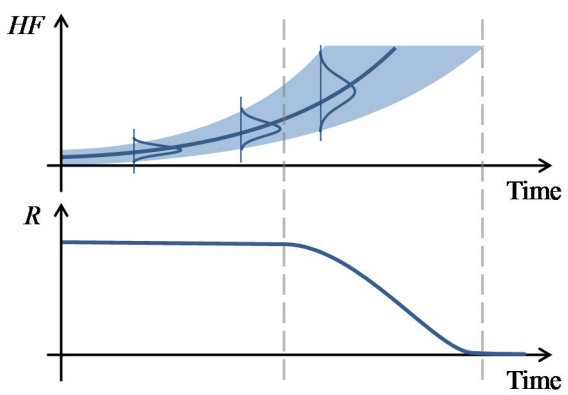


Figure 5-4 Example of analyze time-dependent health feature and time-dependent reliability for brushless direct current (BLDC) fan

5.2.3 Task 2: PHM Analysis

This task evaluates PHM development cost $C_{\mathrm{TFA}}^{\mathrm{PHM}}$ and time-dependent false and missed alarm rates according to PHM design variables. PHM design variables, as described in Chapter 2.1.2.4, consist of hardware and software design variables. The hardware design variables are sensor type, sensor quantity, and their locations. The software design variables are the type of PHM algorithm and corresponding parameters. Correspondingly, PHM development cost is of hardware cost (e.g., sensor unit cost, signal processing unit cost, installation/maintenance cost) and software cost (e.g., algorithm training data acquisition cost, expert consulting fee, qualification cost).

In order to analyze time-dependent false and missed rates, PHM model is trained and tested. Figure 5-5 shows the example of estimating time-dependent false and missed alarm rates when using two-dimensional health feature (i.e., HF_1 and HF_2) and linear classifier as PHM algorithm. In the training, the linear classifier is trained to minimize health state estimation error based upon training data in healthy and faulty health states (HS). The trained linear classifier is plotted as linear health state boundary, and this can differ from true health state boundary because of insufficient data, data uncertainty (e.g., measurement noise, variant operating conditions), improper PHM algorithm selection, inadequate parameters, and so on. And this discrepancy yields false and missed alarm problems. In the testing, time-dependent false and missed alarm rates are calculated. The trained PHM model estimates the health states of the time-dependent health features from Task 1. According to the true and estimated health states, the health estimation of Table 5-1 can be constructed, and then the

time-dependent false and missed alarm rates are calculated using Eqs. (5.4) and (5.5). At initial time, the health features (e.g. kinematic viscosity and dielectric constant) are small and the engineered system (e.g. BLDC fan) is obviously healthy with no false and missed alarm rates. As the health features increase and approach to the health state boundaries, false and missed alarm rates increase. When the health features go beyond the health state boundaries, the engineered system is clearly faulty, and false and missed alarm rates decrease.

In the plot of time-dependent false and missed alarm rates in Figure 5-5, two alarm rates are not plotted for all the time; no false alarm rate for latter time and no missed alarm rate for initial time. This is because they are not quantifiable as the denominators of Eqs. (5.4) and (5.5) are zero. When the engineered system is perfectly healthy ($R(t) = 1$), there is no faulty samples from Monte Carlo simulation (MCS). Thus, the denominator of Eq. (5.5) is zero and missed alarm rate is not assessable. When the engineered system is perfectly faulty ($R(t) = 0$), there is no healthy samples and false alarm rate of Eq. (5.4) is not obtainable.

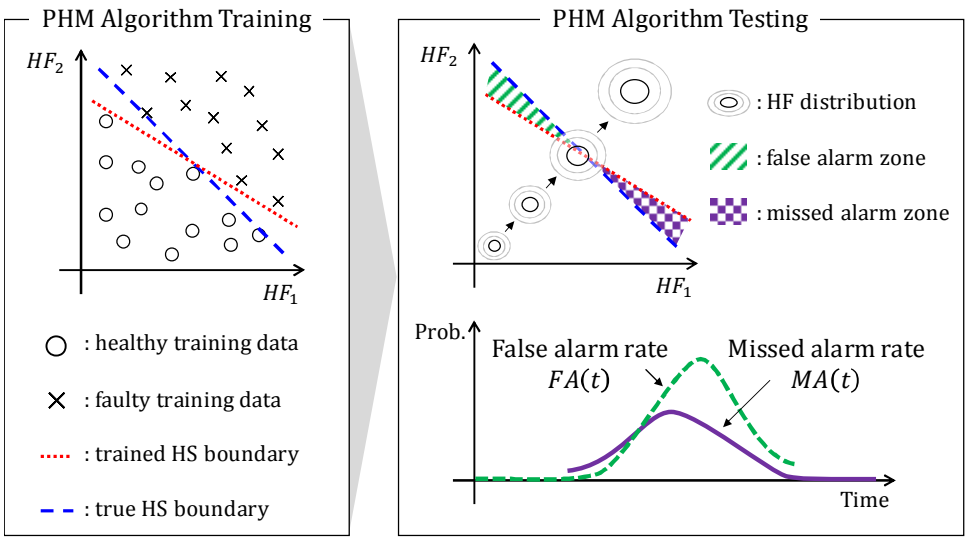


Figure 5-5 Time-dependent false alarm rates estimation

5.2.4 Task 3: Life-Cycle Simulation

This task performs the life-cycle simulation to estimate total maintenance cost considering time-dependent reliability and time-dependent false and missed alarm rates. The total maintenance cost $C_{\mathrm{TFA}}^{\mathrm{M}}$ is the sum of incurred maintenance cost for the designed life-cycle.

$$C_{\mathrm{TFA}}^{\mathrm{M}} = \sum_{i=1}^{N} c_M(t_i) \tag{5.9}$$

where $c_M(t_i)$ is the incurred maintenance cost at i-th life-cycle time t_i, and N is the number of total time steps for the designed life-cycle. Both $C_{\mathrm{TFA}}^{\mathrm{M}}$ and $c_M(t_i)$ are random variables affected by uncertainty factors, such as manufacturing error, material property uncertainties, operating conditions, health degradation, and health restoration by maintenance actions. In order to estimate the costs and their uncertainties, this study proposes the life-cycle simulation considering time-dependent false and missed alarms shown in Figure 5-6. This is

based upon a stochastic simulation that can trace the time-dependent random variables, such as reliability $R(t_i)$, false alarm rate $FA(t_i)$, missed alarm rate $MA(t_i)$, and maintenance cost $c_M(t_i)$, at each time step. Specifically, a discrete-time stochastic process, also called as a random sequence, is employed of which the index set is finite or countable [112]. Compared to a continuous-time stochastic process, this does not require complex calculation as well as can ensure high accuracy by minimize the interval between adjacent indices [130]. The details of the framework are explained below.

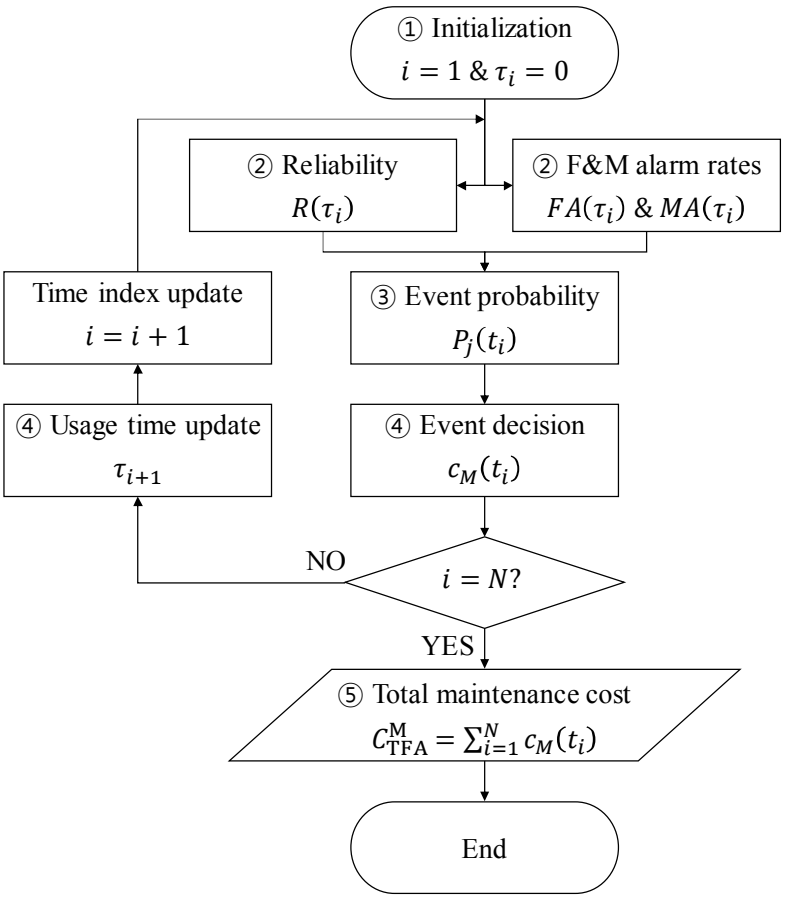


Figure 5-6 Framework of life-cycle simulation for total maintenance cost analysis

Step 1) Initialization

First, time index i and usage time τ_i are initialized. The time index i represents life-cycle time step ranging from one to N which corresponds to the end of the designed life-cycle time. The usage time τ_i is relevant to the health degradation of an engineered system. It increases along with operation time, and becomes zero when system restoration or replacement occurs.

Step 2) Time-dependent probability estimation (Reliability, false alarm rate and missed alarm rate)

From Step 1 and Step 2, the models of time-dependent reliability $R(\tau; \mathbf{d}^{\mathrm{SYS}})$, false alarm rate $FA(\tau; \mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}})$, and missed alarm $MA(\tau; \mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}})$ are obtained. By substituting the usage time τ_i into three models, three probabilities at *i*-th time index can be estimated.

$$R_{LCS}(t_i) = R(\tau_i; \mathbf{d}^{\mathrm{SYS}}) \tag{5.10}$$

$$FA_{LCS}(t_i) = FA(\tau_i; \mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}}) \tag{5.11}$$

$$MA_{LCS}(t_i) = MA(\tau_i; \mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}}) \tag{5.12}$$

where $R_{LCS}(t_i)$, $FA_{LCS}(t_i)$, and $MA_{LCS}(t_i)$ are reliability, false alarm rate, and missed alarm rate of life-cycle simulation (LCS) at *i*-th life-cycle time index respectively.

Step 3) Event probability calculation

At each time step, there are four possible events: normal operation, unnecessary maintenance, corrective maintenance, and predictive maintenance. The probability of four events can be calculated using the probabilities from Step 2. For example, unnecessary maintenance occurs when the given PHM model estimates a heathy engineered system to be faulty (i.e., false alarm). This yields the costs of unnecessary system shutdown, inspection, and unnecessary system replacement in case of incorrect inspection. Its probability $P_{UM}(t_i)$ is the joint probability of the true healthy health state event $\mathrm{E}_{\mathrm{healthy}}^{\mathrm{true}}(t_i)$ and the faulty health state estimation event $\mathrm{E}_{\mathrm{faulty}}^{\mathrm{esti}}(t_i)$. According to conditional probability

theory, $P_{UM}(t_i)$ can be formulated as shown below.

$$\begin{aligned} P_{UM}(t_i) &= \Pr\left(\mathrm{E}^{\mathrm{esti}}_{\mathrm{faulty}}(t_i)\mathrm{E}^{\mathrm{true}}_{\mathrm{healthy}}(t_i)\right) \\ &= \Pr\left(\mathrm{E}^{\mathrm{esti}}_{\mathrm{faulty}}(t_i)|\mathrm{E}^{\mathrm{true}}_{\mathrm{healthy}}(t_i)\right)\cdot \Pr\left(\mathrm{E}^{\mathrm{true}}_{\mathrm{healthy}}(t_i)\right) \\ &= FA_{LCS}(t_i)\cdot R_{LCS}(t_i) \end{aligned} \tag{5.13}$$

The other three event probabilities of normal operation $P_O(t_i)$, corrective maintenance $P_{CM}(t_i)$, and predictive maintenance $P_{PM}(t_i)$, can be formulated in the same manner as Eq. (5.13). Table 5-2 lists the four events with their probabilities.

Table 5-2 Four events and their probabilities in system operation

Health state		**Result**	**Event probability**
True	**Esti.**		
Healthy	Healthy	Normal operation	$P_O(t_i) = \left(1 - FA_{LCS}(t_i)\right) \cdot R_{LCS}(t_i)$
	Faulty	Unnecessary shutdown & mnt.	$P_{UM}(t_i) = FA_{LCS}(t_i)\cdot R_{LCS}(t_i)$
Faulty	Healthy	System failure & corrective mnt.	$P_{CM}(t_i) = MA_{LCS}(t_i) \cdot \left(1 - R_{LCS}(t_i)\right)$
	Faulty	Failure prediction & predictive mnt.	$P_{PM}(t_i) = \left(1 - MA_{LCS}(t_i)\right) \cdot \left(1 - R_{LCS}(t_i)\right)$

Besides the three maintenance actions (unnecessary, corrective, and predictive), another widely used maintenance strategy is preventive maintenance. This is also called scheduled maintenance, time-based maintenance, or planned maintenance. It can be triggered by time (e.g., every three month) or usage (e.g.,

every 1,000 km driving). The cost analysis regarding preventive maintenance action has been investigated by many researchers [113, 131-135]. As preventive maintenance is not related to false and missed alarm issues and well investigated, it is not considered in this study.

Step 4) Event decision

This step uses stochastic discrete event simulation to decide which of the four events occurs [136]. Stochastic discrete event simulation makes an array of probabilities for all possible events and then its cumulative sum, which is a discrete cumulative distribution, is taken. This is used to decide which event occurs by picking a uniformly distributed random number between zero and one. Figure 5-7 shows the example of event decision $\mathrm{E}(t_i)$ at *i*-th life-cycle time index which is formulated as Eq. (5.14).

$$\mathrm{E}(t_i) = \begin{cases} \quad : 0 \le z < P_O(t_i) \\ \mathrm{E_O} : P_O(t_i) \le z < P_O(t_i) + P_{UM}(t_i) \\ \mathrm{E_{UM}} : P_O(t_i) + P_{UM}(t_i) \le z \\ \mathrm{E_{CM}} \qquad\qquad\quad < P_O(t_i) + P_{UM}(t_i) + P_{CM}(t_i) \\ \mathrm{E_{PM}} : P_O(t_i) + P_{UM}(t_i) + P_{CM}(t_i) \le z \le 1 \end{cases} \tag{5.14}$$

where $\mathrm{E_O}$ is the normal operation event, and $\mathrm{E_{UM}}$, $\mathrm{E_{CM}}$, and $\mathrm{E_{PM}}$ are the events of unnecessary, corrective, and predictive maintenance, respectively. z is the uniformly distributed random number from zero to one ($z \sim U(0,1)$).

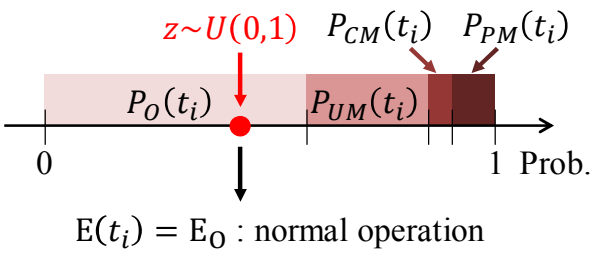


Figure 5-7 Example of event decision

This event decision results in maintenance costs and a change in the usage time; these are relevant to the health degradation of an engineered system (Table 5-3). In the normal operation event, there is no maintenance action and no maintenance cost. The operation time increases by Δt, which is the fixed time interval between the adjacent life-cycle time steps ($\Delta t = t_{i+1} - t_i$), and thus the next time step usage time τ_{i+1} would be $\tau_i + \Delta t$. Unnecessary maintenance yields costs of unnecessary system shutdown, unnecessary inspection, and – in the case of incorrect inspection – unnecessary system replacement. Depending upon the system shutdown time, τ_{i+1} has a value between τ_i (full shutdown & no operation) and $\tau_i + \Delta t$ (no shutdown & full operation). Corrective maintenance as a result of system failure and missed alarm involves system shutdown costs and system replacement costs. Predictive maintenance yields the costs of system shutdown, inspection, and potential failure correction. In this study, it is assumed that both corrective and predictive maintenance make successful restoration, and thus, the health state is initialized to be as good as new with zero usage time ($\tau_i = 0$). In real applications, however, this is not always guaranteed and there are other restoration results that can occur, such as "worse than new" and "better than new" [14, 18, 128].

Step 5) Life-cycle maintenance cost and its uncertainty analysis

Until the designed life-cycle time step t_i $(i = 1, \dots, N)$, the Steps 1~4 are iteratively processed. Then, the total maintenance cost $C_{\mathrm{TFA}}^{\mathrm{M}}$ can be estimated by summing up the incurred maintenance costs (Eq. (5.9)). Its uncertainty can be analyzed by using Monte Carlo simulation (MCS), which repeatedly carries out the analysis framework shown in Figure 5-6. This results in the histogram of $C_{\mathrm{TFA}}^{\mathrm{M}}$, which can be used to evaluate the total maintenance cost and its uncertainty.

Table 5-3 Maintenance cost and usage time update of four events

Event	**Health state change**	**Cost** $c_M(t_i)$	**Usage time update** τ_{i+1}
Normal operation $\mathrm{E_O}$	Health degradation	0	$\tau_i + \Delta t$
Unnecessary mnt. $\mathrm{E_{UM}}$	Partial health degradation	c^{UM}	$\tau_i \sim \tau_i + \Delta t$
Corrective mnt. $\mathrm{E_{CM}}$	Health initialization	c^{CM}	0
Predictive mnt. $\mathrm{E_{PM}}$	Health initialization	c^{PM}	0

5.2.5 Task 4: Design Optimization

This task optimizes a system design variable vector $\mathbf{d}^{\mathrm{SYS}}$ and a PHM design variable vector $\mathbf{d}^{\mathrm{PHM}}$ to minimize life-cycle cost LCC_{TFA}. The optimization updates $\mathbf{d}^{\mathrm{SYS}}$ and $\mathbf{d}^{\mathrm{PHM}}$, and performs Task 1~3 to estimate LCC_{TFA} iteratively until its convergence to minimum.

The design variables, $\mathbf{d}^{\mathrm{SYS}}$ and $\mathbf{d}^{\mathrm{PHM}}$, have continuous values (e.g., geometric shape, material property, sensor location, and PHM algorithm parameter) as well as integer values (e.g., sensor type, PHM algorithm type, and subsystem redundancy). Thus, this optimization problem is a mixed-integer nonlinear programming (MINLP) problem, and can be solved using linearization approaches for a mixed-integer linear problem (MILP) [42, 43] and meta-heuristic algorithms [44, 45].

RDSD-FA in Chapter 4 consists of hierarchical tasks, and they optimizes $\mathbf{d}^{\mathrm{SYS}}$ and $\mathbf{d}^{\mathrm{PHM}}$ one by one. This is possible because each task concerns sole design variable vector: $\mathbf{d}^{\mathrm{SYS}}$ of reliability-based design optimization (RBDO) and $\mathbf{d}^{\mathrm{PHM}}$ of PHM design. Whereas RDSD-TFA optimizes $\mathbf{d}^{\mathrm{SYS}}$ and $\mathbf{d}^{\mathrm{PHM}}$ at once because they affect LCC_{TFA} as shown in Figure 5-3. As a result, RDSD-TFA considers all design variables at once, and this results in high computational cost. In order solve this problem, surrogate modeling can be employed. Surrogate modeling, also called as response surface method or meta modeling, aims to construct a model emulating the responses of interest [116, 117, 137].

5.3 Case studies

This chapter includes two case studies: numerical example of life-cycle simulation, and electro-hydrostatic actuator (EHA) design. The first example helps to comprehend time-dependent false and missed alarm rates and life-cycle simulation for total maintenance cost estimation. The second example is to demonstrate the proposed RDSD-TFA by designing EHA.

5.3.1 Numerical Example of Life-Cycle Simulation

In order to perform a life-cycle simulation, time-dependent reliability and time-dependent false and missed alarm rates are required as shown in Figure 5-3. In order to estimate three probabilities, (1) the health feature model, (2) the true health state model, and (3) the PHM model are needed. For the health feature model, the two-dimensional stochastic model of is assumed as shown in Eq. (5.15).

$$\begin{pmatrix} HF_1(\tau_i) \\ HF_2(\tau_i) \end{pmatrix} \sim N\left(\begin{pmatrix} \mu_1(\tau_i) \\ \mu_2(\tau_i) \end{pmatrix}, \begin{pmatrix} \sigma_1^2(\tau_i) & 0 \\ 0 & \sigma_2^2(\tau_i) \end{pmatrix} \right) \tag{5.15}$$

where health feature values $HF_1(\tau_i)$ and $HF_2(\tau_i)$ are assumed to follow multivariate normal distribution $N(\cdot)$ with mean values $(\mu_1(\tau_i) = \mu_2(\tau_i) = 0.2 + 0.6(\tau_i/100))$ and standard deviation values $(\sigma_1(\tau_i) = \sigma_2(\tau_i) = 0.01 + 0.04(\tau_i/100))$ at usage time τ_i. The contours of HF distribution at three levels (1%, 50%, and 99%) and six operation time steps ($\tau_i = 0,20,\ldots,100$) are shown in Figure 5-8 . This model assumption is quite relevant to real engineering problems. For example, the mechanical faults of a power transformer can be diagnosed with two health features: root mean square (RMS) and root mean square deviation (RMSD) of its tank surface vibration [59]. RMS and RMSD are increased together as the structural strength of a power transformer degrades. And RMS and RMSD are getting scattered as the uncertainty of health degradation is accumulated. Figure 5-9 shows the scatter plot of RMS and RMSD, which is comparable to Figure 5-8.

The true health state model HS_{true} is set to be Eq. (5.16), which is plotted as the solid line in Figure 5-8.

$$HS_{true} = \begin{cases} \text{healthy } H : HF_1 + HF_2 - 1 < 0 \\ \text{faulty } F \ : HF_1 + HF_2 - 1 \geq 0 \end{cases} \tag{5.16}$$

For the PHM model, the linear discriminant analysis (LDA) classifier is employed, which defines a linear boundary or surface between multiclass data by maximizing their separation [99]. The model is trained with randomly generated 30 health feature samples from Eq. (5.15) at random usage time τ_i between 0 and 100. The training health feature samples in healthy and faulty health states are marked as point and cross in Figure 5-8, respectively. The trained PHM models is plotted as the dotted in Figure 5-8.

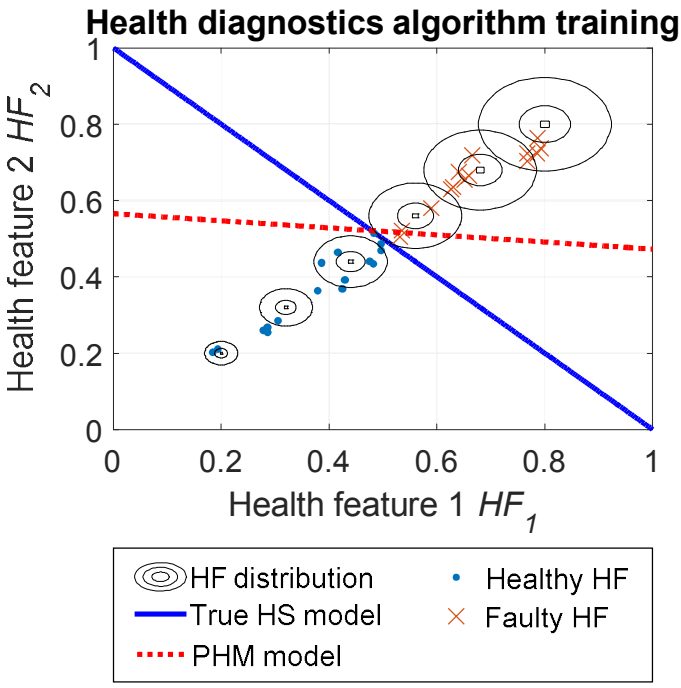


Figure 5-8 Models for numerical example

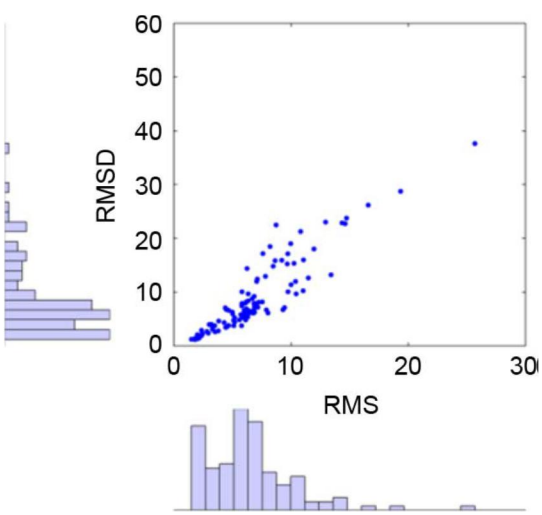


Figure 5-9 Health features of power transformers [59]

Based upon the assumed three models, time-dependent reliability, and time-dependent false and missed alarm rates can be calculated. In order to estimate three time-dependent probabilities, ten thousand health features samples are randomly generated at every life-cycle time step t_i using the health feature model. Based upon the true health state model and the PHM model, the health states of the generated health feature samples are estimated. According to the true and estimated health states, the health feature samples are counted into the health estimation matrix of Table 5-1. Then, three time-dependent probabilities are calculated using Eqs. (5.4), (5.5), and (5.6). The total life-cycle step N is set to 500 and its time interval Δt is set to 0.5.

The calculation results are shown Figure 5-10 and Figure 5-11. When the reliability is one at initial time steps in Figure 5-10, there are no faulty samples and so the missed alarm rate MA cannot be calculated (Eq. (5.5)). In terms of the total maintenance cost analysis, this is not a problem, since it is multiplied by a zero failure rate (=1-reliability) in the calculation of maintenance probabilities (Table 5-2). As the health feature distribution approaches the boundaries of the true health state model and the PHM model, the probabilities change. When the system is restored through corrective or the predictive maintenance, the usage time τ_i is initialized to zero and the probabilities go back to the initial state. In Figure 5-11, the corrective maintenance probability is higher than the other maintenance probabilities, as the missed alarm rate (the dotted line in Figure 5-10) is high. The incurred maintenance costs are one unnecessary maintenance (square marker), four corrective maintenance actions (cross markers), and one predictive maintenance (circle marker). Thus, the estimated total maintenance cost $C_{\mathrm{TFA}}^{\mathrm{M}}$ is

equal to $1 * c^{\mathrm{UM}} + 4 * c^{\mathrm{CM}} + 1 * c^{\mathrm{PM}}$. Assuming the costs of the three maintenance actions as $c^{\mathrm{UM}} = 100$, $c^{\mathrm{CM}} = 1000$, and $c^{\mathrm{PM}} = 300$, the $C_{\mathrm{TFA}}^{\mathrm{M}}$ is 4400.

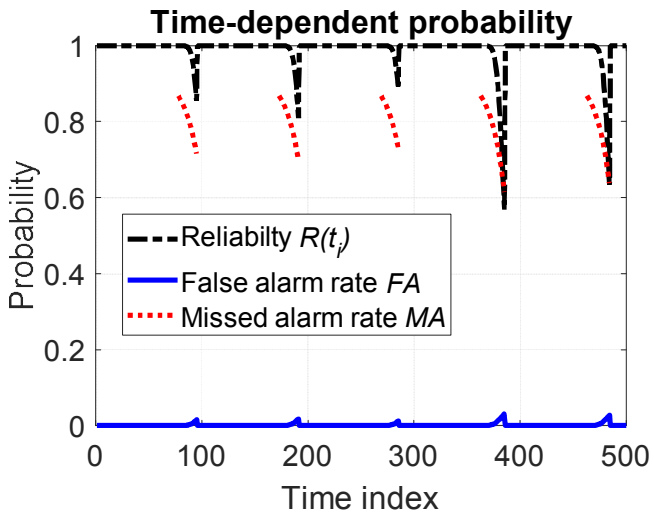


Figure 5-10 Time-dependent reliability, false alarm and missed alarm rates

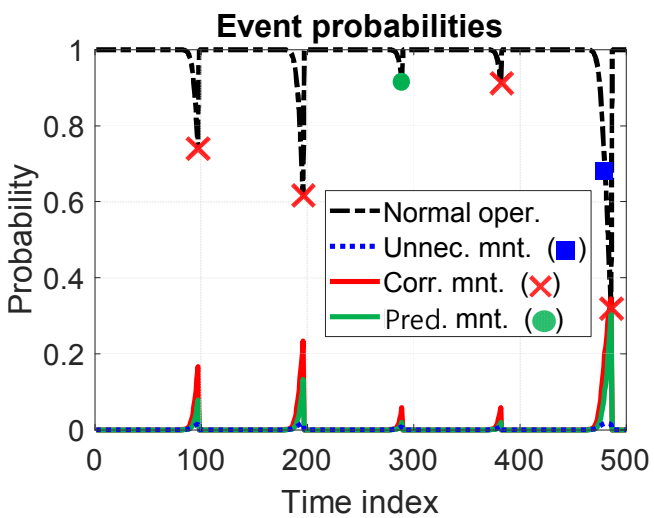


Figure 5-11 Calculated event probabilities and decided events

Figure 5-12 shows $C_{\mathrm{TFA}}^{\mathrm{M}}$ histograms from MCS with 1000 simulations. As false alarm rate is low and missed alarm rate is high (Figure 5-10) resulting high corrective maintenance probability (Figure 5-11). Thus $C_{\mathrm{TFA}}^{\mathrm{M}}$ mainly depends on the number of corrective maintenance occurrences, and its histogram disperses with the interval of the corrective maintenance cost ($c^{\mathrm{CM}} = 1000$).

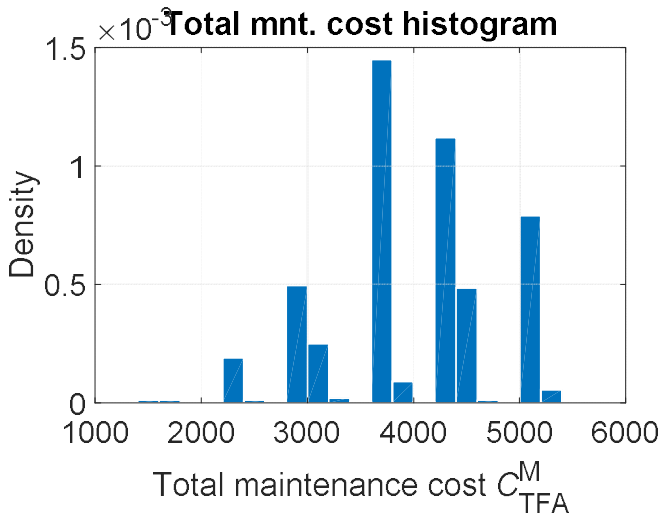


Figure 5-12 Histogram of total maintenance cost from life-cycle simulation

One of efficient ways to minimize $C_{\mathrm{TFA}}^{\mathrm{M}}$ is to adjust false and missed alarm weights. As discussed in Chapter 4.4.3, false and missed alarm weights denote the significances of false and missed alarm rates, and a PHM model is trained differently according to their values. Figure 5-13 shows the three standard deviation error bar of $C_{\mathrm{TFA}}^{\mathrm{M}}$ according to the false alarm weight w_{FA}. Increasing w_{FA} decreases the false alarm rate and increases the missed alarm rate. This makes $C_{\mathrm{TFA}}^{\mathrm{M}}$ converge to 5,000, which corresponds to the cost of five corrective maintenance events ($C_{\mathrm{TFA}}^{\mathrm{M}} = 5 * c^{\mathrm{CM}} = 5{,}000$). In contrast, decreasing w_{FA} increases the false alarm rate and decreases the missed alarm rate. This results in

$C_{\mathrm{TFA}}^{\mathrm{M}}$ decrease at first, as the costly corrective maintenance is reduced. Then, $C_{\mathrm{TFA}}^{\mathrm{M}}$ increases due to frequent, unnecessary maintenance. When w_1 becomes zero, $C_{\mathrm{TFA}}^{\mathrm{M}}$ converges to 50,000, which corresponds to the all-time unnecessary maintenance costs for the entire designed life-cycle ($C_{\mathrm{TFA}}^{\mathrm{M}} = 500 * c^{\mathrm{UM}} = 50{,}000$).

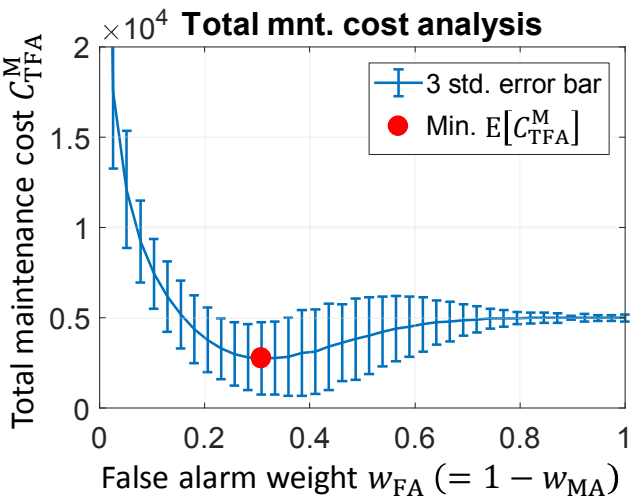


Figure 5-13 Error bar of total maintenance cost

Figure 5-14 compares the total maintenance costs according to false and missed alarm weights adjustment. When the mean total maintenance cost value ($\mathrm{E}[C_{\mathrm{TFA}}^{\mathrm{M}}]$) is minimized, the weight of two alarms are $w_{\mathrm{FA}} = 0.3077$ and $w_{\mathrm{MA}} = 0.6923$. This makes the false alarm rate increase and the missed FA rate decrease. Thus, $C_{\mathrm{TFA}}^{\mathrm{M}}$ arises from unnecessary and predictive maintenance costs instead of from corrective maintenance costs. As the costs of the two maintenance events are comparable ($c_{\mathrm{UM}} = 100, c_{\mathrm{PM}} = 300$) and smaller than c_{CM}, the histogram is not dispersed but instead it is gathered and distributed with smaller costs than that without the weight adjustment.

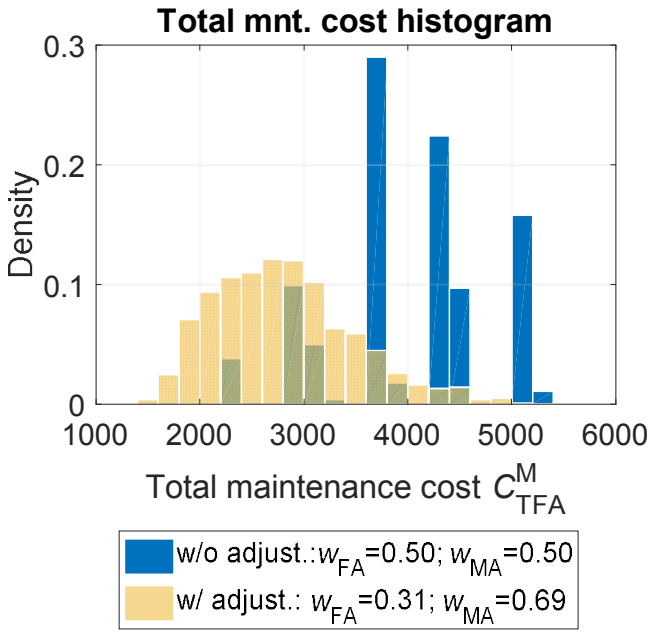


Figure 5-14 Histogram of total maintenance cost with alarm weight adjustment

From this numerical example, it is demonstrated that the life-cycle simulation is capable of estimating total maintenance cost considering time-dependent false and missed alarm rates. It analyzes system availability and incurred costs along with time in a probabilistic way. This helps a system operator to make an optimal maintenance planning such as spare part ordering, shutdown time, and restoration labor arrangement. Additionally, the analysis results can be utilized in modifying a system design and/or a PHM unit design properly as the false alarm weight optimization shown in this numerical example.

In this numerical example, some of parameters are assumed to be deterministic. In real applications, however, they can be uncertain. For example, maintenance costs (i.e., c_{UM}, c_{PM}, and c_{CM}) change due to wage increase, spare/repair part cost change, maintenance error, and so on. Initial health state

and its degradation are affected by manufacturing/assembly tolerance, initial defect, loading condition, and material property uncertainty. These parameter uncertainties result in unexpected $C_{\mathrm{TFA}}^{\mathrm{M}}$ change, which is not desirable for a system operator. Thus, it is required to test the robustness of $C_{\mathrm{TFA}}^{\mathrm{M}}$ in the presence of uncertainties. Regarding this issue, this research performed a sensitivity analysis of $C_{\mathrm{TFA}}^{\mathrm{M}}$ as an example. The uncertainty of three maintenance costs (i.e., c_{UM}, c_{PM}, and c_{CM}) and the fault diagnosis model with the adjusted false and missed alarm weights were considered. One-at-a-time approach was employed which is the most common approach that changes one input factor at a time and observes output factor change [138]. Figure 5-15 shows the sensitivity analysis chart of mean $C_{\mathrm{TFA}}^{\mathrm{M}}$ when changing each maintenance cost from 50% to 150%. It is shown that $C_{\mathrm{TFA}}^{\mathrm{M}}$ is more sensitive to c_{UM} and c_{PM} than c_{CM}. This is because unnecessary and predictive maintenances occur more frequently than corrective maintenance in the case of the fault diagnosis model with the adjusted false and missed alarm weights. This analysis result helps a system operator to make a proper maintenance plan in the presence of maintenance costs change.

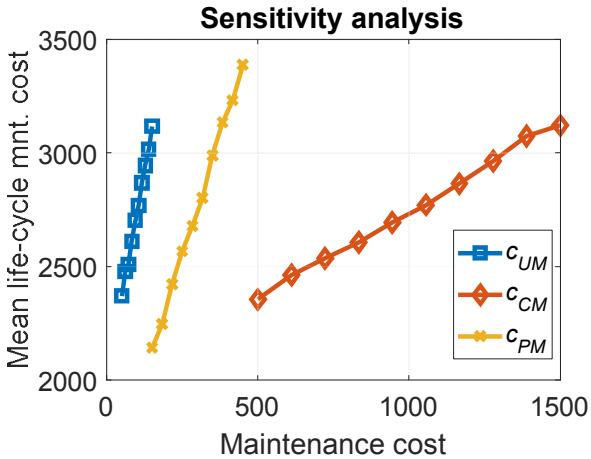


Figure 5-15 Sensitivity analysis results

5.3.2 Electro-Hydrostatic Actuator (EHA)

This case study aims at demonstrating the proposed RDSD-TFA by designing an electro-hydrostatic actuator (EHA) introduced in Chapter 3.2.2. In the following, an overall EHA model is described first, and then its design results is analyzed. Figure 5-16 shows the overall EHA models and variables for life-cycle cost estimation considering time-dependent false and missed alarm rates. Please refer this figure to comprehend the details below.

The design objective of this case study is to make EHA resilient against two failure modes, (1) disturbance control failure and (2) cross-line leakage failure, to minimize its life-cycle cost. The disturbance control failure occurs when the rod position control error exceeds pre-defined critical value. The rod position control error is the steady-state error of rod position as shown in Figure 4-4. This error occurs when actuator force fails to compensate external disturbance. The cross-line leakage failure mode is one of major problems degrades the performance of EHA. This occurs in a hydraulic cylinder mainly due to wear of a piston seal

and/or a ring, and results in position change delay and force reduction [98, 139, 140].

In order to simulate cross-line leakage failure, (1) the seal wear model and (2) the leakage coefficient model are used [98]. The wear model estimates the wear volume V_w due to squeezing stress and relative motion between a seal and cylinder piston surface.

$$V_w = \mu_w s \int_0^{t_w} |\dot{x}(t)| dt \tag{5.17}$$

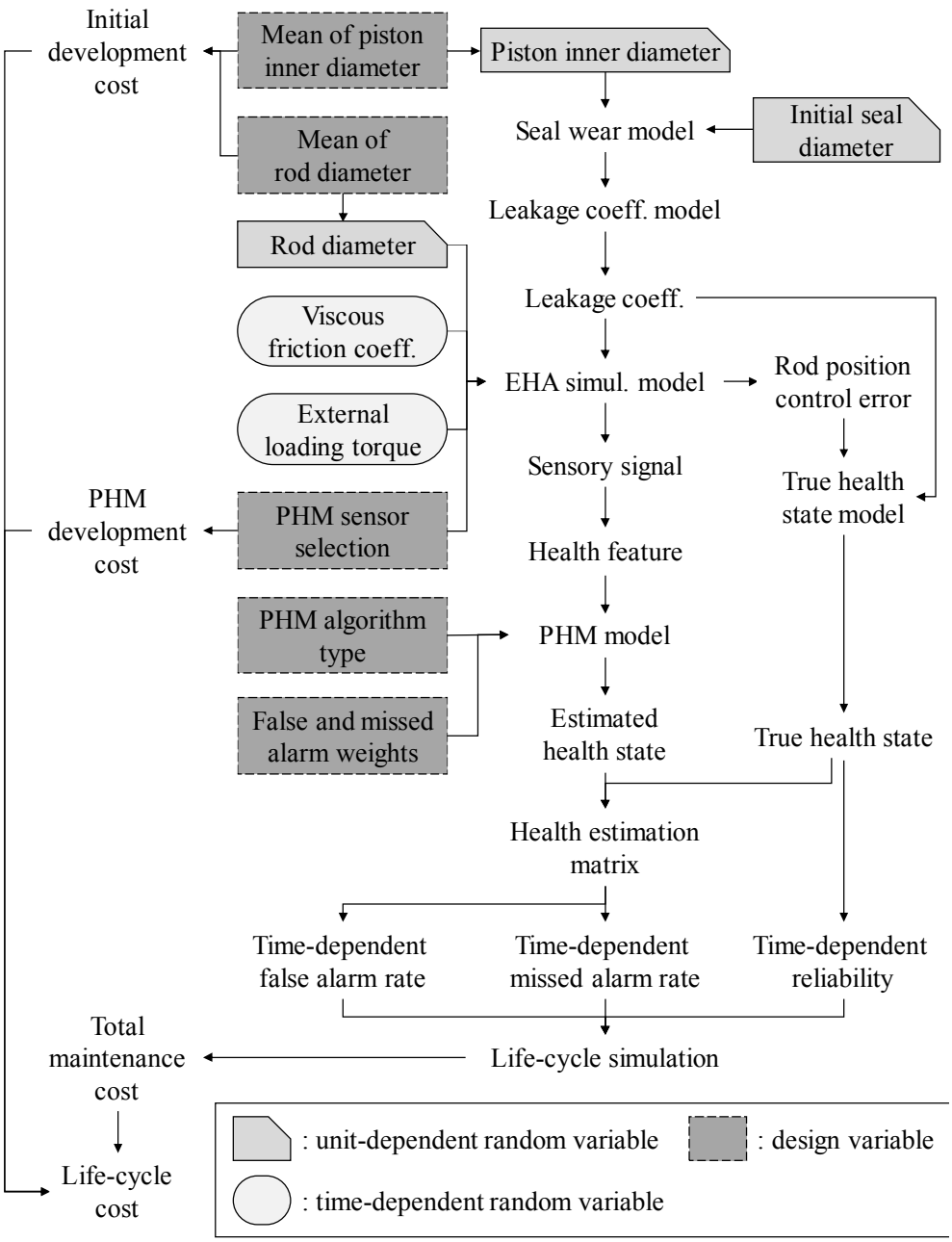


Figure 5-16 Overall EHA models and variables for life-cycle cost estimation

where μ_w is wear coefficient, s is squeezing stress acting on a seal, $\dot{x}(t)$ is the speed of relative motion between a seal and cylinder piston surface, and t_w is sliding time. This is based upon Archard equation that wear volume is proportional to the work done by frictional force [141]. The leakage coefficient model estimates leakage coefficient μ_{leak} for the leak rate caused by pressure drop and percolation channel [140].

$$\mu_{leak} = \mu_c \frac{h_\delta^3 l_y}{12\eta l_x} \tag{5.18}$$

where μ_c is percolation channel shape correction coefficient, h_δ is percolation channel height, l_y is the contact length of seal and cylinder, l_x is the contact width of seal and cylinder along axial direction, and η is working fluid viscosity. The percolation channel is caused by the roughness between seal and cylinder surfaces as shown in Figure 5-17.

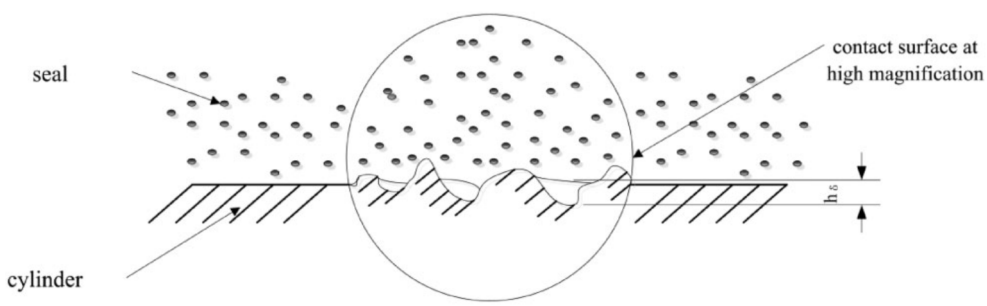


Figure 5-17 Percolation channels due to roughness of contact surface [98]

The progress of seal wear decreases contact pressure between seal and cylinder resulting the increase of percolation channel height h_δ. It also decrease the contact width of seal and cylinder l_x according to Hertzian theory. As a result, the change of leakage coefficient μ_{leak} over time can be estimated

through the wear model and the leakage coefficient model. The details of the models are omitted. For the detail of the models, please refer the references of [98, 139, 140].

For EHA design variables, the mean of piston diameter μ_{d_p}, and the mean of cylinder rod diameter μ_{d_r} are considered. They are key design variables deciding the performances of a hydraulic cylinder [11] as well as its volume related to manufacturing cost. They affect piston diameter d_p and rod diameter d_r respectively which are random due to manufacturing error. Figure 5-18 describes d_p and d_r with the schematic diagram of a hydraulic cylinder.

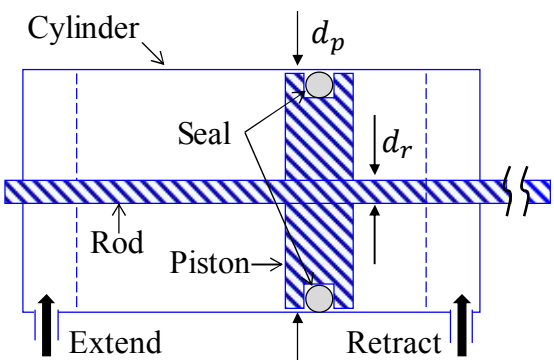


Figure 5-18 Schematic diagram of a hydraulic cylinder (double-acting)

The piston diameter d_p decides the contact length of seal and cylinder $l_y(=\pi d_r)$ in Eq. (5.18), and thus affects the seal wear and the leakage coefficient [98]. Thus, d_p should be minimized to increase reliability against cross-line leakage failure. However, this decreases effective rod end area $(=\frac{\pi}{4}(d_p^2 - d_r^2)$ reducing actuator force which is the product of effective rod end area and cylinder pressure. Thus, the rod position control error can increase.. The rod diameter d_r is also related to the effective rod end area $(=\frac{\pi}{4}(d_p^2 - d_r^2))$. The decrease in d_r increases the effective rod end area, and this reduces the rod

position control error. However, if the rod becomes too thin, applied stress increases and fracture can occur.

As noise variables, the initial diameter of a seal, external loading torque on EHA, and viscous friction coefficient of servomotor are considered. The initial seal diameter is random due to manufacturing error and this affects the seal wear and the leakage coefficient. The external loading torque varies according to operating condition causing rod position control error shown in Figure 4-4. The viscous friction coefficient changes randomly along with lubricant temperature [79].

The aforementioned variables are used as inputs for the EHA simulation model of LMS Imagine.Lab AMESim [97]. This simulates the actuator position request under disturbance: the rod displacement is requested to be 1 cm at 0.5 sec, and loading torque disturbance by the external load occurred at 2.0 sec as shown in Figure 3-4. The types of sensor signal outputs are determined by sensor selection, which is one of PHM design variables. The considered sensors are a rotary speed sensor (R), a cylinder rod displacement sensor (D), and a cylinder pressure sensor (P). The example of their responses are shown in Figure 3-4. The simulated signals from selected sensors are processed to health features according to Table 3-4 of which instances are shown in Figure 3-5.

The processed health features are used in PHM model which estimates the health state of EHA against cross-line leakage failure mode. The design variables of the PHM model are PHM algorithm type and the weights of false and missed alarms. For PHM algorithm, four classifier algorithms are considered: linear

discriminant analysis (LDA) classifier [99, 102], classification tree analysis [99], and weighted support vector machine (WSVM) [99, 102, 142, 143]. False and missed alarm weights determine the relative significances between false and missed alarm rates as shown in Chapter 4.4.3. They range from 0 to 1, and their summation is constrained to be 1.

In order to quantify the time-dependent probabilities, Monte Carlo simulation (MCS) is employed. It generates random samples according to the aforementioned design variables and random variables. Their randomness propagate through the models, and this results in randomness in the true and estimated health states of the samples. The estimated health state is evaluated by the PHM model, and the true health state is determined by the true health state model. The true health state model defines EHA as faulty when its rod position control error exceeds 0.2 cm or leakage coefficient exceeds 0.01 L/min/bar. According to the true and the estimated health states, the generated random samples are counted into the health estimation matrix of Table 5-1. Then, time-dependent false and missed alarm rates are calculated using Eqs. (5.4) and (5.5). The time-dependent reliability is calculated based upon the true health states of the samples using Eq. (5.6).

Based on the calculated time-dependent probabilities, the life-cycle simulation is performed to estimate the total maintenance cost $C_{\mathrm{TFA}}^{\mathrm{M}}$. In addition to the total maintenance cost, the initial development cost and the PHM development cost are required for estimating the life-cycle cost. The initial development cost is defined to be proportional to the material volume of the hydraulic cylinder as below.

$$C_{\mathrm{TFA}}^{\mathrm{I}} = c_c \cdot \left(V_r(d_r) + V_p(d_p) + V_c(d_r, d_p)\right)$$

$$\text{where } V_r(d_r) = 2 \cdot l_r \cdot \frac{\pi d_r^2}{4};\ V_p(d_p) = l_p \cdot \frac{\pi d_p^2}{4}; \tag{5.19}$$
$$V_c(d_r, d_p) = l_c \cdot \frac{\pi\left[\left(d_p + 2t_c\right)^2 - d_p^2\right]}{4} + 2t_c \cdot \frac{\pi\left[d_p^2 - d_r^2\right]}{4};$$

where c_c is the cost coefficient of a cylinder; l_p, l_r, and l_c are the length of a piston, a rod, and a cylinder respectively; d_p and d_r are the diameters of a piston and a rod respectively; t_c is the thickness of a cylinder. The PHM development cost is defined as total cost of the selected sensors.

$$C_{\mathrm{TFA}}^{\mathrm{PHM}} = c_{\mathrm{R}} \cdot I_{\mathrm{R}} + c_{\mathrm{D}} \cdot I_{\mathrm{D}} + c_{\mathrm{P}} \cdot I_{\mathrm{P}} \tag{5.20}$$

where I_k is an indicator function that is one if k-type sensor is used or otherwise zero; c_{R}, c_{D}, and c_{P} are the costs of a rotary speed sensor (R), a cylinder rod displacement sensor (D), and a cylinder pressure sensor (P) respectively. As a result, the life-cycle cost LCC_{MTFA} is calculated by adding $C_{\mathrm{TFA}}^{\mathrm{I}}$, $C_{\mathrm{TFA}}^{\mathrm{PHM}}$, and $C_{\mathrm{TFA}}^{\mathrm{M}}$ together (Eq. (5.8)).

Utilizing the above described models, the RDSD-TFA of EHA is conducted. The optimization problem is formulated as below.

$$\begin{aligned}
&\text{find} && \mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}} \\
&\text{where} && \mathbf{d}^{\mathrm{SYS}} = \left\{\mu_{d_p}, \mu_{d_r}\right\};\ \mathbf{d}^{\mathrm{PHM}} = \left\{\mathbf{d}_{\mathrm{sensor}}^{\mathrm{PHM}}, \mathbf{d}_{\mathrm{alg}}^{\mathrm{PHM}}, \mathbf{d}_{\theta}^{\mathrm{PHM}}\right\} \\
&&& \mathbf{d}_{\mathrm{sensor}}^{\mathrm{PHM}} = \{I_{\mathrm{R}}, I_{\mathrm{D}}, I_{\mathrm{P}}\};\ \mathbf{d}_{\mathrm{alg}}^{\mathrm{PHM}} = \{I_{\mathrm{LDA}}, I_{\mathrm{TREE}}, I_{\mathrm{WSVM}}\} \\
&&& \mathbf{d}_{\theta}^{\mathrm{PHM}} = \{w_{FA}, w_{MA}\} \\
&\text{minimize} && Q_{99}\left(LCC_{\mathrm{TFA}}\left(\mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}}\right)\right) \\
&\text{where} && LCC_{\mathrm{TFA}}\left(\mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}}\right)
\end{aligned} \tag{5.21}$$

$$= C_{\mathrm{TFA}}^{\mathrm{I}}\left(\mathbf{d}^{\mathrm{PHM}}\right) + C_{\mathrm{TFA}}^{\mathrm{PHM}}\left(\mathbf{d}^{\mathrm{PHM}}\right) + C_{\mathrm{TFA}}^{\mathrm{M}}\left(\mathbf{d}^{\mathrm{SYS}}, \mathbf{d}^{\mathrm{PHM}}\right)$$

$$\text{subject to} \quad 55 \leq \mu_{d_p} \leq 75;\ 15 \leq \mu_{d_r} \leq 35;\ \eta \cdot \mu_{d_p} \leq \mu_{d_r};$$
$$0 \leq w_{FA}, w_{MA} \leq 1;\ w_{FA} + w_{MA} = 1;$$

For the objective function of the optimization problem in Eq. (5.7) the 99% quantile function is used ($f_{obj}(LCC_{\mathrm{TFA}}) = Q_{99}(LCC_{\mathrm{TFA}})$). This objective helps to conservatively estimate life-cycle cost, and design EHA. The constraint of $\eta \cdot \mu_{d_p} \leq \mu_{d_r}$ is to avoid a weak rod relative to a piston where η is the critical rod-to-piston diameter ratio ($\eta = 1/3$). The parameters used in the models and the statistical information of random variables and are listed in Table 5-4 and Table 5-5. In Table 5-4, the random variables are categorized into two groups: unit-dependent and time-dependent. When a new EHA unit is introduced for first installation or replacement, its rod diameter, piston inner diameter, and initial seal diameter may differ from those of other units due to manufacturing error. These variables are assumed not to change over time, and called as unit-dependent random variables. Whereas, viscous friction coefficient and external loading torque change randomly over time due to randomness in operating condition; they are called as time-dependent random variables. In Table 5-5, the predictive and corrective and maintenance costs (i.e., c_{PM} and c_{CM}) are formulated as a function of the initial development costs $C_{\mathrm{TFA}}^{\mathrm{I}}$. This is based upon the assumption that a faulty EHA unit is replaced by a new EHA unit.

Table 5-4 Statistical information of random variables in RDSD-TFA of EHA

Random variables	Unit	Distribution		
		Type	Mean	Std. dev.*

Unit-dependent	Piston diameter d_p	mm	Normal	μ_{d_p}	0.3
	Rod diameter d_r	mm	Normal	μ_{d_r}	0.2
	Initial seal diameter	mm	Normal	3	0.05
Time-dependent	External loading torque	Nm	Normal	2000	400
	Viscous friction coefficient	Nm/rpm	Normal	1e-4	1e-5

* Std. dev.: standard deviation

Table 5-5 Parameters in RDSD-TFA of EHA

Parameters		**Value**
Initial development cost model	Cost coefficient c_c [1/mm^3]	110
	Piston length l_p [mm]	10
	Rod length l_r [mm]	60
	Cylinder length l_c [mm]	80
	Cylinder thickness t_c [mm]	10
PHM development cost model	Rotary speed sensor cost c_R	150
	Displacement sensor cost c_D	150
	Pressure sensor cost c_P	150
Maintenance cost model	Unnecessary maintenance cost c^{UM}	100
	Predictive maintenance cost c^{PM}	$C_{\mathrm{TFA}}^{\mathrm{I}}$
	Corrective maintenance cost c^{CM}	1000+$C_{\mathrm{TFA}}^{\mathrm{I}}$
Uncertainty quantification	The number of random samples for time-dependent probability estimation using health estimation matrix	1000
	The number of life-cycle simulation	300
Life-cycle simulation	The number of total life-cycle time steps N	500
	Time interval between the adjacent life-cycle time steps Δt	1

In order to show the importance of time-dependent false and missed alarm rates, and the effectiveness of the proposed RDSD-TFA, it is desirable to compare the design results from RDSD-TFA and RDSD-FA. But the comparison is infeasible because they are different in terms of total maintenance cost formulation. RDSD-TFA performs life-cycle simulation which estimates the number of maintenance occurrences even after its health restoration as shown in Figure 5-11. This enables to calculates total maintenance cost as the sum of incurred maintenance costs (see Eq. (5.9)). Whereas, RDSD-FA cannot estimate the number of maintenance occurrences, and estimates the expectation value of total maintenance cost (see Eqs. (4.12)-(4.15)). As a result, two cost models are different and it is impossible to compare them.

Instead of comparing design results from RDSD-TFA and RDSD-FA, the designs of initial, RDSD-TFA without PHM, and RDSD-TFA with PHM are compared as shown in Table 5-6. This helps to show how RDSD-TFA minimize life-cycle cost by assigning resilience, i.e., reliability and restoration, on an engineered system. The reliability is controlled by modifying system design variables $\mathbf{d}^{\mathrm{SYS}}$, and the restoration is realized by designing PHM design variables $\mathbf{d}^{\mathrm{PHM}}$. In order to solve the design optimization problem of Eq. (5.21), a genetic algorithm (GA) was used which can handle both discrete and continuous design variables. In order to find near-global minimum solution, the optimization was performed ten times repeatedly. The initial development cost $C_{\mathrm{TFA}}^{\mathrm{I}}$, the total maintenance cost $C_{\mathrm{TFA}}^{\mathrm{M}}$ and the life-cycle cost LCC_{TFA} are random due to the random variables, and thus their objective values (i.e., $Q_{99}(\cdot)$) are listed. As $Q_{99}(LCC_{\mathrm{TFA}})$ is $Q_{99}\left(C_{\mathrm{TFA}}^{\mathrm{I}} + C_{\mathrm{TFA}}^{\mathrm{PHM}} + C_{\mathrm{TFA}}^{\mathrm{M}}\right)$, this can slightly

different from the sum of $Q_{99}(C_{\mathrm{TFA}}^{\mathrm{I}})$, $C_{\mathrm{TFA}}^{\mathrm{PHM}}$, and $Q_{99}(C_{\mathrm{TFA}}^{\mathrm{M}})$. The detail analysis regarding Table 5-6 is described below.

Table 5-6 Optimal design variables and resulting costs

Hydraulic cylinder design		Initial	RDSD-TFA	
			w/o PHM	w/ PHM
$\mathbf{d}^{\mathrm{SYS}}$	μ_{d_p} [mm]	65	71	71
	μ_{d_r} [mm]	25	28	28
$\mathbf{d}^{\mathrm{PHM}}$	$\mathbf{d}_{\mathrm{sensor}}^{\mathrm{PHM}} = [I_{\mathrm{R}}\ I_{\mathrm{D}}\ I_P]$	[0 0 0]	[0 0 0]	[1 0 1]
	$\mathbf{d}_{\mathrm{alg}}^{\mathrm{PHM}} = [I_{\mathrm{LDA}}\ I_{\mathrm{TREE}}\ I_{\mathrm{WSVM}}]$	[0 0 0]	[0 0 0]	[0 0 1]
	w_{FA}	-	-	0.225
	w_{MA}	-	-	0.775
Cost	$Q_{99}(C_{\mathrm{TFA}}^{\mathrm{I}})$	303.323	345.366	345.484
	$C_{\mathrm{TFA}}^{\mathrm{PHM}}$	0	0	300
	$Q_{99}(C_{\mathrm{TFA}}^{\mathrm{M}})$	18246.521	4036.097	1437.125
	$Q_{99}(LCC_{\mathrm{TFA}})$	18549.383	4386.100	2085.467

In order to resolve this reliability issue, RDSD-TFA increased both mean values of piston and rod diameter (i.e., μ_{d_p} and μ_{d_r}). This reduced the control error as the dotted line in Figure 5-19, and EHA has no failure until about 130 usage time steps as shown in Figure 5-20. As a result, the number of corrective maintenances was significantly reduced by three as shown in Figure 5-21. The other maintenance probabilities are zero because PHM is not implemented. In terms of costs, the initial development cost was increased by 13.86% (303.323 → 345.366) and the total maintenance cost was reduced by 77.88% (18246.521 → 4036.097).

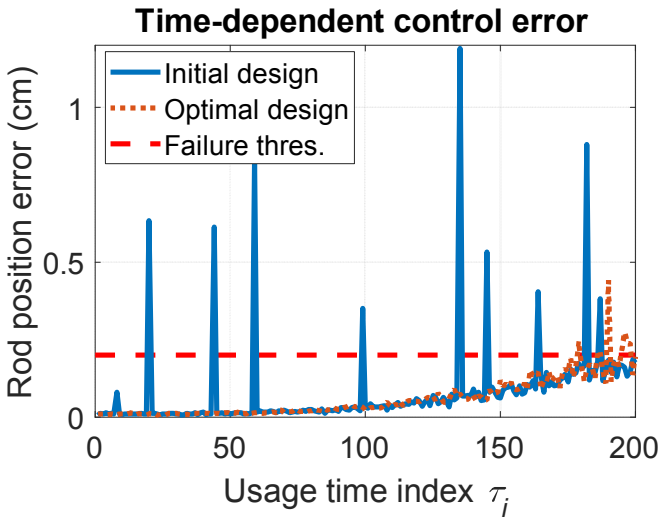


Figure 5-19 Time-dependent rod position control error of EHA

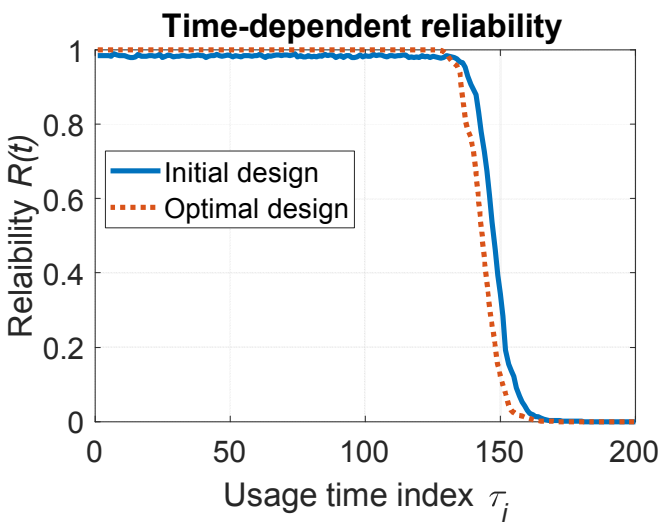


Figure 5-20 Time-dependent reliability of EHA

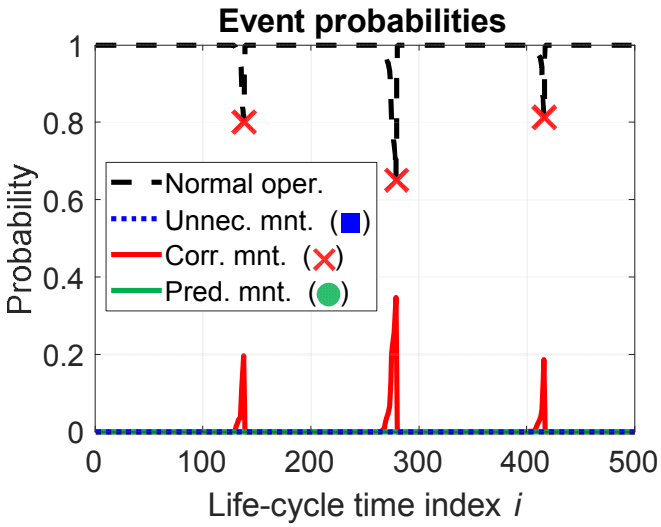


Figure 5-21 Event probabilities of the design by RDSD-TFA without PHM

In Figure 5-20, meanwhile, the reliability of the optimal design was decreased faster than that of the initial design. This is because of the increase in the piston diameter. As explained above, the increase in the piston diameter raised the contact length of seal and cylinder $l_y(=\pi d_r)$ in Eq. (5.18). This resulted in larger leakage coefficient as well as greater seal wear. Thus, the cross-line leakage coefficient increased faster and the reliability decreased faster than those of the initial design. Figure 5-22 shows the randomly generated samples of time-dependent cross-line leakage coefficients from the initial and the optimal designs. The leakage coefficients of the optimal design reached the failure threshold earlier, and thus its reliability degraded faster than that of the initial design as Figure 5-20.

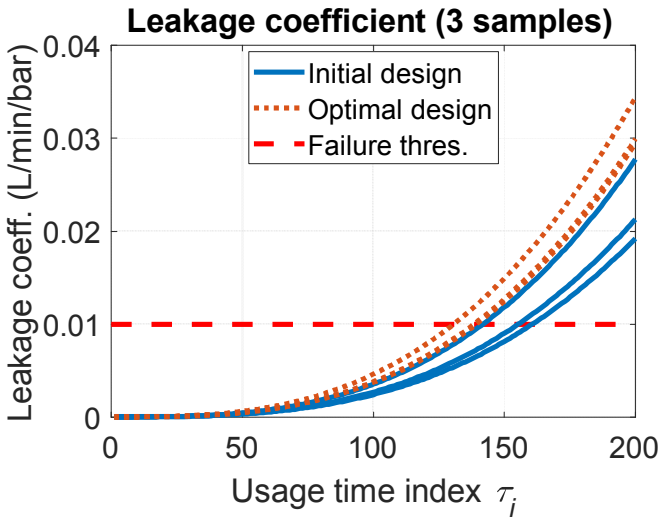


Figure 5-22 Time-dependent cross-line leakage coefficient of EHA

For PHM design variables $\mathbf{d}^{\mathrm{PHM}}$, RDSD-TFA resulted in selecting two sensors of the rotary speed sensor (R) and the cylinder pressure sensor (P). The rotary speed sensor (R) is effective to diagnose cross-line leakage failure (see Figure 3-5 (a)), and the pressure sensor (P) can analyze the uncertainty of health features from external disturbance (see Figure 3-5 (c)). The reason for excluding the cylinder rod displacement sensor (D) is that the health feature from D sensor is highly correlated with that from R sensor as shown in Figure 3-5 (e) (Pearson correlation coefficient ρ_{Pearson}=−0.9910). For the PHM algorithm, the weighted support vector machine (WSVM) with the lowest total maintenance cost was selected. Its false and missed alarm weights, w_{FA} and w_{MA}, were optimized as 0.225 and 0.775 to reduce missed alarm rates resulting costly corrective maintenance.

As a result of PHM design, the corrective maintenances were replaced with the unnecessary and predictive maintenances as shown in Figure 5-23. The

corrective maintenance probability was decreased to zero, and other probabilities were increased. This PHM implementation reduced the total maintenance cost by 64.39% (4036.097 → 1437.125), but caused the PHM development cost of 300 from employing two sensors (i.e., R and P sensors).

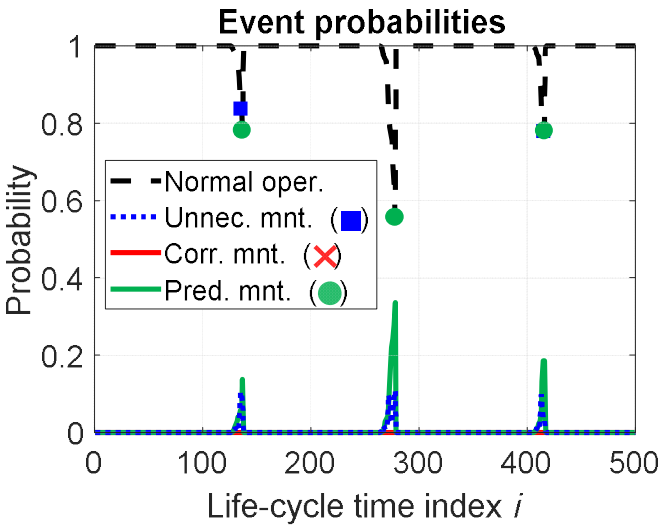


Figure 5-23 Event probabilities of the design by RDSD-TFA with PHM

The overall effectiveness of RDSD-TFA is shown in Figure 5-24. This figure shows the one standard deviation error bar of maintenance occurrences. It is noted that the costly corrective maintenance was eliminated via the two properties of resilience: reliability and restoration. The reliability was improved by adjusting system design variables $\mathbf{d}^{\mathrm{SYS}}$, and the number of system failures (i.e., corrective maintenances) was reduced. The restoration property was realized by designing PHM design variables $\mathbf{d}^{\mathrm{PHM}}$, and the system failures were totally prevented. In assigning this resilience property, the initial development cost $C_{\mathrm{TFA}}^{\mathrm{I}}$ and the PHM development cost $C_{\mathrm{TFA}}^{\mathrm{PHM}}$ were increased, and the total maintenance cost $C_{\mathrm{TFA}}^{\mathrm{M}}$ was significantly decreased.

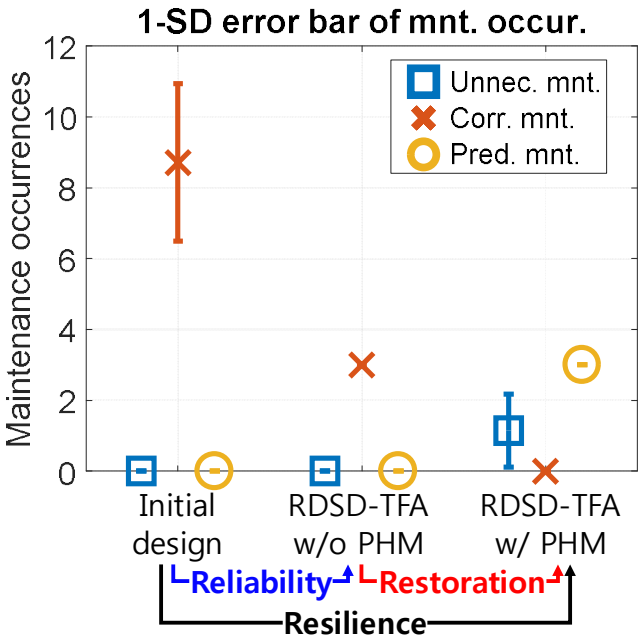


Figure 5-24 Error bar of maintenance occurrences

As a result, RDSD-TFA reduced the 99% quantile of life-cycle cost $Q_{99}(LCC_{TFA})$ by 88.76% compared to that of the initial design. Figure 5-25 shows the histogram of life-cycle costs. The initial design life-cycle cost is widely distributed as its corrective maintenance occurrences are quite random as Figure 5-24. The life-cycle cost of the deign from RDSD-TFA with PHM is dispersed with the interval of the unnecessary maintenance cost ($c^{\mathrm{UM}} = 100$).

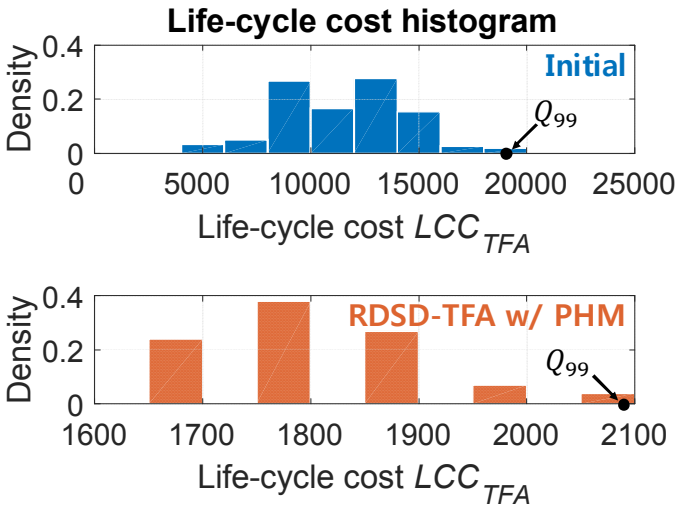


Figure 5-25 Histogram of life-cycle cost

5.4 Summary and Discussion

Resilience-driven system design (RDSD) aims at designing an engineered system to be resilient by cohesively incorporating reliability-based design optimization (RBDO), and prognostics and health management (PHM) design. The resilient engineered system can maintain its performance by resisting and recovering against adverse events. As a result, this helps to enhance system availability and reduces life-cycle cost.

However, conventional RDSD is of two major limitations. First, it does not consider time-dependent variability of an engineered system. As an engineered system deteriorates, its reliability, false alarm rate, missed alarm rate, and resilience also change. But, these are regarded as time-independent or static in conventional RDSD. Second, there is no systematic approach to determine target resilience level. RDSD optimizes design variables to satisfy target resilience

level. Thus, the design result of RDSD depends on target resilience level, and its determination is one of most important concerns. However, there is no research regarding its determination.

In order to resolve these two limitations, this chapter proposed RDSD considering time-dependent false alarms (RDSD-TFA). In order to incorporate systems' time-dependent variability, time-dependent false and missed alarm rates are newly proposed, and life-cycle simulation method is adopted. And the target resilience constraint is eliminated, and its optimality is evaluated in terms of life-cycle cost instead. The framework of RDSD-TFA is different from that of conventional RDSD, and consists of four tasks: system analysis, PHM analysis, life-cycle simulation, and design optimization.

Table 5-7 lists the differences between RDSD-FA and RDSD-TFA. Compared to conventional RDSD, RDSD-TFA can estimate life-cycle cost accurately and rigorously without concerning target resilience constraint. However, it is of greater computational cost to analyze an engineered system in time-domain. And, it requires many information to analyze and model the time-dependent characteristics of an engineered system. Thus, it is recommended to select the adequate design method according to given information and computing power.

Table 5-7 Comparison of RDSD-FA and RDSD-TFA

	RDSD-FA	RDSD-TFA
Pros	- Fast design optimization via hierarchical framework - No need for time-dependent variable information	- Accurate and rigorous life-cycle cost estimation - No target resilience constraint
Cons	- Inaccurate life-cycle cost estimation - Subjective issue of determining target resilience level	- High computational cost - Need for time-dependent variable information

Chapter 6. Conclusions

6.1 Summary and Contributions

In this dissertation, an advanced resilience engineering considering false alarms has been proposed that analyzes and designs a resilient engineered system in an accurate and rigorous manner. This consists of three research thrusts: 1) resilience analysis considering false alarms, 2) resilience-driven system design considering false alarms (RDSD-FA), and 3) resilience-driven system design considering time-dependent false alarms (RDSD-TFA). The contributions and significance of the research are summarized as follows.

Contribution 1: Accurate Estimation of System Resilience Considering False Alarms

In this dissertation, a resilience measure is newly formulated to consider false alarms. According to conditional probability theory, false alarm rate as well as missed alarm rate are quantified using a uncertainty propagation method and health estimation matrix. Based upon the analysis on resilience scenarios, the new resilience measure is formulated in a probabilistic manner. This consists of a passive survival rate and a proactive survival rate, and can evaluate system availability loss due to both false and missed alarms.

The conventional resilience measure does not consider resilience loss due to false alarms, and can estimate system resilience larger than actual. This inaccurate estimation results in unexpected system unavailability with social and financial loss. Whereas, the new resilience measure considering false alarms can

accurately estimate system resilience. In addition, the new measure facilitates resilience analysis of on-site operating systems while still being applicable to the design of new resilient systems with minimized life-cycle cost. The proposed resilience measure is expected to help a system operator as well as a designer to make a decision on an engineered system. The system operator refers system resilience in estimating system availability, and makes an adequate maintenance plan (e.g., spare part ordering, shutdown time, restoration labor arrangement) to minimize operation and maintenance costs. The system designer analyzes the causes of low system resilience (e.g., low reliability, high false alarm rate, or high missed alarm rate), and suggests a way to retain required system resilience in a cost-effective manner.

Contribution 2: Advances in Resilience-Driven System Design Considering False Alarms (RDSD-FA)

Second contribution is to advance a resilience-driven system design framework by considering false alarms (RDSD-FA). This designs a complex engineered system to satisfy target resilience level while minimizing its life-cycle cost. The framework consists of three hierarchical optimization problems: resilience allocation problem (RAP), reliability-based design optimization (RBDO), and prognostics and health management (PHM) design. RAP allocates target performance values (reliability, false alarm rate, and missed alarm rate) to RBDO and PHM design. RBDO designs an engineered system to satisfy the allocated target reliability while minimizing initial development cost. PHM design optimizes the PHM unit configuration to satisfy the allocated false and missed alarm rates while minimizing PHM development cost and total

maintenance cost.

The previous RDSD does not consider false alarms, and a designed engineered system is of insufficient resilience and prone to false alarm problems. This makes the system unavailable resulting unexpected financial loss. Whereas RDSD-FA considers false alarms, and allocates appropriate target performance values to satisfy target resilience level. And, a PHM unit is designed specifically to manage false alarm problems as well as missed alarm problems. As a result, the designed system can fulfill the expected target resilience, and maintain its performance with minimized life-cycle cost.

Contribution 3: Development of Resilience-Driven System Design Considering Time-Dependent False Alarms (RDSD-TFA)

Third contribution is to develop a resilience-driven system design framework considering time-dependent false alarms (RDSD-TFA). This considers time-dependent variability of an engineered system, and analyzes time-dependent variables and probabilities. RDSD-TFA aims at designing an resilient engineered system to minimize its life-cycle cost. The framework of RDSD-TFA consists of four tasks: system analysis, PHM analysis, life-cycle simulation, and design optimization. The system analysis evaluates initial development cost and analyzes the degree of health degradation in terms of time-dependent reliability and sensory signal changes. The PHM analysis calculate PHM development cost and estimates time-dependent false and missed alarm rates using sensory signals from the system analysis. The life-cycle simulation analyzes time-dependent event probabilities and total maintenance costs based upon the estimated time-

dependent probabilities (i.e., reliability, false alarm rate, and missed alarm rate). The design optimization calculate life-cycle cost by adding three costs, and updates system design variables and PHM design variables until the convergence to the minimal life-cycle cost.

In RDSD-FA, reliability, false and missed alarm rates, and resilience are considered to be time-independent or static. This regarding results in inaccurate life-cycle cost estimation, and thus exposes the designed system to unexpected financial loss. Whereas, RDSD-TFA considers considering the time-dependent variability of an engineered system, and estimates life-cycle cost in an accurate and rigorous manner. This helps to design an engineered system more precisely to minimize the life-cycle cost. In addition, one of major concerns in RDSD-FA is to determine target resilience level. According to its value, the design of system and life-cycle cost are changed. RDSD-TFA resolves this issue by eliminating a resilience constraint function. Instead, it evaluates the optimality of target resilience value in terms of life-cycle cost minimization.

6.2 Suggestions for Future Research

This dissertation is elaborated to advance resilience engineering by considering false alarms. But there still exist several issues to be solved for the maturing of resilience engineering further. The details of the issues are listed as follows.

Issue 1: Diversity of resilience measure

In current engineering field, the definition and metric of resilience are not unified. Whenever researchers attempt to apply resilience engineering, they have

to compare and find out which resilience metric is suitable among many resilience measures. In order to solve this problems, it is necessary to suggest the general concept of resilience as well as its metric.

Issue 2: Computational cost in false and missed alarm quantification

In order to quantify false and missed alarm rates, sampling-based uncertainty propagation method is employed. This method is generally applicable to various problems and has high accuracy, but requires high computational cost. In order to analyze system resilience as well as design a resilient engineered system, a computationally efficient quantification method for false and missed alarm rates is required.

Issue 3: Computational cost of design optimization

Designing a resilient engineered systems necessitates high computational cost due to numerous variables including system design variable, PHM design variable, and random variable. In RDSD-TFA, this computational cost will be much higher as it considers system variability over time. Therefore, it is required to make RDSD-FA and RDSD-TFA time-efficient.

Issue 4: Difficulties in parameter setting

In RDSD-FA and RDSD-TFA, there are many parameters to be determined such as cost model parameters, maintenance costs, and target total life-cycle time. They highly affect the design results, and thus should be determined carefully. Regarding cost-related parameters, they would be uncertain due to parameters

estimation uncertainty, deficiency of supply chain for spare parts, shutdown time uncertainty, inspection and maintenance error, net discount rate of money, and so on [144, 145]. The guideline to determine adequate parameters and the consideration of uncertainties in cost-related parameters need to be investigated.

Issue 5: Other infant mortality failure

There are mainly three types of failures in life-cycle of an engineered system: infant mortality failure, constant or random failure, and wear out failure [146]. Among them, the infant mortality failure is not considered in this study. This occurs due to factors which are not considered in design stage such as design blunder, manufacturing defects, transportation error, and installation error. The infant mortality failure result in high failure rate at early operation stage or burn-in stage. Thus, this needs to considered in future works to design a resilient engineered system in a rigorous and accurate manner.

References

1. The real cost of power outages and unplanned industrial downtime, http://www.trinitypower.com/real-cost-power-outages-unplanned-industrial-downtime/; 11 November 2017.

2. Blackout Tracker - United States Annual Report 2016. Eaton; 2016

3. Karen Bain, David G. Orwig. F/A-18E/F Built-in-test (BIT) Maturation Process. National Defense Industrial Associated 3rd Annual systems Engineering & Supportability Conference: Citeseer; 2000.

4. Samir Khan, Paul Phillips, Ian Jennions, Chris Hockley. No Fault Found events in maintenance engineering Part 1: Current trends, implications and organizational practices. Reliab Eng Syst Saf. 2014;123:183-95.

5. Samir Khan, Paul Phillips, Chris Hockley, Ian Jennions. No Fault Found events in maintenance engineering Part 2: Root causes, technical developments and future research. Reliab Eng Syst Saf. 2014;123:196-208.

6. Israel Beniaminy, David Joseph. Reducing the "No Fault Found" problem: Contributions from expert-system methods. Proceedings, IEEE Aerospace Conference2002. p. 6-2971-6-3.

7. Debra Werner. A maddening, costly problem. Aerosp Am. 2015;53:28-33.

8. Online etymology dictionalry, http://www.etymonline.com/index.php?term=resilience; 21 August 2016.

9. Kate H Orwin, David A Wardle. New indices for quantifying the resistance and resilience of soil biota to exogenous disturbances. Soil Biol Biochem. 2004;36:1907-12.

10. Lino Briguglio, Gordon Cordina, Nadia Farrugia, Stephanie Vella. Economic vulnerability and resilience: concepts and measurements. Oxford development studies. 2009;37:229-47.

11. Byeng D. Youn, Chao Hu, Pingfeng Wang. Resilience-Driven System Design of Complex Engineered Systems. Journal of Mechanical Design. 2011;133.

12. Erik Hollnagel, David Woods, Nancy Leveson. Resilience Engineering : Concepts and Precepts2006.

13. Gian Paolo Cimellaro, Daniele Solari, Michel Bruneau. Physical infrastructure interdependency and regional resilience index after the 2011 Tohoku earthquake in Japan. Earthquake Eng Struct Dyn. 2014;43:1763-84.

14. Bilal M. Ayyub. Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision Making. Risk Anal. 2014;34:340-55.

15. Seyedmohsen Hosseini, Kash Barker, Jose E. Ramirez-Marquez. A review of definitions and measures of system resilience. Reliab Eng Syst Saf. 2016;145:47-61.

16. Nita Yodo, Pingfeng Wang. Engineering Resilience Quantification and System Design Implications: A Literature Survey. Journal of Mechanical Design. 2016;138:111408--13.

17. Junxuan Li, Zhimin Xi. Engineering Recoverability: A New Indicator of Design for Engineering Resilience. ASME 2014 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference: American Society of Mechanical Engineers; 2014. p. V02AT3A044-V02AT03A.

18. Zhen Hu, Sankaran Mahadevan. Resilience Assessment Based on Time-Dependent System Reliability Analysis. Journal of Mechanical Design. 2016;138:111404--3.

19. Hans Janssen. Monte-Carlo based uncertainty analysis: Sampling efficiency and sampling convergence. Reliab Eng Syst Saf. 2013;109:123-32.

20. Zhe Zhang, Chao Jiang, Gary Wang, Xu Han. First and second order approximate reliability analysis methods using evidence theory. Reliab Eng Syst Saf. 2015;137:40-9.

21. Jongmin Lim, Byungchai Lee, Ikjin Lee. Second-order reliability method-based inverse reliability analysis using Hessian update for accurate and efficient reliability-based design optimization. International Journal for Numerical Methods in Engineering. 2014;100:773-92.

22. Zhen Hu, Xiaoping Du. First order reliability method for time-variant problems using series expansions. Structural and Multidisciplinary Optimization. 2014;51:1-21.

23. Byeng D. Youn, Pingfeng Wang. Bayesian reliability-based design optimization using eigenvector dimension reduction (EDR) method. Structural and Multidisciplinary Optimization. 2008;36:107-23.

24. Byeng D. Youn, Zhimin Xi. Reliability-based robust design optimization using the eigenvector dimension reduction (EDR) method. Structural and Multidisciplinary Optimization. 2009;37:475-92.

25. Zhou Changcong, Lu Zhenzhou, Zhang Feng, Yue Zhufeng. An adaptive reliability method combining relevance vector machine and importance sampling. Structural and Multidisciplinary Optimization. 2015;52:945-57.

26. Chao Hu, Byeng D. Youn, Heonjun Yoon. An adaptive dimension decomposition and reselection method for reliability analysis. Structural and Multidisciplinary Optimization. 2013;47:423-40.

27. Pingfeng Wang, Zequn Wang, Byeng D. Youn, Soobum Lee. Reliability-based robust design of smart sensing systems for failure diagnostics using piezoelectric materials. Computers & Structures. 2015;156:110-21.

28. Pingfeng Wang, Byeng D. Youn, Chao Hu, Jong Moon Ha, Byung Chul Jeon. A probabilistic detectability-based sensor network design method for system health monitoring and prognostics. Journal of Intelligent Material

Systems and Structures. 2014;26:1079-90.

29. Marine Jouin, Rafael Gouriveau, Daniel Hissel, Marie-Cécile Péra, Noureddine Zerhouni. Particle filter-based prognostics: Review, discussion and perspectives. Mechanical Systems and Signal Processing. 2016;72–73:2-31.

30. Abhinav Saxena, Jose Celaya, Edward Balaban, Kai Goebel, Bhaskar Saha, Sankalita Saha, et al. Metrics for evaluating performance of prognostic techniques. 2008 International Conference on Prognostics and Health Management2008. p. 1-17.

31. Raúl Baños, Juan Reca, Juan Martínez, Consolación Gil, Antonio L. Márquez. Resilience Indexes for Water Distribution Network Design: A Performance Analysis Under Demand Uncertainty. Water Resour Manage. 2011;25:2351-66.

32. Kalyan R. Piratla. Investigation of sustainable and resilient design alternatives for water distribution networks. Urban Water Journal. 2016;13:412-25.

33. Yanglin Gong. Analysis and design for the resilience of shear connections. Canadian Journal of Civil Engineering. 2010;37:1581-9.

34. Shabnam Rezapour, Reza Zanjirani Farahani, Morteza Pourakbar. Resilient supply chain network design under competition: A case study. European Journal of Operational Research. 2017;259:1017-35.

35. Sonia Mari, Young Lee, Muhammad Memon. Sustainable and Resilient Supply Chain Network Design under Disruption Risks. Sustainability. 2014;6:6666.

36. Pradeep M. Hettiarachchi, Nathan Fisher, Masud Ahmed, Le Yi Wang, Shinan Wang, Weisong Shi. A Design and Analysis Framework for Thermal-Resilient Hard Real-Time Systems. ACM Trans Embed Comput Syst. 2014;13:1-25.

37. Chris Sweetapple, Guangtao Fu, David Butler. Reliable, Robust, and Resilient System Design Framework with Application to Wastewater-Treatment Plant Control. J Environ Eng. 2017;143:04016086.

38. Anoop K. Dhingra. Optimal apportionment of reliability and redundancy in series systems under multiple objectives. IEEE Transactions on Reliability. 1992;41:576-82.

39. Frank A. Tillman, Ching-Lai Hwang, Way Kuo. Determining Component Reliability and Redundancy for Optimum System Reliability. IEEE Transactions on Reliability. 1977;R-26:162-5.

40. Byeng D. Youn, Chao Hu, Pingfeng Wang, Joung Taek Yoon. Resilience Allocation for Resilient Engineered System Design. Journal of Institute of Control, Robotics and Systems. 2011;17:1082-9.

41. Nita Yodo, Pingfeng Wang. Resilience Allocation for Early Stage Design of Complex Engineered Systems. Journal of Mechanical Design.

2016;138:091402--10.

42. Akomeno Omu, Ruchi Choudhary, Adam Boies. Distributed energy resource system optimisation using mixed integer linear programming. Energy Policy. 2013;61:249-66.

43. Ryohei Yokoyama, Yuji Shinano, Syusuke Taniguchi, Masashi Ohkura, Tetsuya Wakui. Optimization of energy supply systems by MILP branch and bound method in consideration of hierarchical relationship between design and operation. Energy Conversion and Management. 2015;92:92-104.

44. Xin-She Yang. Review of meta-heuristics and generalised evolutionary walk algorithm. Int J Bio-Inspired Comput. 2011;3:77-84.

45. Mirko Stojiljković, Mladen Stojiljković, Bratislav Blagojević. Multi-Objective Combinatorial Optimization of Trigeneration Plants Based on Metaheuristics. Energies. 2014;7:8554.

46. R.J. Eggert. Quantifying design feasibility using probabilistic feasibility analysis. 1991 ASME Advances in Design Automation1991. p. 235-40.

47. Po Ting Lin, Hae Chang Gea, Yogesh Jaluria. A modified reliability index approach for reliability-based design optimization. Journal of Mechanical Design. 2011;133:044501.

48. Byeng D. Youn, Kyung K Choi, Liu Du. Enriched performance measure approach for reliability-based design optimization. AIAA J. 2005;43:874-

84.

49. Y-T Wu, Youngwon Shin, Robert Sues, Mark Cesare. Safety-factor based approach for probability-based design optimization. 19th AIAA Applied Aerodynamics Conference2001. p. 1522.

50. Xiaoping Du, Wei Chen. Sequential optimization and reliability assessment method for efficient probabilistic design. Journal of Mechanical Design. 2004;126:225-33.

51. T. Zou, Sankaran Mahadevan. A direct decoupling approach for efficient reliability-based design optimization. Structural and Multidisciplinary Optimization. 2006;31:190-200.

52. Xiaoguan Chen, Timothy K Hasselman, Douglas J Neill. Reliability based structural design optimization for practical applications. Proceedings of the 38th AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics, and materials conference1997. p. 2724-32.

53. Byeng D. Youn, Kyung K. Choi, Young H. Park. Hybrid analysis method for reliability-based design optimization. Journal of Mechanical Design. 2003;125:221-32.

54. Jinghong Liang, Zissimos P Mourelatos, Efstratios Nikolaidis. A single-loop approach for system reliability-based design optimization. Journal of Mechanical Design. 2007;129:1215-24.

55. Fan Li, Teresa Wu, Adedeji Badiru, Mengqi Hu, Som Soni. A single-loop

deterministic method for reliability-based design optimization. Engineering Optimization. 2013;45:435-58.

56. Jongmin Lim, Byungchai Lee. A semi-single-loop method using approximation of most probable point for reliability-based design optimization. Structural and Multidisciplinary Optimization. 2016;53:745-57.

57. Joon Ha Jung, Byung Chul Jeon, Byeng D. Youn, Myungyon Kim, Donghwan Kim, Yeonwhan Kim. Omnidirectional regeneration (ODR) of proximity sensor signals for robust diagnosis of journal bearing systems. Mechanical Systems and Signal Processing. 2017;90:189-207.

58. Jungho Park, Jong Moon Ha, Hyunseok Oh, Byeng D. Youn, Joo-Ho Choi, Nam Ho Kim. Model-Based Fault Diagnosis of a Planetary Gear: A Novel Approach Using Transmission Error. IEEE Transactions on Reliability. 2016;65:1830-41.

59. Chao Hu, Pingfeng Wang, Byeng D. Youn, Wook-Ryun Lee, Joung Taek Yoon. Copula-Based Statistical Health Grade System Against Mechanical Faults of Power Transformers. Ieee Transactions on Power Delivery. 2012;27:1809-19.

60. Byeng D. Youn, Kyung Min Park, Chao Hu, Joung Taek Yoon, Hee Soo Kim, Beom Chan Jang, et al. Statistical Health Reasoning of Water-Cooled Power Generator Stator Bars Against Moisture Absorption. IEEE Transactions on Energy Conversion. 2015;30:1376-85.

61. Taejin Kim, Hyunseok Oh, Hyunjae Kim, Byeng D. Youn. An Online-Applicable Model for Predicting Health Degradation of PEM Fuel Cells With Root Cause Analysis. IEEE Transactions on Industrial Electronics. 2016;63:7094-103.

62. Alp Ustundag, Emre Cevikcan. Industry 4.0: Managing The Digital Transformation. Springer; 2017.

63. Joung Taek Yoon, Byeng D. Youn, Kyung Min Park, Wook-Ryun Lee. Sensor network optimization for mechanical failure detection of power transformers. The Korean Society of Mechanical Engineers; 2013. p. 1060-6.

64. Jiuping Xu, Yusheng Wang, Lei Xu. PHM-Oriented Sensor Optimization Selection Based on Multiobjective Model for Aircraft Engines. Ieee Sensors Journal. 2015;15:4836-44.

65. Nayeff Najjar, Shalabh Gupta, James Hare, Sherif Kandil, Rhonda Walthall. Optimal Sensor Selection and Fusion for Heat Exchanger Fouling Diagnosis in Aerospace Systems. IEEE Sensors Journal. 2016;16:4866-81.

66. Yang Hu, Piero Baraldi, Francesco Di Maio, Enrico Zio. A Systematic Semi-Supervised Self-adaptable Fault Diagnostics approach in an evolving environment. Mechanical Systems and Signal Processing. 2017;88:413-27.

67. Pingfeng Wang, Prasanna Tamilselvan, Chao Hu. Health diagnostics using

multi-attribute classification fusion. Engineering Applications of Artificial Intelligence. 2014;32:192-202.

68. Qingmin Li, Tong Zhao, Li Zhang, Jie Lou. Mechanical Fault Diagnostics of Onload Tap Changer Within Power Transformers Based on Hidden Markov Model. Ieee Transactions on Power Delivery. 2012;27:596-601.

69. Jim Lauffer. Diagnostics driven phm. First European Conference of the Prognostics and Health Management Society 2012. Dresden, Germany: PHM Society; 2012.

70. Prasanna Tamilselvan, Pingfeng Wang. Failure diagnosis using deep belief learning based health state classification. Reliab Eng Syst Saf. 2013;115:124-35.

71. Achmad Widodo, Bo-Suk Yang. Support vector machine in machine condition monitoring and fault diagnosis. Mechanical Systems and Signal Processing. 2007;21:2560-74.

72. Sotiris B. Kotsiantis. Supervised Machine Learning: A Review of Classification Techniques. Proceedings of the 2007 conference on Emerging Artificial Intelligence Applications in Computer Engineering: Real Word AI Systems with Applications in eHealth, HCI, Information Retrieval and Pervasive Technologies: IOS Press; 2007. p. 3-24.

73. Claudio M. Rocco S, Enrico Zio. A support vector machine integrated system for the classification of operation anomalies in nuclear components

and systems. Reliab Eng Syst Saf. 2007;92:593-600.

74. Kwok L. Tsui, Nan Chen, Qiang Zhou, Yizhen Hai, Wenbin Wang. Prognostics and Health Management: A Review on Data Driven Approaches. Mathematical Problems in Engineering. 2015.

75. Linxia Liao, Felix Köttig. A hybrid framework combining data-driven and model-based methods for system remaining useful life prediction. Applied Soft Computing. 2016;44:191-9.

76. Seyed Mohammad Rezvanizaniani, Zongchang Liu, Yan Chen, Jay Lee. Review and recent advances in battery health monitoring and prognostics technologies for electric vehicle (EV) safety and mobility. Journal of Power Sources. 2014;256:110-24.

77. Zhimin Xi, Rong Jing, Pingfeng Wang, Chao Hu. A copula-based sampling method for data-driven prognostics. Reliab Eng Syst Saf. 2014;132:72-82.

78. Woo Sung Choi, Gee Wook Song, Jae Raeraeyang Koo, Jae Sil Heo. Development of damage parameter measurement method to predict remaining life for aged turbine rotor. KSME2010. p. 110-1.

79. Junda Zhu, Jae M. Yoon, David He, Yongzhi Qu, Eric Bechhoefer. Lubrication Oil Condition Monitoring and Remaining Useful Life Prediction with Particle Filtering. International Journal of Prognostics and Health Management. 2013;4.

80. Chao Hu, Byeng D. Youn, Taejin Kim, Pingfeng Wang. A co-training-

based approach for prediction of remaining useful life utilizing both failure and suspension data. Mechanical Systems and Signal Processing. 2015;62-63:75-90.

81. Bruce R. Ellingwood, Yasuhiro Mori. Probabilistic methods for condition assessment and life prediction of concrete structures in nuclear plants. Nucl Eng Des. 1993;142:155.

82. A Fatemi, Lianxiang Yang. Cumulative fatigue damage and life prediction theories: a survey of the state of the art for homogeneous materials. Int J Fatigue. 1998;20:9-34.

83. Nagi Gebraeel, Alaa Elwany, Jing Pan. Residual life predictions in the absence of prior degradation knowledge. IEEE Transactions on Reliability. 2009;58:106-17.

84. Shun-Peng Zhu, Hong-Zhong Huang, Li-Ping He, Yu Liu, Zhonglai Wang. A generalized energy-based fatigue–creep damage parameter for life prediction of turbine disk alloys. Eng Fract Mech. 2012;90:89-100.

85. Vicente Climente-Alarcon, Jose Alfonso Antonino-Daviu, Elias G. Strangas, Martin Riera-Guasp. Rotor-Bar Breakage Mechanism and Prognosis in an Induction Motor. Ieee Transactions on Industrial Electronics. 2015;62:1814-25.

86. Pingfeng Wang, Byeng D. Youn, Chao Hu. A generic probabilistic framework for structural health prognostics and uncertainty management.

Mechanical Systems and Signal Processing. 2012;28:622-37.

87. Pierluigi Pisu, Andrea Serrani, Song You, Laci Jalics. Adaptive threshold based diagnostics for steer-by-wire systems. Journal of Dynamic Systems Measurement and Control-Transactions of the Asme. 2006;128:428-35.

88. Luca Massimiliano Capisani, Antonella Ferrara, Alejandra Ferreira de Loza, Leonid M. Fridman. Manipulator Fault Diagnosis via Higher Order Sliding-Mode Observers. Ieee Transactions on Industrial Electronics. 2012;59:3979-86.

89. Guishuang Tian, Shaoping Wang, Zhaomin He. False alarm mechanism and control of aircraft hydraulic system. 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA): IEEE; 2013. p. 1565-8.

90. Jongwan Kim, Sungsik Shin, Sang Bin Lee, Konstantinos N Gyftakis, M'hamed Drif, Antonio J Marques Cardoso. Power spectrum-based detection of induction motor rotor faults for immunity to false alarms. IEEE Transactions on Energy Conversion. 2015;30:1123-32.

91. Chanseung Yang, Tae-June Kang, Sang Bin Lee, Ji-Yoon Yoo, Alberto Bellini, Luca Zarri, et al. Screening of false induction motor fault alarms produced by axial air ducts based on the space-harmonic-induced current components. IEEE Transactions on Industrial Electronics. 2015;62:1803-13.

92. Yiqian Cui, Junyou Shi, Zili Wang. Multi-State Adaptive BIT False Alarm

Reduction Under Degradation Process. IEEE Transactions on Instrumentation and Measurement. 2015;64:671-82.

93. The Institute of Asset Management. Asset Management - an anatomy (Version 3). The Institute of Asset Management; 2015.

94. Khairy Ahmed Helmy Kobbacy, DN Prabhakar Murthy. Complex System Maintenance Handbook: Springer London; 2008.

95. John K. Kruschke, Torrin M. Liddell. The Bayesian New Statistics: Hypothesis testing, estimation, meta-analysis, and power analysis from a Bayesian perspective. Psychonomic Bulletin & Review. 2017:1-29.

96. Renato Galluzzi, Nicola Amati, Andrea Tonoli. Modeling and Characterization of Rotary Electrohydrostatic Actuators. Journal of Vibration and Acoustics. 2016;138:011016.

97. The LMS Imagine.Lab AMESim, http://www.plm.automation.siemens.com/en_us/products/lms/imagine-lab/amesim/index.shtml; 30 August 2017.

98. Yuanguo Cao, Xudong Dai. Modeling for performance degradation induced by wear of a hydraulic actuator of a hydraulic excavator. Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science. 2015:0954406214535926.

99. Christopher M. Bishop. Pattern Recognition and Machine Learning (Information Science and Statistics): Springer-Verlag New York, Inc.;

2006.

100. A. Garcia, J. Cusido, J. A. Rosero, J. A. Ortega, L. Romeral. Reliable electro-mechanical actuators in aircraft. Ieee Aerospace and Electronic Systems Magazine. 2008;23:19-+.

101. Chao Hu, Byeng D. Youn. Adaptive-sparse polynomial chaos expansion for reliability analysis and design of complex engineering systems. Structural and Multidisciplinary Optimization. 2011;43:419-42.

102. Leo H. Chiang, Mark E. Kotanchek, Arthur K. Kordon. Fault diagnosis based on Fisher discriminant analysis and support vector machines. Comput Chem Eng. 2004;28:1389-401.

103. Iman Izadi, Sirish L Shah, David S Shook, Tongwen Chen. An introduction to alarm analysis and design. IFAC Proceedings Volumes. 2009;42:645-50.

104. Amandeep Singh, Zissimos P. Mourelatos, Jing Li. Design for Lifecycle Cost Using Time-Dependent Reliability. Journal of Mechanical Design. 2010;132.

105. Zhen Hu, Xiaoping Du. Mixed Efficient Global Optimization for Time-Dependent Reliability Analysis. Journal of Mechanical Design. 2015;137:051401.

106. Zequn Wang, Pingfeng Wang. A Nested Extreme Response Surface Approach for Time-Dependent Reliability-Based Design Optimization.

Journal of Mechanical Design. 2012;134.

107. Yao Wang, Shengkui Zeng, Jianbin Guo. Time-Dependent Reliability-Based Design Optimization Utilizing Nonintrusive Polynomial Chaos. Journal of Applied Mathematics. 2013.

108. Hyunseok Oh, Seunghyuk Choi, Keunsu Kim, Byeng D. Youn, Michael Pecht. An empirical model to describe performance degradation for warranty abuse detection in portable electronics. Reliab Eng Syst Saf. 2015;142:92-9.

109. Dae Whan Kim, Hyunseok Oh, Byeng D. Youn, Dongil Kwon. Bivariate Lifetime Model for Organic Light-Emitting Diodes. IEEE Transactions on Industrial Electronics. 2017;64:2325-34.

110. Herbert Hecht. Prognostics for electronic equipment: an economic perspective. RAMS '06 Annual Reliability and Maintainability Symposium, 20062006. p. 165-8.

111. Jeffrey Banks, John Merenich. Cost Benefit Analysis for Asset Health Management Technology. 2007 Annual Reliability and Maintainability Symposium2007. p. 95-100.

112. Kiri Feldman, Taoufik Jazouli, Peter A. Sandborn. A Methodology for Determining the Return on Investment Associated With Prognostics and Health Management. IEEE Transactions on Reliability. 2009;58:305-16.

113. Wenbin Wang, Michael Pecht. Economic Analysis of Canary-Based

Prognostics and Health Management. IEEE Transactions on Industrial Electronics. 2011;58:3077-89.

114. Jeffrey Banks, Karl Reichard, Ed Crow, Ken Nickell. How engineers can conduct cost-benefit analysis for PHM systems. IEEE Aerospace and Electronic Systems Magazine. 2009;24:22-30.

115. Dirk Gorissen, Ivo Couckuyt, Piet Demeester, Tom Dhaene, Karel Crombecq. A surrogate modeling and adaptive sampling toolbox for computer based design. Journal of Machine Learning Research. 2010;11:2051-5.

116. Wei Gong, Qingyun Duan. An adaptive surrogate modeling-based sampling strategy for parameter optimization and distribution estimation (ASMO-PODE). Environ Model Software. 2017;95:61-75.

117. Chen Wang, Qingyun Duan, Wei Gong, Aizhong Ye, Zhenhua Di, Chiyuan Miao. An evaluation of adaptive surrogate modeling based optimization with two benchmark problems. Environ Model Software. 2014;60:167-79.

118. Richard Fujimoto. Parallel and distributed simulation. Proceedings of the 2015 Winter Simulation Conference: IEEE Press; 2015. p. 45-59.

119. Tapabrata Ray, Md Asafuddoula, Hemant Kumar Singh, Khairul Alam. An Approach to Identify Six Sigma Robust Solutions of Multi/Many-Objective Engineering Design Optimization Problems. Journal of Mechanical Design. 2015;137:051404.

120. Xiaotian Zhuang, Rong Pan, Xiaoping Du. Enhancing product robustness in reliability-based design optimization. Reliab Eng Syst Saf. 2015;138:145-53.

121. Lelai Zhou, Shaoping Bai, Michael Rygaard Hansen. Design optimization on the drive train of a light-weight robotic arm. Mechatronics. 2011;21:560-9.

122. S. M. Muzakkir, K. P. Lijesh, Harish Hirani. Failure Mode and Effect Analysis of Journal Bearing. Int J Appl Eng Res. 2015;10:37752-9.

123. Cristiano Fragassa, Martin Ippoliti. Failure Mode Effects and Criticality Analysis (Fmeca) as a Quality Tool to Plan Improvements in Ultrasonic Mould Cleaning Systems. Int J Qual Res. 2016;10:847-69.

124. Hyunseok Oh, Michael H Azarian, Michael Pecht, Clifford H White, Richard C Sohaney, Edward Rhem. Physics-of-failure approach for fan PHM in electronics applications. Prognostics and Health Management Conference, 2010 PHM'10: IEEE; 2010. p. 1-6.

125. Houman Hanachi, Jie Liu, Avisekh Banerjee, Ying Chen, Ashok Koul. A Physics-Based Modeling Approach for Performance Monitoring in Gas Turbine Engines. Ieee Transactions on Reliability. 2015;64:197-205.

126. Mauricio Sánchez-Silva, Georgia-Ann Klutke. Reliability and life-cycle analysis of deteriorating systems: Springer; 2016.

127. Nima Gorjian, Lin Ma, Murthy Mittinty, Prasad Yarlagadda, Yong Sun. A

review on degradation models in reliability analysis. In: Kiritsis D, Emmanouilidis C, Koronios A, Mathew J, editors. Engineering Asset Lifecycle Management: Proceedings of the 4th World Congress on Engineering Asset Management (WCEAM 2009), 28-30 September 2009. London: Springer London; 2010. p. 369-84.

128. Fan Wu, Seyed A. Niknam, John E. Kobza. A cost effective degradation-based maintenance strategy under imperfect repair. Reliab Eng Syst Saf. 2015;144:234-43.

129. Abdenour Soualhi, Kamal Medjaher, Noureddine Zerhouni. Bearing Health monitoring based on Hilbert-Huang Transform, Support Vector Machine and Regression. IEEE Transactions on Instrumentation and Measurement. 2014:1-11.

130. Peter E. Kloeden, Eckhard Platen. Numerical Solution of Stochastic Differential Equations: Springer Berlin Heidelberg; 2013.

131. Nabil Nahas. Buffer allocation and preventive maintenance optimization in unreliable production lines. J Intell Manuf. 2014;28:85-93.

132. Bram de Jonge, Ruud Teunter, Tiedo Tinga. The influence of practical factors on the benefits of condition-based maintenance over time-based maintenance. Reliab Eng Syst Saf. 2017;158:21-30.

133. Vladimir Babishin, Sharareh Taghipour. Joint optimal maintenance and inspection for a k-out-of-n system. The International Journal of Advanced

Manufacturing Technology. 2016;87:1739-49.

134. Peter A. Sandborn, Chris Wilkinson. A maintenance planning and business case development model for the application of prognostics and health management (PHM) to electronic systems. Microelectronics Reliability. 2007;47:1889-901.

135. Christer Stenström, Per Norrbin, Aditya Parida, Uday Kumar. Preventive and corrective maintenance – cost comparison and cost–benefit analysis. Struct Infrastruct E. 2016;12:603-17.

136. Kun-Peng Lin, Meng-Li Wang, Yuan Hong, Yang Yang, Jia-Xin Zhou. Discrete event simulation of long-duration space station operations for rapid evaluation. Aerospace Science and Technology. 2017;68:454-64.

137. Xianguang Gu, Jianwei Lu, Hongzhou Wang. Reliability-based design optimization for vehicle occupant protection system based on ensemble of metamodels. Structural and Multidisciplinary Optimization. 2014;51:533-46.

138. D. M. Hamby. A review of techniques for parameter sensitivity analysis of environmental models. Environ Monit Assess. 1994;32:135-54.

139. B. Lorenz, B. N. J. Persson. Leak rate of seals: Comparison of theory with experiment. EPL (Europhysics Letters). 2009;86:44006.

140. Bo Persson, Chongjun Yang. Theory of the leak-rate of seals2008.

141. JeFoa Archard. Contact and Rubbing of Flat Surfaces. Journal of Applied Physics. 1953;24:981-8.

142. Min-Kook Choi, Hyun-Gyu Lee, Sang-Chul Lee. Weighted SVM with classification uncertainty for small training samples. 2016 IEEE International Conference on Image Processing (ICIP)2016. p. 4438-42.

143. Hyeongjin Song, K. K. Choi, Ikjin Lee, Liang Zhao, David Lamb. Adaptive virtual support vector machine for reliability analysis of high-dimensional problems. Structural and Multidisciplinary Optimization. 2013;47:479-91.

144. Dan M. Frangopol, Kai-Yung Lin, Allen C. Estes. Life-Cycle Cost Design of Deteriorating Structures. J Struct Eng. 1997;123:1390-401.

145. Seong-yeob Lee, Choonghee Jo, Pål Bergan, Bjørnar Pettersen, Daejun Chang. Life-cycle cost-based design procedure to determine the optimal environmental design load and target reliability in offshore installations. Struct Saf. 2016;59:96-107.

146. Georgia-Ann Klutke, Peter C Kiessler, Martin A Wortman. A critical look at the bathtub curve. IEEE Transactions on Reliability. 2003;52:125-9.

147. Gill Windle, Kate M Bennett, Jane Noyes. A methodological review of resilience measurement scales. Health and quality of life outcomes. 2011;9:1.

148. Jonas Joerin, Rajib Shaw, Yukiko Takeuchi, Ramasamy Krishnamurthy.

The adoption of a climate disaster resilience index in Chennai, India. Disasters. 2014;38:540-61.

149. Maria Nogal, Alan O'Connor, Beatriz Martinez-Pastor, Brian Caulfield. Novel Probabilistic Resilience Assessment Framework of Transportation Networks against Extreme Weather Events. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering. 2017;3.

150. Devanandham Henry, Jose Emmanuel Ramirez-Marquez. Generic metrics and quantitative approaches for system resilience as a function of time. Reliab Eng Syst Saf. 2012;99:114-22.

Appendix

Table A-1 Definitions and measures of resilience in various research areas

Research area	Definition	Measure	Ref.
Psychology	process of negotiating, managing and adapting to significant sources of stress or trauma	- various measures (about 15 measures) - different purpose, survey items, and target population - ex: Connor-Davidson resilience scale (CD-RISC), resilience scale for adults (RSA), and brief resilience scale (BRS)	[147]
Ecology	speed with which a system returns to its pre-disturbance level following a disturbance	- Resilience $\mathrm{RL}(t_x) = \frac{2\lvert D_0\rvert}{\lvert D_0\rvert+\lvert D_x\rvert} - 1$ - D_0: response difference at the end of disturbance (t_0) with respect to initial response - D_x: current response difference (t_x) with respect to initial response	[9]
Economy	policy-induced ability of an economy to recover from or adjust to the negative impacts of adverse exogenous shocks and to benefit from positive shocks	- composed of four components: macroeconomic stability, microeconomic market efficiency, good governance and social development - subjective variable selection and weight allocation for the summing of four components	[10]
Environ-mental science	capability to withstand climate-related disasters from a community perspective	- Climate Disaster Resilience Index (CDRI): weighted average of 125 variables from five dimensions: economic, institutional, natural, physical, and social - subjective questionnaire and weighting scheme	[148]
Civil engineering	normalized function indicating capability to sustain a level of functionality or performance for a	- resilience index of infrastructure R_i is the time-averaging of functionality Q_i for period T_c $R_i = \int_0^{T_c} \frac{Q_i(t)}{T_c} dt$	[13]

	given building, bridge, lifeline, networks, or community over a period of time (life cycle, life span, etc.)	- regional resilience index is the weighted average of the infrastructure resilience index $R = \sum_i R_i \times w_i$ - the weight coefficient w_i is calculated from a modified version of the interdependence index	
	ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions	- rates of performance change from incident time T_i, through failure time T_f to recovery time T_r considering failure profile F and recovery profile R Resilience $R_e = \frac{T_i + F\Delta T_f + R\Delta T_r}{T_i + \Delta T_f + \Delta T_r}$ - F and R are the performance change rates during failure duration $\Delta T_f = T_f - T_i$ and recovery duration $\Delta T_r = T_r - T_f$ respectively	[14]
	capacity of a system potentially exposed to hazards to adapt by resisting or changing in order to reach and maintain an acceptable level of functioning	- the resilience of a traffic network impacted by extreme weather events - the normalized area over an exhaustion curve by the traffic network to measure how far the system is from complete exhaustion (0~100%)	[149]
Industrial and system engineering	ability of a system to bounce back	- the ratio of recovery to loss at previous time point $R(t_r) = \frac{F(t_r) - F(t_d)}{F(t_d) - F(t_0)}$ - $F(\cdot)$: a specific figure of merit - t_r: resilience evaludation time - t_d: disruptive event end time - t_0: initial stable state time	[150]
Mechanical engineering	degree of a passive survival rate (reliability) plus a proactive survival rate (restoration)	- resilience = reliability + restoration - reliability: ability to maintain capacity and performance during a given period of time under stated conditions - restoration: ability to restore	[11]

		capacity and performance by detecting, predicting, and maintaining	
	degree of a passive survival rate (reliability) plus a proactive survival rate (restoration) plus recovery capability (recoverability)	- engineering resilience = reliability + restoration + recoverability - recoverability: probability to recover a failed component or systems at a given time	[17]
	ability of a system to recover to its normal operating condition after occurrence of one or more disruptive events	- combining the measure by Youn et al. [11] with vulnerability - time-dependency of reliability is considered	[18]

Abstract(Korean)

복잡한 공학 시스템에 대한 오경보를 고려한 리질리언스 해석 및 설계 방법론 연구

서울대학교 공과대학
기계항공공학부 대학원
윤 정 택

공학 시스템은 생애주기에 걸쳐 다양한 불확실성에 노출되며, 이로 인해 목표 성능을 충족시키지 못할 경우 사회적, 경계적, 인적 소실을 야기하게 된다. 이에 대한 해결 방안 중 하나로 리질리언스 주도 설계 기술 (resilience-driven system design; 이하 RDSD)이 개발되었다. RDSD는 건전성 예측 및 관리 기술 (prognostics & health management; 이하 PHM)을 설계에 도입함으로써 비용 효율적인 고장 예방을 가능케 하였다. 하지만, RDSD는 PHM의 고장 오경보 현상을 고려하지 않는 한계점을 갖는다. 고장 오경보는 건전한 시스템을 고장이라 추정하는 현상으로, 불필요한 시스템 정지 및 검사 비용을 야기하여, PHM과 RDSD의 기술적 효용성을 떨어트리게 된다. 따라서, RDSD의 기술적 약진과 실적용을 도모하기 위해서는 고장 오경보 현상을 해결해야 한다.

본 논문에서는 고장 오경보의 고려를 통해 리질리언스 해석 및 설계 방법론을 개선하고자 하며, 이를 위해 세 가지 연구 주제를 제안한다. 첫 번째 주제는 오경보를 고려한 리질리언스 분석으로, 공학 시스템의 리질리언스 시나리오 분석에 기반해 리질리언스 지수를

새롭게 정식화 한다. 이 지수는 고장 오경보로 인한 리질리언스의 저하를 분석함으로써, 정확한 리질리언스 추정을 가능케 한다. 두 번째 주제는 고장 오경보를 고려한 리질리언스 주도 설계 방법론이다. 이는 3단계의 계층적 요소로 구성된다. 먼저 목표 리질리언스 지수를 만족하면서 생애주기비용을 최소화하기 위해, 목표 신뢰도와 목표 오경보 및 유실경보율을 최적화한다. 이후 신뢰성 기반 최적 설계 (reliability-based design optimization)를 통해 목표 신뢰도를 확보하고, PHM 설계를 통해 할당된 목표 오경보 및 유실경보율을 충족시킨다. 세 번째 주제는 시변(時變) 오경보를 고려한 리질리언스 주도 설계 방법론이다. 기존의 설계 방법론들은 시스템의 건전성 상태를 시불변(時不變)하다 간주하였으나, 실제 시스템은 운행에 따라 점진적으로 건전성이 저하된다. 본 연구에서는 시변성을 분석하기 위해 시변 오경보율 및 유실경보율에 대한 개념을 새롭게 제안하였으며, 생애주기 시뮬레이션을 통한 총 유지보수 비용 분석 방법론을 개발하였다. 이를 통해 생애주기비용을 보다 엄밀하고 정확하게 추정할 수 있게 되었으며, 이를 최소화하는 방향으로 시스템과 PHM의 설계를 최적화였다. 본 연구에서 제안한 방법론들은 이론적 분석과 사례 연구를 통해 그 효용성을 입증하였다.

주제어 : 리질리언스 (resilience)
신뢰도 (reliability)
건전성 예측 및 관리 (prognostics & health management)
고장 오경보 (false alarm)
시스템 설계 (system design)

학 번 : 2011-20729