

PROCESS RESILIENCE ANALYSIS FRAMEWORK FOR DESIGN AND
OPERATIONS

A Dissertation

by

PRERNA JAIN

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	M. Nazmul Karim
Committee Members,	Mahmoud El-Halwagi
	Thomas Ferris
	Estratios N. Pistikopoulos
Head of Department,	M. Nazmul Karim

December 2018

Major Subject: Chemical Engineering

Copyright 2018 Prerna Jain

ABSTRACT

Process plants are complex socio-technical systems that degrade gradually and change with advancing technology. This research deals with exploring and answering questions related to the uncertainties involved in the process systems, and their complexity. It aims to systematically integrate resilience in process design and operations through three different phases of prediction, survival, and recovery using a novel framework called Process Resilience Analysis Framework (PRAF). The analysis relies on simulation, data-driven models and optimization approach employing the resilience metrics developed in this research. In particular, an integrated method incorporating aspects of process operations, equipment maintenance, and process safety is developed for the following three phases:

- Prediction: to find the feasible operating region under changing conditions using Bayesian approach, global sensitivity analysis, and robust simulation methods,
- Survival: to determine optimal operations and maintenance strategies using simulation, Bayesian regression analysis, and optimization, and
- Recovery: to develop a strategy for emergency barriers in abnormal situations using dynamic simulation, Bayesian analysis, and optimization.

Examples of a batch reactor, and cooling tower operations process unit are used to illustrate the application of PRAF. The results demonstrate that PRAF is successful in capturing the interactions between the process operability characteristics, maintenance, and safety policy. The prediction phase analysis leads to good dynamic response and stability

of operations. The survival phase helps in the reduction of unplanned shutdown and downtime. The recovery phase results in in reduced severity of consequences, and response time and overall enhanced recovery. Overall, PRAF achieves flexibility, controllability and reliability of the system, supports more informed decision-making and profitable process systems.

DEDICATION

Dedicated to my family! Thank you for your love and support.

ACKNOWLEDGEMENTS

I have now been on this journey for a little over five years, and it has been an incredible experience for me. There are several people whom I met and connected with during this time and they all made it possible for me to achieve my goals.

I would like to begin by thanking my parents, husband, and my in-laws. Their selfless support and love have always been the prime drivers towards my development and achievements. Their strength and sacrifice are my inspiration to overcome any personal challenges. To my parents, in-laws, husband, brothers, and family: thank you very much for encouraging me to set higher goals for myself, for believing in me, and for being there to support me whole-heartedly in all my endeavors. Special thanks to my loving husband Pankaj, who has stood with me like a rock in every happy or sad, easy or difficult moments in this journey. I never would have made it without you all. I love you all.

I extend my most sincere gratitude and appreciation to late Dr. Sam Mannan. His guidance and support have been crucial during my graduate school years. I am grateful to him for all his influence in my life and the message to be my best in whatever I do. I would like to thank my Committee chair, Dr. Nazmul Karim, and my Committee members, Dr. Stratos Pistikopoulos, Dr. Mahomoud El-Halwagi, and Dr. Thomas Ferris, for their guidance and support throughout the course of this research.

I am profoundly grateful to Professor Stratos Pistikopoulos. His excellent mentoring and development opportunities he provided made graduate school a great experience. I am especially grateful to him for sharing his passion for knowledge and

research and encouraging me to explore new research horizons. He is a terrific advisor and person; it has been my utmost honor working with him all these years.

I thank my group members, from both the Mary Kay O'Connor Process Safety Center and Dr. Pistikopoulos's group. It is a pleasure to be part of such great groups of individuals. Thanks for your friendship, mentoring, collaboration, and guidance. It means a lot to me.

I would also like to express my deep gratitude to Dr. Hans Pasman, Dr. Simon Waldram, and Dr. William Rogers for their research guidance and their time to hear my ideas and giving these ideas direction.

I also appreciate all the help from my mentors, specially Captain James Pettigrew, Mr. Kelly Keim, and Dr. Ray Mentzer for their guidance to keeping my research close to real industry applications.

I would also like to thank Sheera Helms, and Vickie Torres for their extensive support during these years. I would like to acknowledge the financial support for this research from The Mary Kay O'Connor Process Safety Center.

Finally, I want to extend my gratitude to the Texas A&M University for providing me with excellent opportunities to serve in various student leadership roles, serve the Aggie community and keep me motivated in my research journey.

CONTRIBUTORS AND FUNDING SOURCES

This work was supported by a dissertation committee consisting of Professor M. Nazmul Karim, Professor Estratios N. Pistikopoulos, and Professor Mahmoud El-Halwagi of the Department of Chemical Engineering and Professor Thomas Ferris of the Department of Industrial and Systems Engineering.

The Mary Kay O'Connor Process Safety Center sponsored this research with partial financial support from Texas A&M Energy Institute.

NOMENCLATURE

ALARP	As low as reasonably practicable
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
BART	Bay area rapid transit
BLHAZID	Blended Hazid
BOEM	Bureau of Ocean Energy Management
BOEMRE	Bureau of Ocean Energy Management, Regulation and Enforcement
BSEE	Bureau of Safety and Environmental Enforcement
CBA	Cost benefit analysis
CCPS	Center for chemical process safety
CFD	Computational fluid dynamics
COMAH	Control of Major Accident Hazards
CM	Corrective Maintenance
CMMS	Centralized Maintenance Management System
C_{st}	Socio-technical congruence
DMM	Domain mapping matrix
DSM	Design structure matrix
DTBN	Discrete time bayesian network
ED	Early Detection
EPR	Expected Process Revenue
ER	Expected Revenue
ETD	Error Tolerant Design

ESD	Emergency shutdown
ETA	Event tree analysis
EWDS	Early warning detection system
FDD	Fault detection and diagnosis
FEM	Finite element method
FMEA	Failure mode and effect analysis
FTA	Fault Tree Analysis
GAMS	General Algebraic Modeling System
GSA	Global sensitivity analysis
HAZID	Hazard identification
HAZOP	Hazard and operability study
HMI	Human machine interface
HRA	Human reliability analysis
HRO	High reliability organization
IE	Initiating event
IRF	International Regulator's Forum
IS	Inherent safety
ISA	International society of automation
KPI	Key performance indicators
LCCA	Life cycle cost analysis
LFI	Learning from incident
LNG	Liquefied natural gas
LOC	Loss of containment

LOPA	Layer of protection analysis
MCMC	Monte Carlo Markov Chain
MDM	Multi domain matrix
MHA	Major hazard analysis
MINLP	Mixed integer non-linear programming
MOC	Management of Change
MMS	Minerals Management Service
MTPoD	Maximum tolerable period of disruption
MTTR	Mean time to repair
NPD	Norwegian Petroleum Directorate
OCS	Outer Continental Shelf
OD	Operational discipline
ODE	Ordinary differential equation
ORA	Optimal risk analysis OSHA
P	Plasticity
PdM	Predictive Maintenance
PE	Propagation event
PFD	Probability of failure on demand
PHA	Process hazard analysis
PI	Proportional integral
PM	Preventive Maintenance
PRA	Probabilistic risk analysis
PRAF	Process Resilience Analysis Framework

PRI	Process resilience index
PSM	Process Safety Management
PSSR	Pre-startup safety review
QAISD	Qualitative Assessment for Inherently Safer Designs
QoD	Unavailability on demand
R	Recoverability
RBA	Risk benefit analysis
REWI	Resilience based early warning indicator
RIPSHA	Resilience-based integrated process system hazard analysis
RPI	Resilience prediction index
RPO	Recovery point objective
RRI	Resilience recovery index
RSI	Resilience survivability Index
RTO	Recovery time objective
SA	Sensitivity analysis
SAP	System analysis and program development
SCE	Safety critical equipment
SEMS	Safety and Environment Management System
SI	Sensitivity index
SIF	Safety instrumented function
SIS	Safety instrumented system
SMS	Safety management system
SSI	System Survivability Index

STPA	System theoretic process analysis
STS	Socio-technical system
TAC	Total Annualized Cost

TABLE OF CONTENTS

ABSTRACT	ii
DEDICATION	iv
ACKNOWLEDGEMENTS	v
CONTRIBUTORS AND FUNDING SOURCES.....	vii
NOMENCLATURE.....	viii
TABLE OF CONTENTS	xiii
LIST OF FIGURES.....	xvii
LIST OF TABLES	xxi
CHAPTER I INTRODUCTION: MOTIVATION, CHALLENGES AND NEED FOR ADVANCED RISK AND RESILIENCE ASSESSMENT	1
1.1. Motivation and Challenges.....	2
1.1.1. Limitations of risk assessment and management	3
1.1.2. Incidents over the years	4
1.1.3. Complex systems failure	6
1.2. Need for Advanced Risk and Resilience Assessment.....	8
1.2.1. Regulations	8
1.2.2. Country-specific regulations	11
1.2.3. Results: Data analysis.....	13
1.2.4. Knowledge growth and gaps	25
1.2.5. Process Hazard and Risk analysis	25
1.2.6. Safety management	28
1.2.7. System approach, complexity, causality	29
1.2.8. Uncertainty, Fuzzy logic, Bayesian statistics and networks	29
1.3. Looking into the future: top-down problem analysis	31
1.4. Research challenges and objectives	33
1.5. Summary	35
CHAPTER II BACKGROUND: PREVIOUS WORK AND LITERATURE REVIEW... 40	
2.1. System Resilience and Resilience Engineering	40
2.2. Process System Resilience Modeling Aspects	44
2.2.1. Process Risk: Analysis and Reduction	45
2.2.2. Systems thinking	47
2.2.3. Early fault detection	50
2.2.4. Dynamic simulation, optimization and major events modeling.....	52

2.3.	Summary	54
CHAPTER III PROCESS RESILIENCE ANALYSIS FRAMEWORK		56
3.1.	Process Resilience Analysis Framework (PRAF): basic concepts and structure	58
3.1.1.	Four aspects of process resilience	62
3.1.2.	Three-phase analysis	65
3.2.	Resilience metrics	67
3.2.1.	Phase I – Avoidance	72
3.2.2.	Phase II– Survival	74
3.2.3.	Phase III– Recovery	76
3.2.4.	Common metrics	77
3.3.	PRAF survey	77
3.3.1.	Survey content and methodology	78
3.3.2.	Survey respondents.....	79
3.3.3.	Survey quality and analysis.....	81
3.3.4.	Results	84
3.3.5.	Application	102
3.4.	Quantification of social aspects (DSM)	103
3.4.1.	Motivating example.....	104
3.5.	Summary	108
CHAPTER IV QUALITATIVE ASSESSMENT: RESILIENCE BASED INTEGRATED PROCESS SYSTEM HAZARD ANALYSIS (RIPSHA).....		111
4.1.	Overview of existing hazards identification and analysis techniques.....	113
4.2.	Overview of existing evaluation studies for the management layer	115
4.2.1.	Accimap.....	116
4.2.2.	System-theoretic process analysis (STPA).....	116
4.2.3.	Blended Hazid (BLHAZID).....	116
4.2.4.	Dynamic Procedure for Atypical Scenarios Identification (DyPASI)	117
4.3.	Systems hazard analysis vs process hazard analysis.....	117
4.4.	RIPSHA: Resilience-based Integrated Process Systems Hazard Analysis	119
4.5.	Bi-layered system approach	120
4.5.1.	Management system hazard analysis	121
4.5.2.	Plant system hazard analysis	127
4.6.	Multi-mode approach	132
4.7.	Methodology	133
4.8.	Management system hazard analysis example: Tank Explosion	139
4.9.	Plant system hazard analysis example: a liquefied natural gas (LNG) facility.	142
4.10.	Summary	147
CHAPTER V QUANTITATIVE ASSESSMENT: PREDICTABILITY ANALYSIS....		148
5.1.	Background	149
5.2.	Predictability assessment methodology	150

5.2.1. Bayesian methods	153
5.2.2. Sensitivity Analysis	154
5.2.3. Global Sensitivity Analysis (GSA)	155
5.2.4. Flexibility analysis	156
5.3. Case study: Batch reactor case study	157
5.3.1. Process description	157
5.4. Methodology application.....	159
5.5. Summary	184
CHAPTER VI QUANTITATIVE ASSESSMENT: SURVIVABILITY ANALYSIS	186
6.1. Background	187
6.2. Maintenance policies.....	190
6.3. Survivability assessment: model development	192
6.3.1. Process model.....	192
6.3.2. Maintenance model	195
6.3.3. Safety model.....	199
6.3.4. Cost/revenue model.....	200
6.4. Application to the cooling tower operations	202
6.4.1. System and process description.....	202
6.4.2. Process model.....	204
6.4.3. Maintenance model (Safeguard analysis).....	207
6.4.4. Safety Model	209
6.4.5. Cost/revenue model.....	211
6.5. Results and Discussion.....	211
6.5.1. System reliability.....	212
6.5.2. Maintenance action analysis.....	214
6.5.3. Maintenance action selection	218
6.5.4. Reliability and expected process revenue	219
6.6. Summary	225
CHAPTER VII PROCESS SYSTEM RESILIENCE, BUSINESS CONTINUITY AND SUSTAINABILITY	227
7.1. Business Continuity	229
7.1.1. Definition of Business Continuity.....	229
7.1.2. Business Continuity Metrics	229
7.2. Sustainability.....	230
7.2.1. Definition of Sustainable Process System.....	230
7.2.2. Sustainability Metrics.....	230
7.3. Case study: Chevron Refinery Fire	230
7.3.1. Analysis	231
7.4. Summary	239
CHAPTER VIII CONCLUSIONS AND FUTURE WORK	240

8.1. Conclusions	240
8.2. Recommendations for future directions	244
REFERENCES	248
APPENDIX A SOBOL SENSITIVITY INDICES	290
APPENDIX B STATISTICAL METHODS	293
APPENDIX C EULERS METHOD	295
APPENDIX D RELIABILITY AND MAINTAINABILITY	296
APPENDIX E COOLING TOWER PROCESS MODEL	298
APPENDIX F VALUES OF CONSTANTS AND COST NUMBERS	300

LIST OF FIGURES

	Page
Figure I.1 Percentage of global incidents (developed using data from Marsh report ⁶)	5
Figure I.2 Property damage (developed using data from Marsh report ⁶)	5
Figure I.3: Differences between the two process safety regulations	9
Figure I.4: Total damage	14
Figure I.5: Petrochemical losses.....	15
Figure I.6: Refinery losses.....	15
Figure I.7: Upstream losses	16
Figure I.8: Fatalities.....	19
Figure I.9: Major injuries	19
Figure I.10: Major fires	20
Figure I.11: Number of oil spills	20
Figure I.12: Number of refinery incidents.....	21
Figure I.13: Incident rate	22
Figure I.14: Average refinery incident rate	23
Figure I.15: Fatality rate	24
Figure I.16: Evolution in process safety and risk management methods	34
Figure II.1: Causal loop diagram – safety is a non-linear problem	50
Figure II.2: System life cycle V-model	51
Figure III.1: Process resilience analysis framework overview	58
Figure III.2: Process plant system	61
Figure III.3: System transition diagram.....	62
Figure III.4: Resilience aspects under PRAF	65

Figure III.5: Resilience analysis diagram in three stages with aspects and metrics	67
Figure III.6: Respondents by area of experience	80
Figure III.7: Respondents by employment sector	80
Figure III.8: Avoidance phase metrics and respondents perception on effectiveness	88
Figure III.9: Survival phase metrics and respondents perception on effectiveness	90
Figure III.10: Recovery phase metrics and respondents perception on effectiveness	91
Figure III.11: Relationship between experience areas (LFI communication metric)	98
Figure III.12: Relationship between employment sectors (LFI communication metric).....	99
Figure III.13: Relationship between phases and significance	100
Figure III.14: The four quadrants of a two-domain MDM for reactor charging	105
Figure III.15: Reactor charging procedure	106
Figure III.16: Reactor charging procedure: congruence matrix	107
Figure III.17: Summary statistics	108
Figure IV.1: RIPSHA: bi-layered approach	121
Figure IV.2: Tank explosion accident timeline	139
Figure IV.3: LNG storage tank P&ID	143
Figure V.1: Predictability assessment	151
Figure V.2: Bayesian analysis for uncertainty management	153
Figure V.3: Batch reactor process system	157
Figure V.4: Batch reactor process system transition diagram	159
Figure V.5: Effect of medium temperature on the KPIs.....	162
Figure V.6: Effect of agitator revolutions on the KPIs.....	162
Figure V.7: Effect of inert composition (A) on the KPIs	163
Figure V.8: Effect of inert composition (B) on the KPIs	163
Figure V.9: Combined effect of uncertain process parameters on the KPIs.....	164

Figure V.10: First order sensitivity indices for the uncontrolled case.....	166
Figure V.11: First order sensitivity indices for the controlled case.....	167
Figure V.12: Second order sensitivity indices for the uncontrolled case	167
Figure V.13: Second order sensitivity indices for the controlled case	168
Figure V.14: Algorithm: jacket medium temperature analysis	170
Figure V.15: Algorithm: agitator failure analysis.....	172
Figure V.16: Scatterplot showing the clustering of (I_1, I_2)	174
Figure V.17: Algorithm: reactor mischarging analysis	175
Figure V.18: Scatterplot of Z_1 and Z_2	176
Figure V.19: Jacket medium temperature: Prior (black) and posterior (blue).....	179
Figure V.20: Boxplot of prior and posterior samples: agitator failure probability	180
Figure V.21: Boxplot of prior and posterior samples: reactor mischarging probability.....	181
Figure V.22: Feasible region	182
Figure V.23: KPIs vs time at critical point.....	183
Figure V.24: Jacket flowrate vs time at critical point.....	183
Figure VI.1: Survivability assessment methodology.....	195
Figure VI.2: Model for maintenance action selection	196
Figure VI.3: Methodology for data-driven maintenance model.....	198
Figure VI.4: Cooling tower operations process system.....	203
Figure VI.5: Survivability assessment methodology: cooling tower operations	204
Figure VI.6: Extracted features snapshot	208
Figure VI.7: System reliability for different states	214
Figure VI.8: Trace and density plots for coefficients for pump 1: a – Equipment life; b,c – Frequency; d,e – Downtime.....	216
Figure VI.9: Autocorrelation plots for pump 1: a – Equipment life; b – Frequency; c – Downtime	217

Figure VI.10: Posterior probability density functions for P1, P2, and P3	218
Figure VI.11: System reliability vs expected revenue.....	220
Figure VI.12: Trend of expected revenue with and without safety impact cost.....	221
Figure VI.13: A pareto chart showing system reliability and expected revenue.....	221
Figure VI.14: System reliability vs safety impact cost.....	224
Figure VI.15: System reliability vs RSI	224
Figure VII.1: Total annual revenue of Chevron	234
Figure VII.2: Total annual profit of Chevron.....	234
Figure VII.3: Trendline result for Business Continuity and Resilience relationship.....	237
Figure VII.4: Trendline results for Sustainability and Resilience Relationship	238

LIST OF TABLES

	Page
Table I.1: Complex system failures	7
Table I.2: Summary: comparison of regulatory regimes	10
Table I.3: Process safety events (non-normalized data)	17
Table II.1 Resilience definitions.....	42
Table II.2: Resilience engineering applications.....	43
Table II.3: Selected works on process risk analysis	47
Table II.4: Selected works on early fault detection	52
Table II.5: Selected works on resilience and major events modeling	53
Table III.1: Comparative analysis of resilience models or studies	60
Table III.2: Different phases of process resilience	66
Table III.3: Selected list of works on process safety or risk management metrics.....	70
Table III.4: List of works on resilience metrics.....	71
Table III.5: Ordinal alpha and Cronbach's alpha for Avoidance phase metrics.....	81
Table III.6: Ordinal alpha and Cronbach's alpha for Survival phase metrics	82
Table III.7: Ordinal alpha and Cronbach's alpha for Recovery phase metrics.....	83
Table III.8: Descriptive statistics (Avoidance phase).....	85
Table III.9: Descriptive statistics (Survival phase).....	86
Table III.10: Descriptive statistics (Recovery phase).....	87
Table III.11: Polychoric correlation matrix (Avoidance).....	93
Table III.12: Polychoric correlation matrix (Survival).....	94
Table III.13: Polychoric correlation matrix (Recovery)	95
Table III.14: Kruskal-Wallis test results.....	96
Table IV.1: Hazid and Analysis Methods	114
Table IV.2: Works on evaluation studies for the management layer.....	115

Table IV.3: Process safety culture and leadership: suggested guidewords	123
Table IV.4: Operational discipline: suggested guidewords	125
Table IV.5: Process safety systems: suggested guidewords	126
Table IV.6: Operator/human: suggested guidewords	129
Table IV.7: Procedure: suggested guidewords	130
Table IV.8: RIPS HA Worksheet: Plant system layer	136
Table IV.9: RIPS HA Worksheet: Management system layer	137
Table IV.10: RIPS HA worksheet management system layer analysis – Tank explosion	141
Table IV.11: Incidents in LNG facilities	144
Table IV.12: RIPS HA worksheet plant system layer analysis – LNG storage tank.....	146
Table V.1: Major causes of batch reactor incidents	150
Table V.2: Comparison of screening, local, and global methods	155
Table V.3: Uncertainty analysis: simulation results	178
Table VI.1: An indicative list of works on maintenance optimization	191
Table VI.2: Maintenance action analysis (ground truth)	196
Table VI.3: Resilience metrics for maintenance model.....	197
Table VI.4: Process specifications of process example scenarios	206
Table VI.5: Optimization results	211
Table VI.6: System reliability for different scenarios	213
Table VI.7: Results of maintenance action analysis	219
Table VII.1: Business continuity metrics	231
Table VII.2: Sustainability metrics.....	233
Table VII.3: Resilience metrics	236

CHAPTER I

INTRODUCTION: MOTIVATION, CHALLENGES AND NEED FOR ADVANCED RISK AND RESILIENCE ASSESSMENT*

Risk management challenges and continuous increase of global public aversion to hazards and risks associated with the process industry have been observed in the recent years. In order to manage process industry risk, several studies and methods have been developed and are currently used. Two types of interacting factors: 1) technical (equipment malfunction, process parameter variation), and 2) social (regulations/policy, human and organizational factors) are important in assessment of risk for a process system. However, current methods are based on an analysis of either technical factors, often quantitatively, or social factors, usually qualitatively. Apart from failure to establish all critical scenarios due to either factors, their combined and interactive effects are seldom considered. This research need calls for the development of a holistic and integrated systems framework for effective risk management, although full coverage of possible mishaps will be utopian.

The application of the resilience engineering perspective is gradually being explored as an approach for considering the dynamics of socio-technical aspects based on systems theory to provide a safety net. This research presents a novel framework - Process Resilience Analysis Framework (PRAF) for incorporating both technical and

*Reproduced in part with permission from Jain, P., Pasma, H. J., Waldram, S. P., Rogers, W. J., & Mannan, M. S., "Did we learn about risk control since Seveso? Yes, we surely did, but is it enough? An historical brief and problem analysis," JLPPI, Vol 49, Part A, Pages 5-17. Copyright 2017 Elsevier Ltd.

Reproduced in part with permission from Jain, P., Reese, A. M., Chaudhari, D., Mentzer, R. A., & Mannan, M. S., "Regulatory approaches-Safety case vs US approach: Is there a best solution today?", JLPPI, Vol 46, Pages 154-162. Copyright 2017 Elsevier Ltd.

social factors in an integrated approach. This is based on four aspects: Early Detection (ED), Error Tolerant Design (ETD), Plasticity (P) and Recoverability (R). The resilience methodology emphasizes dynamics, unforeseen and even unknown types of threats, uncertainty, systems degradation and complex interactions. With resilience metrics a combined framework for predictability, survivability and recoverability, all via dynamic analysis, is introduced. PRAF primarily focuses on early detection of unsafe domains of operation, assessment of aggregate risks and prioritization of safety barriers during process upset situations and reduction in response time resulting in a reduced frequency of loss of containment events LoC, reduced consequences and enhanced recovery.

1.1. Motivation and Challenges

Statistics for incidents and LoC events show that they have continued to happen globally and have occurred across a wide variety of industrial sectors. Also, there are limitations in existing risk management methods. For this research, a systems-based resilience approach is proposed to address the gaps identified from literature and to answer the following questions:

- How to predict or find frequency of occurrence of LoC events with developing technology, complexities and stringent regulations?
- How to assess risk with existing safety barriers?
- How to prioritize emergency barriers, and signals from them, in order to reduce response time?

In the next sub-sections, the limitations of risk assessment methods, incident statistics, and failure of complex systems are briefly described.

1.1.1. Limitations of risk assessment and management

There are different types of risk assessment methods: Deterministic and Probabilistic, or Qualitative and Quantitative¹. Some of the major risk identification, estimation and evaluation methods used currently for risk assessment and management are²:

- Risk identification: Hazard and operability study (HAZOP), What-if analysis.
- Risk estimation: Fault Tree Analysis FTA, Failure mode and effect analysis (FMEA), Human reliability analysis HRA, Event tree analysis (ETA), Cost benefit and risk benefit analysis (CBA/RBA), Sensibility analysis (SA), Expert systems, and databases.
- Risk evaluation: Monte-Carlo simulation, Hertz-type simulation.

The following are two main observations:

- In general risk assessments are based on a mechanistic approach for problem solving. In such cases, the emergent properties arising from the whole system are not recognized.
- Thus far, social factors related to regulations, humans and organizations are not considered in an integrated way during the risk assessment.

The general methods ignore specificities of the studied scenario and complexities of scenarios are generally simplified. The knowledge background of the people, who are participating in the risk analysis, is critical (*e.g.*, as with the main hazard identification technique of HAZOP), and is susceptible to bias and ignorance. Additionally, in HAZOP studies, analysts may miss half of the significant scenarios, resulting from a variety of causes, such as failure to anticipate human errors and often miss the interconnections

between various system elements¹; not discovering design errors^{3, 4}; and weaknesses of the method itself and team competency⁵. Furthermore, there is a great disconnection between risk analysis methodologies and social factors (human and organization). The most comprehensive method is quantitative risk analysis, however, analysts have a tendency, to model only equipment failures that appear in databases whereas failure modes may differ widely and historical data may be orders of magnitude different from actual values for a case at hand. Apart from that there are many assumptions made on the nature and follow-up of unintentional hazardous material releases and consequence effects that leads to uncertainty. Often, uncertainty boundaries are vaguely defined. Also, in practice, a thorough review of risk assessment studies is rare.

1.1.2. Incidents over the years

Developments and advancements in areas of process safety and risk management have arisen and been implemented over the years in the industry. However, a retrospective look at the major incidents in the process industry as shown in Figures I.1 and I.2 reveal that incidents continue to happen globally⁶. It is evident from Figure I.1 that the incidents are global in nature with the maximum percentage of incidents reported in the United States. Figure I.2 illustrates the property damage for 100 largest losses in the last two decades in various business sectors. It can be seen that losses as high as 12,488 US million dollars have occurred in the upstream business unit. This data is supporting the fact that there is an increasing trend of incidents, complexity and degradation of the process systems.

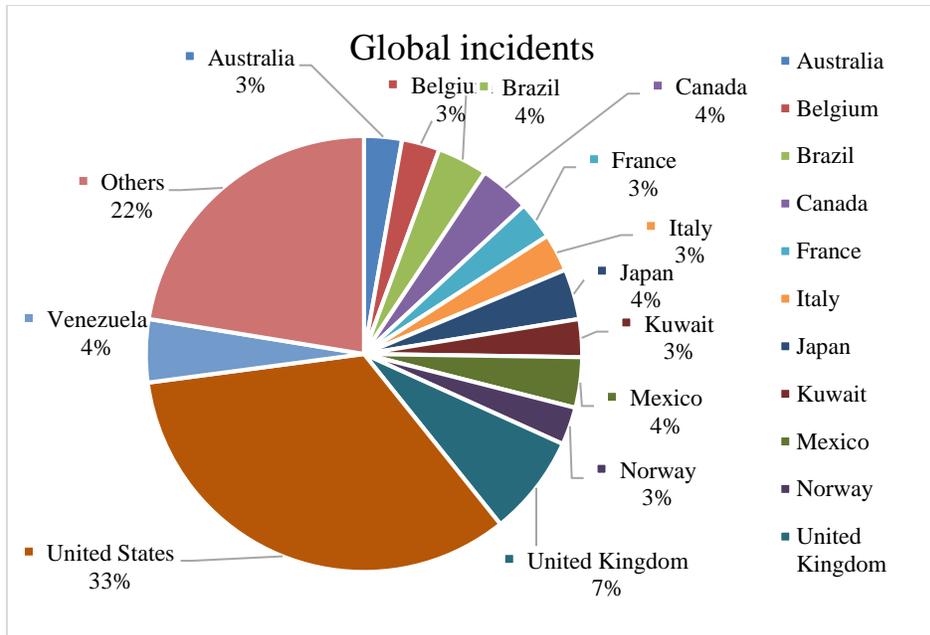


Figure I.1 Percentage of global incidents (developed using data from Marsh report⁶)

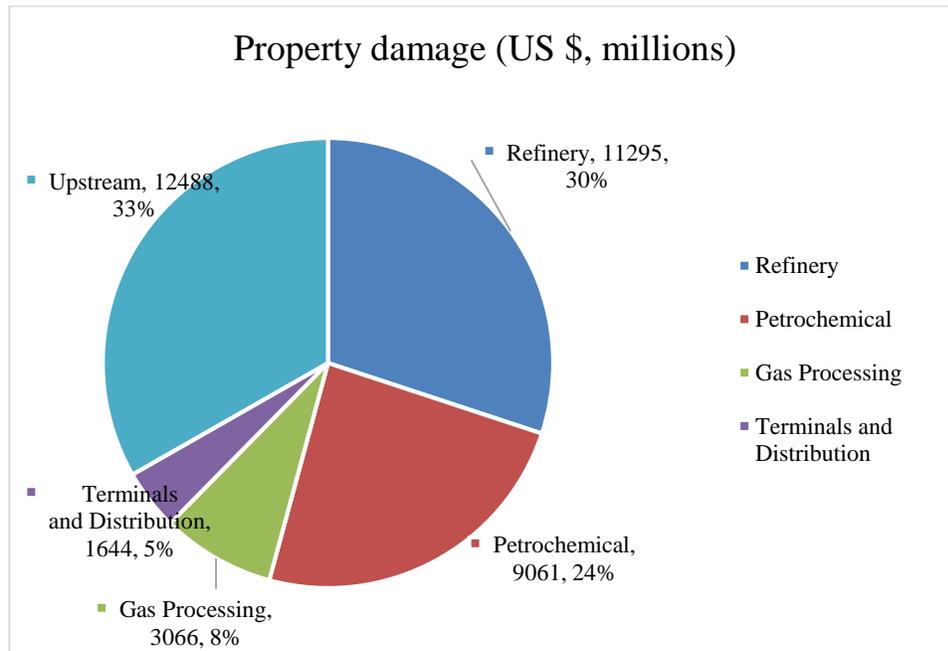


Figure I.2 Property damage (developed using data from Marsh report⁶)

1.1.3. Complex systems failure

Evaluating and managing risk for complex systems such as infrastructure – power, transport; the aerospace industry; the nuclear and energy sector; process industries; medical units; financial and business divisions, *etc.*, is critical for the survival and growth of the nation and its people. However, in the modern world one of the major challenges in the risk management of these is the relative lack of knowledge and expertise to deal with the uncertainties. Hence, looking at the risk problem from a systemic viewpoint will be conducive in effective risk management and thus avoid the conventional notions of risk independence. It is evident that it is the relationships between various components and parts of the systems and their structure that lead to many failures⁷. Examples of such failures of complex systems are summarized in Table I.1.

The research questions that need to be answered are - how do we address the systemic issues and elevate them to the attention of higher management levels, and more importantly do these complex systems require new approaches and models. For example, degradation of both process systems (due to ageing assets) and safety culture do not occur overnight. It is a slow process, which may not be perceived by many who are involved. However, can we make such organizational drifts visible with process system indicators and resilience metrics that are subject to temporal fluctuations? Therefore, what is needed is a new approach *i.e.*, the systems approach of resilience and hence recognition of process upset events as potential precursors of catastrophic incidents. This is all about early detection of weak signals and hence providing maximum time for a considered response.

Table I.1: Complex system failures

Sector	Failure	Brief description	Major reasons	Effects
Process industry ⁸	Bhopal, India, 1984 Union Carbide Methyl Isocyanate Release	Over 40 tons of (MIC) was released into the atmosphere and the toxic vapors spread into the nearby neighboring community	<ul style="list-style-type: none"> • Management failure towards accountability and corporate commitment to safety • No management of change system for evaluation of safe shutdown • Failure of safeguards on demand due to poor equipment integrity and operating procedures • Safety equipment such as scrubber, flare were not in service 	>3800 fatalities, >100 000 injuries, severe damage to area livestock and crops, long term health effects, \$470 M compensation
Medical ⁹	Josie, John Hopkins Hospital, 2001	Ninety-eight thousand people die every year from medical errors ¹⁰ . Communication system broke down and Josie was given a fatal dose of methadone	<ul style="list-style-type: none"> • Lack of communication between the different healthcare providers involved. • Lack of consideration for her parents' concerns 	18-month-old Josie King died of dehydration and a wrongly-administered narcotic
Financial ¹¹	Bear Stearns Companies, 2008	Financial firms much more susceptible to systemic risk due to high interconnections with one another Due to the collapse of the company, Bear Stearns was finally sold to J P Morgan	<ul style="list-style-type: none"> • Weak supervision resulted in undue risk and a failure to maintain sufficient capital 	Company was sold to JP Morgan Chase for \$10 per share, a price far below its pre-crisis 52-week high of \$133.20 per share
Aerospace ¹²	Challenger Disaster, USA NASA Explosion, 1986	The space shuttle Challenger exploded 73 seconds after launch	<ul style="list-style-type: none"> • Failure of one of the O-rings on one of the solid rocket boosters. Significant pressure on the NASA managers. • Policy related issues, <i>e.g.</i>, from policy, 'fully operational' meant that it could be used for routine operations (not test flights) and 'cost effective' was interpreted to mean that it could be launched on schedule without delays 	Loss of crew (7 fatalities), loss of space shuttle (>\$8 B USD), recovery of debris

1.2. Need for Advanced Risk and Resilience Assessment

Since the Seveso disaster 40 years ago, not only risk management methods, but also challenges to the process industry, have increased along with change in the public's risk perception globally. The Seveso incident brought to attention some critical issues, such as lack of knowledge on runaway reaction scenarios, hazards of formation of dioxins, lack of regulatory requirements, poor communication and coordination, and no emergency response or evacuation plans. Regulations related to process safety and risk management have evolved with time as compared to earlier when there were no specific regulations for controls of such major hazards as became evident during the Seveso incident. Some existing gaps are lack of learning from previous incidents, scale-up issues, limitations of experiments related to real scenarios (*e.g.*, vapor cloud explosion), uncertainties involved in complex systems and their gradual degradation. This necessitates developing and using advanced methods and a holistic approach such as resilience and advanced mathematic-statistical methods to resolve these issues.

1.2.1. Regulations

Regulations give a great impulse to improvement of environmental protection, and also of occupational and process safety, both in the United States (US) and in Europe. Regulatory regimes – safety case and US Process Safety Management (PSM) regulations are analyzed with regard to their effectiveness in preventing process safety events. In order to compare industry's safety performance within the different regulatory regimes and rationale behind the statements/claims made globally, a comparative assessment of the process safety performance of four countries was carried out: Australia, Norway, United Kingdom (UK) and US for two major sectors: offshore upstream and refining. Also, a brief

comparison based on data from an operator with global facilities has been included. As will be further addressed, the regulatory approach is only one of several factors impacting safety performance, and robust evaluation of such regulatory regimes should also consider operator and regulator roles and competency, age of facilities and inherent hazards.

The various country regulations evolved over time, with Norway the first to use a safety case approach in the 1980's, followed by the UK after the Piper Alpha incident and Lord Cullen report, and then Australia. US regulations themselves have evolved over time, with a combination of prescriptive regulations and the performance based PSM approach in 1992. Table I.2 presents the comparison between the safety case regulations and a more hybrid approach of US PSM regulations¹³.

Figure I.3 summarizes the differences between the two regulatory approaches by highlighting the various elements¹³. The Safety case approach covers more elements as compared to the US-based regulations.

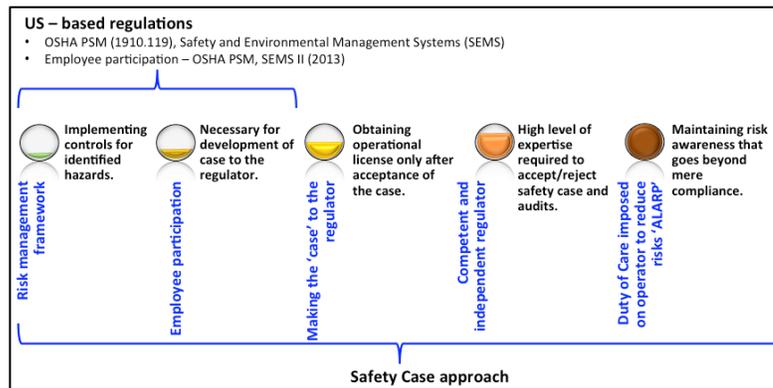


Figure I.3: Differences between the two process safety regulations

Table I.2: Summary: comparison of regulatory regimes

Safety Case	US PSM regulations
<p>A risk – or – hazard management framework</p> <ul style="list-style-type: none"> - Identifying controls to deal with identified hazards and measures taken to ensure continual working of the controls function. 	<p>Analogous to requirement of PHA by PSM standard</p> <ul style="list-style-type: none"> - 1910.119 states PHA ‘should be appropriate to the complexity of the process and shall identify, evaluate, and control the hazards involved in the process.’
<p>A requirement to make the case to the regulator</p> <ul style="list-style-type: none"> - Company demonstrates process of hazard analysis, and why certain controls are chosen over other. Safety case acceptance provides license to operate. - Regulator can impose higher standard on operators to respond to hazards. 	<ul style="list-style-type: none"> - US regulators do not evaluate and pass judgment of hazard management plans before allowing an operation to commence. - Misconception that safety case regulation is abandonment of prescription.
<p>A competent and independent regulator</p> <ul style="list-style-type: none"> - Safety case jurisdiction cannot be enacted. High level of expertise is necessary to accept/reject safety case. - Safety case changes what auditors do on the site visits. Rather than ensuring updated documents/working hardware, they need to ensure if specified control is functioning as intended. 	<ul style="list-style-type: none"> - Comments of US offshore safety regulator, James Watson, suggests that the agency does not intend to engage companies in the way that is necessary to impose safety case.
<p>Workforce involvement</p> <ul style="list-style-type: none"> - Employee participation is necessary for development of the case to the regulator. 	<ul style="list-style-type: none"> - PSM also requires employee participation. SEMS II, which became active in 2013 also requires employee consulting. OSHA requires inspectors to consult employee representatives on site, but no such regulation for offshore.
<p>A general duty of care imposed on the operator to reduce risk to ‘as low as reasonably practicable’ (ALARP)</p> <ul style="list-style-type: none"> - Provides leverage for regulators. <ul style="list-style-type: none"> o This is why fire protection standards on rigs in UK waters are higher than those in Gulf of Mexico. - Duty of operator to do whatever practicable to identify and control all hazards. <ul style="list-style-type: none"> o Operator cannot claim to be in compliance just because it has gone through hazard identification process. - If there is no directly applicable rule, operators still have a duty to manage risk. <ul style="list-style-type: none"> o They should maintain some reasonable level of risk awareness that goes beyond mere compliance. 	<ul style="list-style-type: none"> - Blind compliance mentality characterized by Minerals Management Service (MMS) regime. - US OSH Act. Section 5(a)(1) of the Act specifies that employers must provide a workplace that is “free from recognized hazards that are causing or are likely to cause death or serious physical harm.” <ul style="list-style-type: none"> o Impose a duty on employers only when the hazard is actually causing or likely to cause harm. o There is no rule that unequivocally requires adopting a performance standard.

1.2.2. Country-specific regulations

The country specifics are summarized below.

Australia

The Australian regulatory system is performance-based, but with prescriptive elements. There are different regulations on safety critical equipment and safety outcomes for exploration and production operations for various states in Australia. These include Petroleum (Submerged Lands) Act 1982 (Western Australia); Offshore Petroleum and Greenhouse Gas Storage Act 2010 (Victoria); Petroleum (Submerged Lands) Act 1981 (Northern Territory); Petroleum (Submerged Lands) Act 1982 (South Australia); Petroleum (Submerged Lands) Act 1982 (Tasmania); Petroleum (Submerged Lands) Act 1982 (Queensland); Petroleum (Offshore) Act 1982 (New South Wales); Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009.

Norway

Norway's regulatory system dates back to 1972 when the Norwegian Petroleum Directorate (NPD) and Statoil were created. The NPD has most of the responsibility as government's technical advisor and ensures companies comply with the obligations of the Norwegian regulations. Norwegian Maritime Authority, Norwegian coastal administration, and civil aviation administration eventually came on board as supervisory bodies for exploration and drilling, helidecks and so on. The regulatory system advocates a performance-based system with the major concern being minimizing the risk posed by various operations. The regulations provide flexibility with regard to the use of technology by encouraging use of standards to comply with the regulatory requirements. The Alexander L Kielland accommodation facility incident in 1980¹⁴ led to organizational

change, with NPD more involved in a coordinating role and other supervisory bodies acquired the role of providing technical assistance in their area of specialty to NPD. Petroleum Safety Authority (PSA), after splitting from NPD, came into effect in 2004 to administer safety and working environment¹⁵.

United Kingdom

The recommendations of the Lord Cullen report after the Piper Alpha disaster in 1988 were reinforced by implementing a new regulation, Safety Case Regulation. This is a goal-setting approach where the operator prepares a detailed safety case assessment of the hazards and actions to mitigate risk to an acceptable level, while the regulator is to provide an independent assessment that hazards and risks are being appropriately identified and managed. In 2005, UK HSE revised the Safety Case Regulations and included more details on significance of Quantitative Risk Assessment. The purpose of Offshore Installations (Safety Case) Regulations (2005) is to help in the reduction and mitigation of risks and hazards associated with the offshore installations and related activities. For onshore facilities, UK follows a similar regulation called Control of Major Accident Hazards (COMAH).

United States

As previously noted, the US approach to regulation has both prescriptive and performance-based aspects. The regulations provide minimum criteria of design, maintenance, and reporting to be achieved by each facility. A number of requirements or best practices included in voluntary standards and guidelines like API and ASME have been incorporated into the CFR. OSHA PSM applies to onshore facilities like refineries. It is considered a performance-based approach, requiring the operator to perform various

activities such as Process Hazard Analysis and Management of Change but the approach taken to meet those objectives is left to the operator.

The Minerals Management Service (MMS) was created in 1982 to manage oil, gas and mineral resources on the Outer Continental Shelf (OCS). It assumed responsibility to administer execution of activities in the OCS. The Macondo incident in 2010 led to major organizational reforms and discussions. Suggestions were made to adopt a performance-based regulatory system. MMS, which was renamed the Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE), was reorganized into two separate agencies – the Bureau of Safety and Environmental Enforcement (BSEE) and the Bureau of Ocean Energy Management (BOEM). The BOEM was given authority to manage environmental and economic development of offshore resources while the BSEE undertook the role of ensuring safety of offshore operations, permitting conditions, inspections, and the regulatory program. In 2010 an updated API recommended practice in the form of the Safety & Environmental Management System (SEMS) was put forth by BSEE to regulate offshore operations, with a performance-based format similar to OSHA PSM. SEMS contains the elements of PSM (*e.g.*, hazard analysis, mechanical integrity, emergency response) with additional third party facility audit requirements and inspections.

1.2.3. Results: Data analysis

Financial loss

Figures I.4, I.5, I.6, and I.7 give the non-normalized data for cumulative value of damage in million dollars for total, petrochemical, refinery and upstream losses, respectively. These charts are based on the “100 Largest Losses” report by Marsh ⁶. It is

evident from Figures I.4, I.5, I.6, and I.7 that there was progress made in safety in the US, Australia and UK since the installation of PSM and safety case regulations. However, the lack of a common and consistent normalization factor makes it very difficult to interpret the data appropriately. The number of major incidents has remained low in Norway over time, but all incidents in the database have occurred since the installation of the safety case regulation. US safety has generally improved since PSM has been implemented. The data also indicates UK's safety performance has improved since safety case was instituted. There is no clear distinction between performances among countries. There is improvement, but no country is a clear leader.

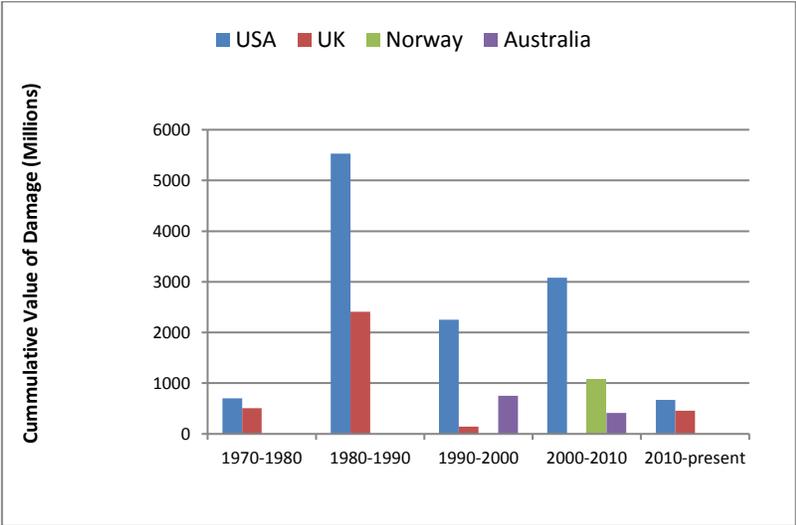


Figure I.4: Total damage

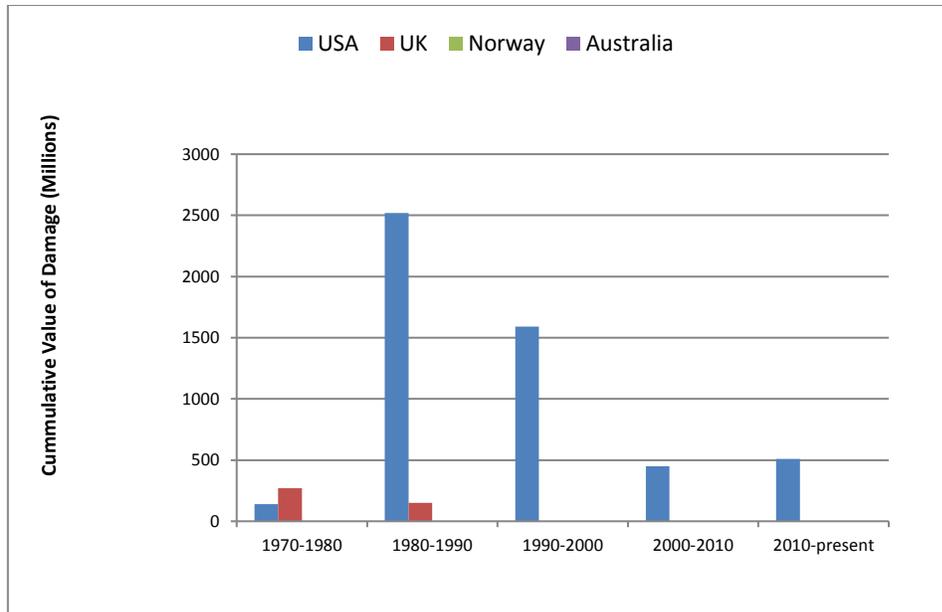


Figure I.5: Petrochemical losses

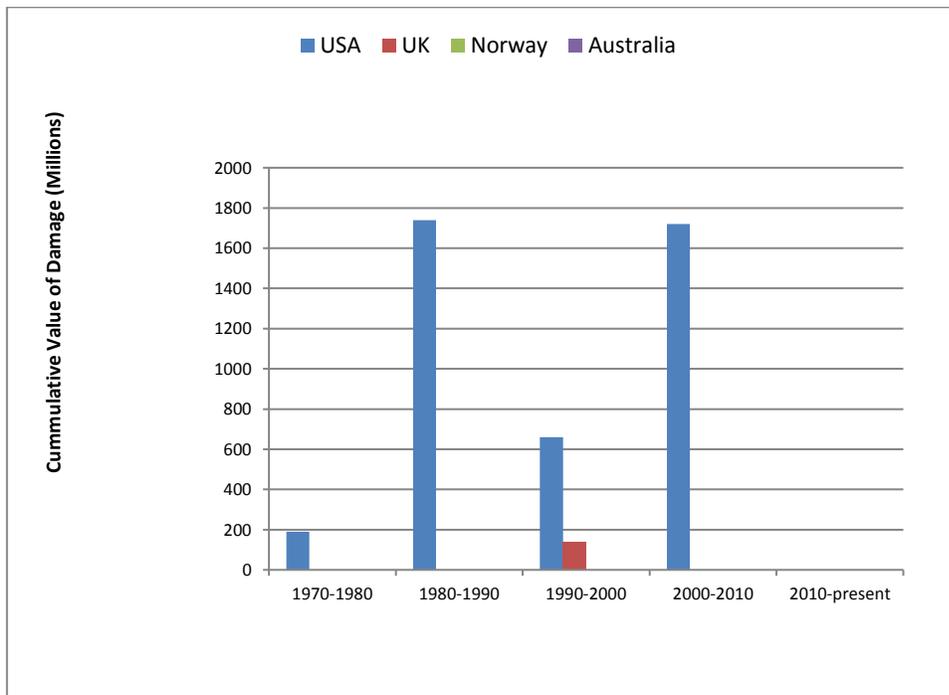


Figure I.6: Refinery losses

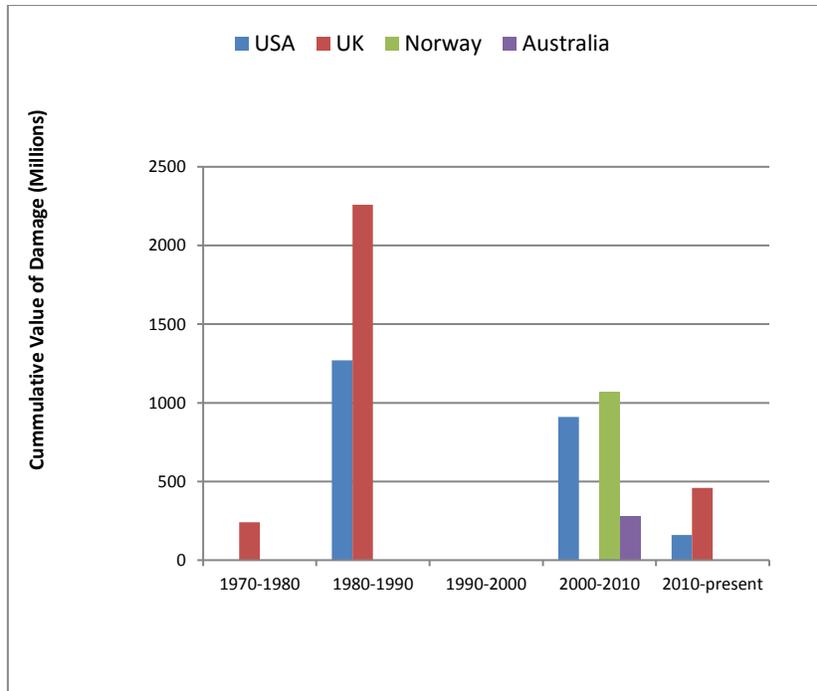


Figure I.7: Upstream losses

Process Safety consequences by country (offshore upstream)

This study presents an analysis based on the best available data. However, it should not be ignored that process safety performance data reporting and collection lacks a globally accepted criteria. There is a need of a universal system of process safety performance measurement, reporting and data collection. Process Safety performance of different countries is compared based on fatalities, major injuries, major fires and oil spills data from IRF and Oslo & Paris Conventions Commission¹⁶.

Table I.3 provides the number of events that are represented within the normalized graphs in Figures I.8, I.9, I.10 and I.11.

Table I.3: Process safety events (non-normalized data)

Countries	US	UK	Norway	Australia
No. of fatalities				
2007	4	1	1	0
2008	11	0	0	1
2009	4	0	1	0
2010	12	0	0	0
2011	3	2	1	0
2012	4	0	0	2
No. of major injuries				
2007	50	36	34	7
2008	70	38	31	13
2009	59	42	31	11
2010	78	44	27	9
2011	38	32	27	8
2012	49	46	29	5
No. of major fires				
2007	10	1	0	1
2008	4	0	0	1
2009	3	0	0	3
2010	1	0	0	0
2011	4	0	0	0
2012	9	0	0	0
No. of oil spills				
2005	146	438	147	-
2006	45	313	122	-
2007	37	279	167	-
2008	84	270	173	-
2009	42	299	146	-
2010	22	271	140	-

It can be observed from Figure I.8, that the US had fatal incidents every year and had the worst performance in three out of six years (2007, 2009 and 2010). Australia has two spikes for years 2008 and 2012, while Norway has a more or less flat trend. Hence, there is a varying trend and it is difficult to conclude which performance trends and thus which type of regulation is better.

Figure I.9 gives the normalized performance of the number of major injuries. The definition of the term ‘Major Injury’ has been developed by IRF based on HSE (UK) and PSA¹⁵ requirements. It is defined as any work-related injury that results in one or more of the following: amputation, skeletal injuries, burns, injuries to internal organs only if the injured person becomes unconscious, is admitted to the hospital, or requires resuscitation, eye injuries, any acute illness, hypothermia, any injury resulting in unconsciousness, resuscitation, or admittance to the hospital. It can be concluded from Figure I.8 that UK has the highest number of major injuries for three years - 2009, 2010 & 2012. Australia has a peak in year 2008. Norway’s injuries are typically +50% higher than US. All three safety case countries have a higher number of injuries than the US for all the years except for 2012.

Number of major fires per 100 offshore installations has been plotted vs. year as shown in Figure I.10. It is clear that there is no trend, although Australia has the worst performance for three consecutive years, and none since ‘09. US can be seen to have a relatively flat trend. Norway’s performance is best, followed by UK. Figure I.11 covers the number of normalized spills for three countries Norway, UK and US. It can be seen that the UK has the least number of normalized spills, closely tracked by the US with a decreasing trend. Norway’s normalized spills are comparatively high. As a reminder, the OSPAR database does not include Australian spills to water.

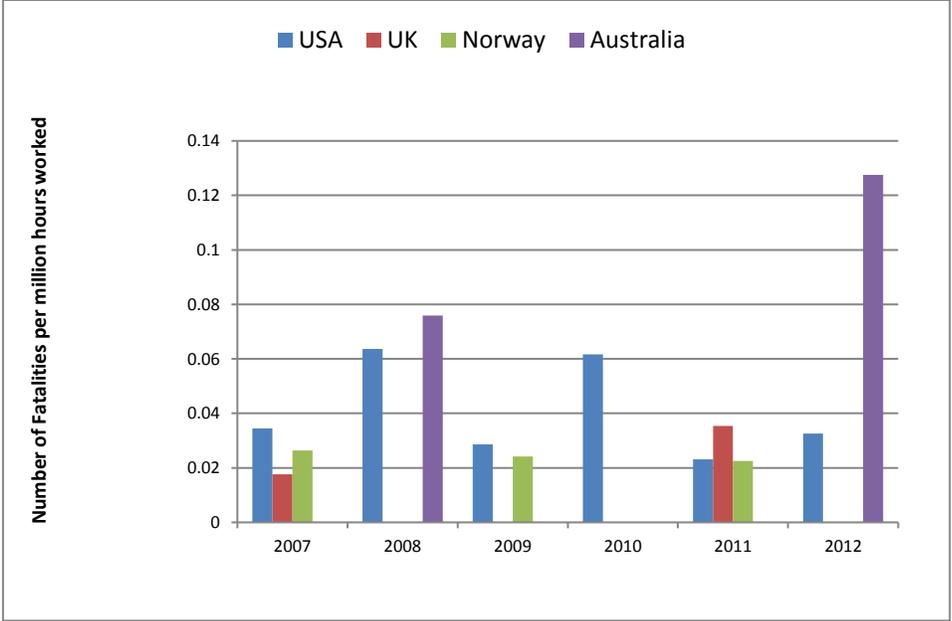


Figure I.8: Fatalities

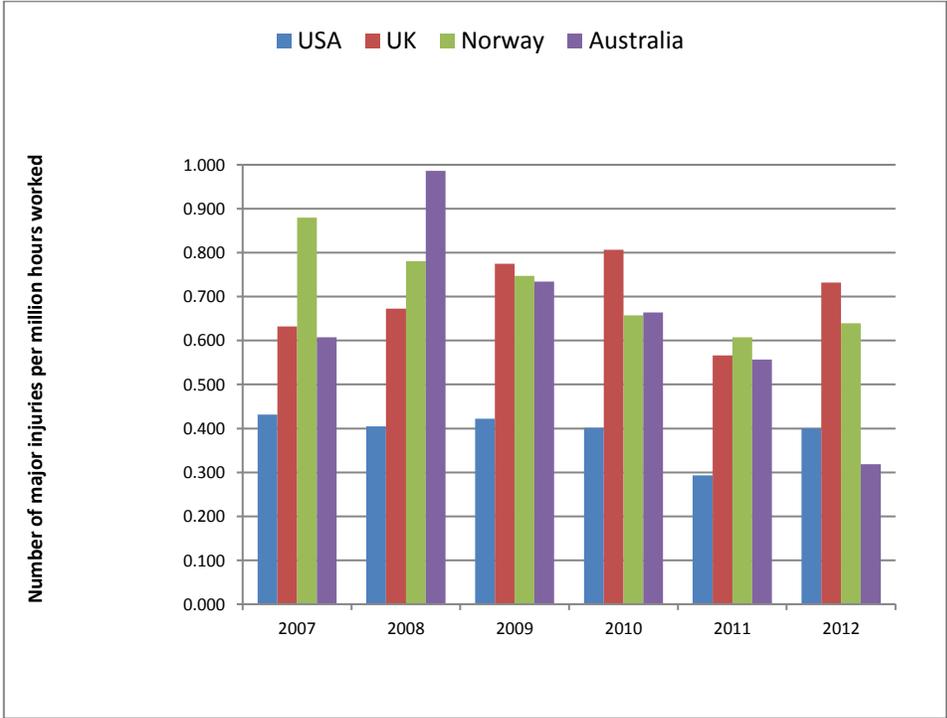


Figure I.9: Major injuries

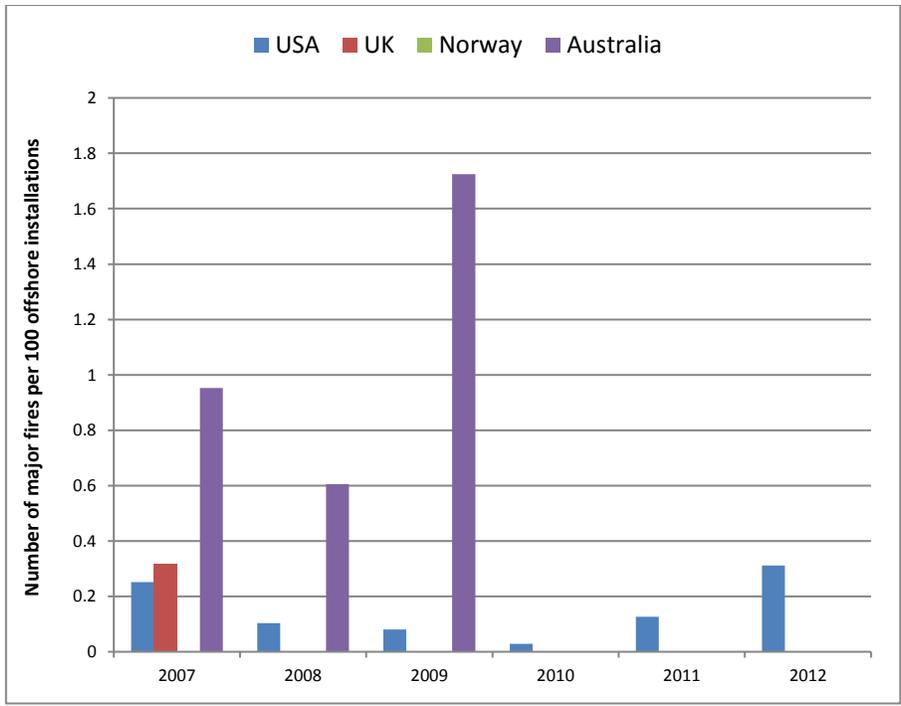


Figure I.10: Major fires

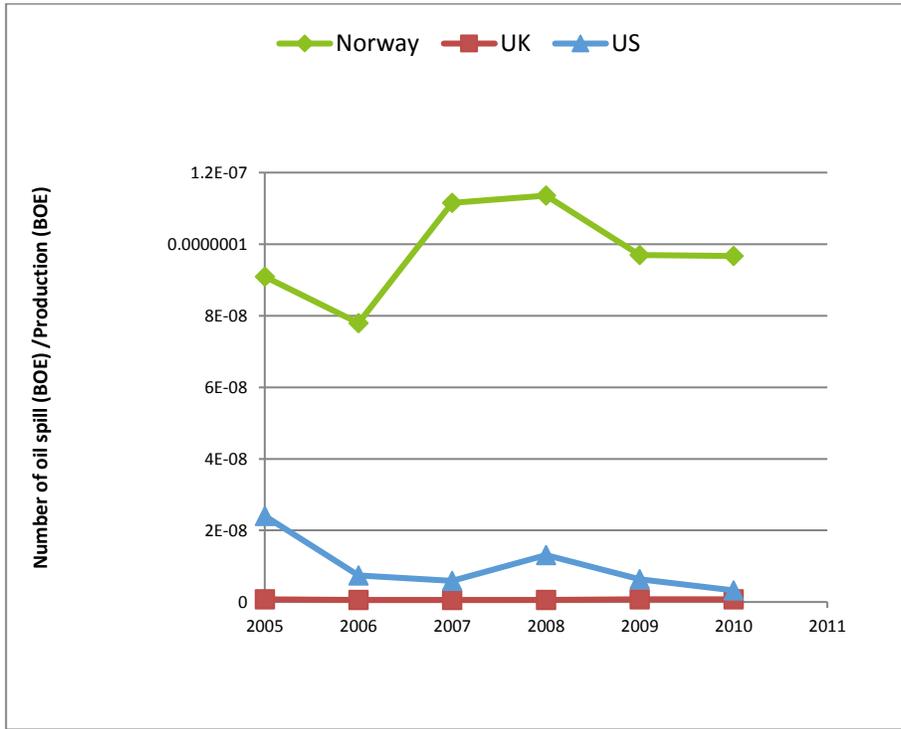


Figure I.11: Number of oil spills

Process Safety consequences by country (refining)

Incidents in refineries across four countries, US, UK, Norway and Australia were analyzed. The timeline for incidents was from 1994 to 2012 as per Marsh data. Figure I.12 shows the number of incidents per country per year. Here, it can be observed that the total number of incidents per year in the US is very high compared to UK, Norway and Australia. However, when normalized in Figure I.13 a more valid representation of the data shows that all countries have similar safety performance.

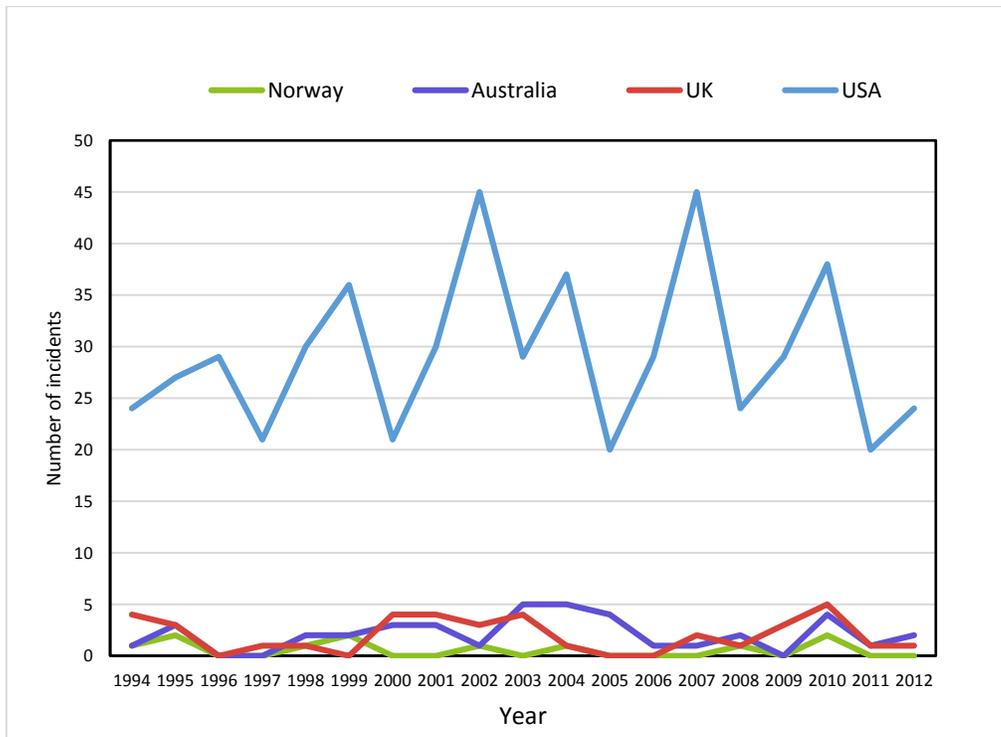


Figure I.12: Number of refinery incidents

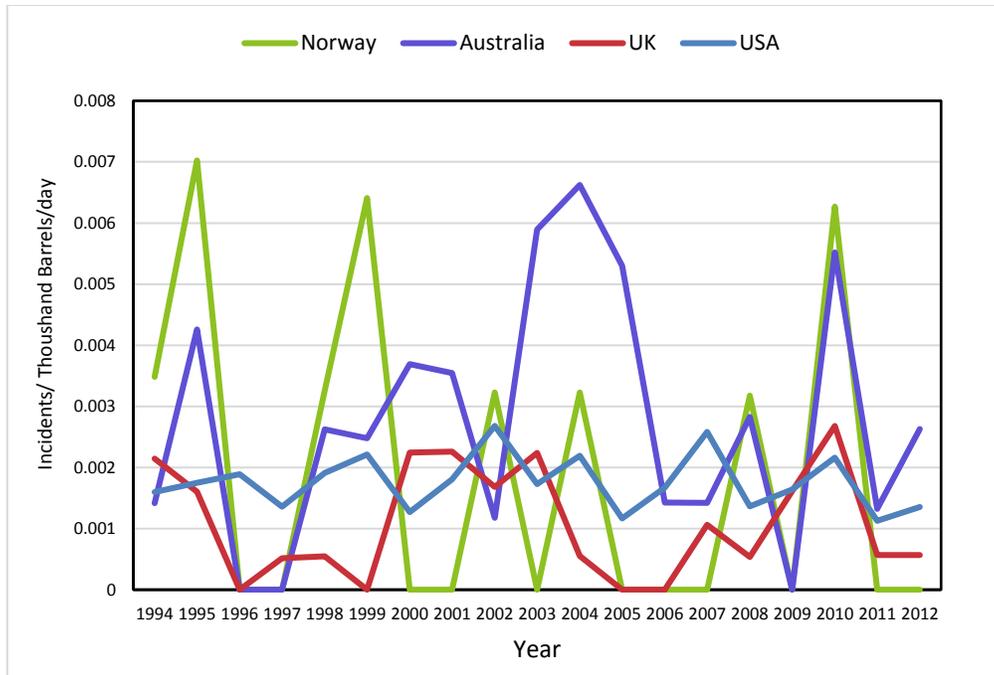


Figure I.13: Incident rate

The number of refineries in each country is quite different, as is the refinery capacity. For example, average capacity of refineries in the US in 2012 was around 17,737 thousand barrels per day (BPD) and for Australia in the same year a much more modest 760 thousand BPD. The Energy Information Administration (EIA) database was used to obtain the values of capacity of refineries for all countries from years 1994 to 2012. This capacity was used as a normalization factor to calculate the incident rate, defined as below.

$$Incident\ Rate = \frac{Number\ of\ Incidents}{Capacity\ of\ country\ in\ thousand\ barrels\ per\ day\ per\ calendar\ day} \quad (1.1)$$

Normalized refinery incident rates are shown in Figure I.14. The plot shows that there is no clear difference between the performances of countries with respect to safety. In some years, UK and Norway show remarkable performance with zero incidents, while in other years, Norway has highest incident rate among all countries. Australia has a few

peaks and a varying trend over the years. US performance is fairly uniform compared to others.

To dampen out the annual variation in Figure I.14, average incident rates for the four countries were calculated and are shown in Figure I.15. Analyzing the average incident rate per country, Australia and Norway data have higher rates than the US and the UK. The UK clearly has the best average performance on this metric. Fatalities were also computed based on the Marsh data and normalized using capacities obtained from EIA. Fatality rate was calculated by using the following formula:

$$\text{Fatality Rate} = \frac{\text{Number of fatalities}}{\text{Capacity of country in thousand barrels per day per calendar day}} \quad (1.2)$$

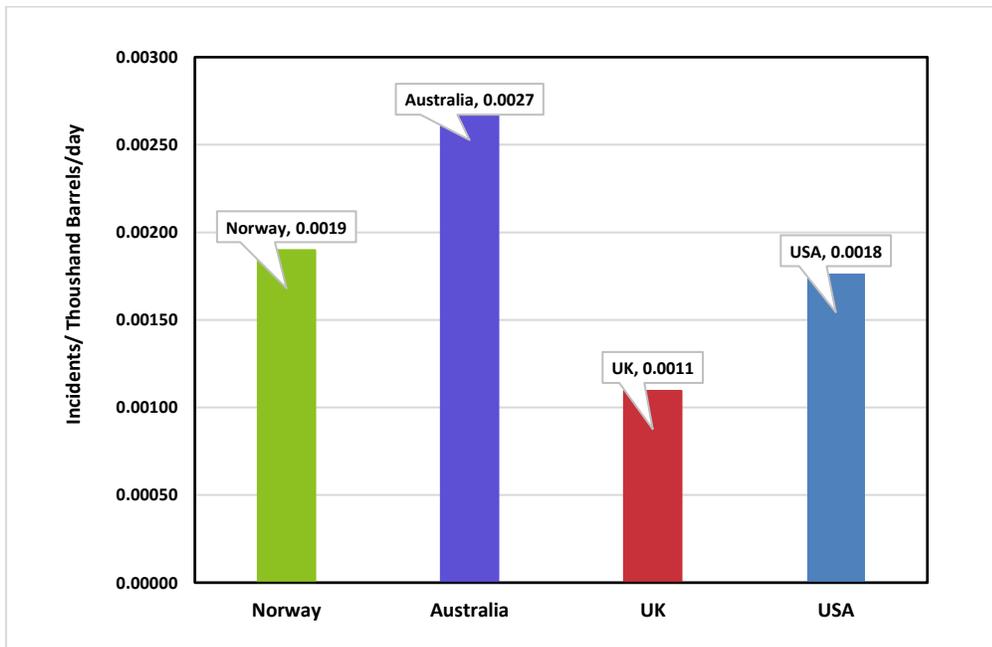


Figure I.14: Average refinery incident rate

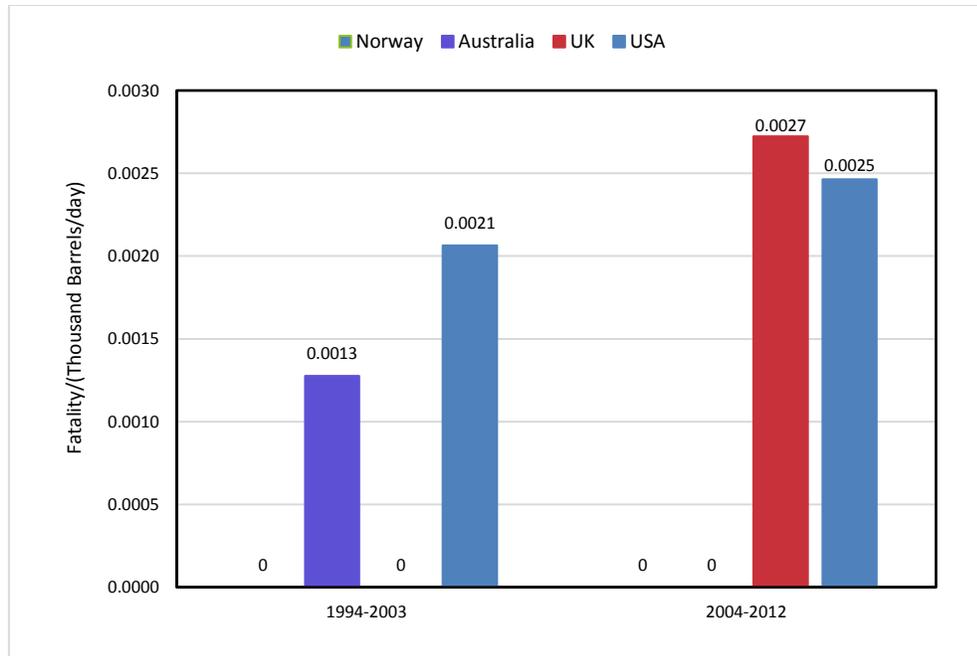


Figure I.15: Fatality rate

From Figure I.14, it can be seen that from years 1994-2012 Norway’s fatality rate has been exceedingly good. The UK fatality rate is more than the US for 2004-2012, and markedly less for the prior period.

Operator data

Data provided by an anonymous operator allows for a more definitive observation, based on API RP 754 Tier 1 & 2 incident data for 2014. Process safety incidents in the company’s refining and chemical operations in Europe and Australia where the safety case approach is used, were compared with those in the US, Canada, and other locations where the PSM approach is used. The operations are substantial, with over 50 million man-hours in aggregate for the included sites. Man-hours were used to normalize the incidents. Tier 1 incidents were 33% greater in the countries using the safety case approach and 16% greater for Tier 2 incidents, for an overall average of 19%. Similar results were obtained

with data from the prior year. No hypotheses are provided as to why the PSM countries had fewer incidents, nor is there justification to make definitive conclusions without data from additional operators over a broader time horizon.

In summary, based on the varying trends in fatality and incident rates one cannot conclude which country and which regulatory regime is best. Furthermore, aside from data limitations, Swiss Re, *et al.* have concluded that regulatory regime is just one of several factors influencing a facility's risk, including mode of operation, turnaround intervals, use of contractors, *etc.*¹⁷. Clearly such factors are also impacting safety performance as measured by lagging indicators. A more comprehensive and holistic systems approach of building process resilience including technical, human and organization factors would be useful. Hence, there is a need to explore and develop a Resilience Analysis Framework for process design as well as operations.

1.2.4. Knowledge growth and gaps

Altogether, knowledge about how to prevent environmental pollution and to maintain process safety is strongly developed. The growing knowledge resulted in designs, materials, and constructions becoming much more reliable and safe in use; new concepts were born such as fail-safe applications and inherent safety. The difference between hazard and risk became clear, and risk assessment started its development with consequence analysis methods describing the phenomenology of releases of hazardous materials in physical and chemical terms.

1.2.5. Process Hazard and Risk analysis

Process safety starts with identifying and locating hazards. Hence, HAZOP developed in the 1970s at Imperial Chemical Industries (ICI) in the UK became quickly a

“must-do” all over the world and found application in other engineering applications. HAZOP puts emphasis on operational hazardous situations that may be caused by bad design, procedures, human failure, and failure of critical safety measures. At the same time, techniques developed elsewhere in the military, aerospace, or nuclear power, such as Failure Mode and Effect Analysis (FMEA), were adopted for identifying potential component failures. Both still form the backbone of hazard identification as well as additional techniques, such as checklists and ‘What-if’. However, application of the techniques does not guarantee that all hazards are found. Not at all, and for a variety of reasons as pointed out recently by Leveson from a system’s point of view and by Baybutt from human failure in the HAZOP team^{18, 5, 19}. Heavy computerization as proposed by Cameron and coworkers in their Blended Hazid (BLHAZID) approach offers good perspective, but still more can be done²⁰.

Parallel to the early HAZOP and FMEA developments have been those in reliability engineering. Reliability thinking enabled mapping failure causation in complex installations, such as fault and event tree analysis. Where fault trees from basic failures merge and end in a top-event, which in processes exist as a hazardous release, event trees branch out to possible subsequent events such as evaporation, dispersion, and ignition et cetera, to final events with major consequences. Hence, with these tools in the 1980s risk assessment came off the ground with defining risk metrics, such as the individual and societal risk, and the use of risk matrices. Some countries in the EU adopted risk assessment methods for land use planning, others kept the basis of a license procedure to calculate effect distances based on threshold intensities of toxic concentration, radiant heat, and explosion blast²¹.

With respect to physical effects of mishaps since the 1980s, many simplifying models have been developed. As computational fluid dynamics (CFD) became faster over the years, more sophisticated, and professional, it developed into quite a powerful tool for predicting consequences of mishaps, such as cloud dispersion and explosion effects. Toxicologists formulated probit relations to assess lethality risk as a function of exposure to a toxic cloud, while also probits were obtained for the effect of explosion blast on structures and the probability of injury and fatality by radiant heat. A considerable number of commercial CFD and Finite Element (FEM) codes have become available. Like the EU SMEDIS project in the 1990s, a verification and validation protocol for these codes would strengthen confidence in the results. Where effect and damage models are producing in the end the magnitude of safe distances, this will be of high importance, both in accidental and potential terrorist attack situations.

In the middle of the 1990s developments in electronics and automation enabled introduction of safety instrumented systems, while at the same time CCPS' Layers of Protection Analysis (LOPA), started its tour of conquering the world²². Difficult cases, however, still depended on Quantitative Risk Analysis, also known as Probabilistic Risk Analysis. At the end of the 1990s it became clear that the basis of risk assessment results was still far from being sound and solid. This initiated work to improve QRA methodology: Bowtie became popular, and ARAMIS brought QRA a step further²³. Following this is the work of Cozzani and colleagues facilitated developing methods and acquiring data to include domino scenarios leading to cascading effects and escalation, and risks of natural threats, such as earthquake, flooding, storms, and lightning enabling protection requirements²⁴.

1.2.6. Safety management

Already early on, the effect of human actions and organizational factors to influence accident occurrence has been recognized, but it took until the middle of the 1980s before management became aware that they were key in having a good level of both occupational and process safety. Safety management gave a boost to understanding the management influence on human failure, and the interest of taking adequate organizational measures such as regarding roles, training, procedures, incident investigation, audits, and emergency planning.

All of these measures reduced the number of accidents significantly, but not sufficiently, and certainly not the major ones. There were no indicators to measure the trend other than personal safety indicators, such as lost time incident rate and fatal accident rate, *i.e.* metrics of failure. Meanwhile, there is industry-wide fair agreement on lagging process safety performance indicators such as hazardous substance releases above a minimum threshold quantity depending on properties. However, with respect to the many possible leading indicators, which in the end are more important because their nature is predictive, more work must be done.

Following a system approach, probabilistic predictions to supplement deterministic (usually not available) and covariate models reduce the uncertainty of when an event, such as an upset, is expected to occur under specified conditions. Therefore, using traditional and Bayesian methods, prediction within a socio-technical system is consistent with a scientific approach in the same way that the Higgs boson was identified and validated (to 5.9 sigma, 1 in 588 million) by probabilistic methods developed in 20th century science to

model uncertainties that were established to be inherent in all reality including engineering socio-technical systems.

1.2.7. System approach, complexity, causality

Rasmussen's idea of a system approach and its dynamics (socio-technical system), which has been much further expanded and elaborated by Leveson is very helpful in battling complexity and obtaining a more comprehensive view on accident causality^{18, 25, 26}. Leveson proposes a control loop approach to identify possible causes by deficiencies in the four elements of the loop (controlled process, sensor, controller, and actuator) at the various levels of the socio-technical system from shop floor via management and board up to government authority. In this way any possible cause whether in organization, human action / in-action, or in technology, either in design or operation, including software should become identified. Causes will include faults by dysfunctional interactions of by themselves safe and well-functioning components. This way of thinking is very promising, but it still lacks a workable computer tool to handle the masses of data needed to predict possible scenarios required for effective risk management. As Kahneman observes, a human is too focused by the WYSIATI (What you see is all there is) limitation and a human's availability heuristic to anticipate well unexpected event chains²⁷. For prediction of potential mishaps, we shall need a fast and sensitive cause identification system and as mentioned before, HAZOP is not sufficient.

1.2.8. Uncertainty, Fuzzy logic, Bayesian statistics and networks

Uncertainty is inherent to a possible risk event and is expressed in its likelihood or rather probability of occurrence. Predicting a risk quantitatively requires determination of the value distributions of consequence and probability, which are both afflicted with

uncertainty in their value, because of uncertainty in the data that were used to estimate these distributions. In QRA in particular, the uncertainty in estimated probability can be easily one or two orders of magnitude. And when it concerns a rare event, which is mostly the focus of interest, validation is not possible. This problem has surfaced in EU-projects such as ASSURANCE²⁸, and it led to much skepticism about the sense of performing QRA. The main problem of scenario definition was already noted. Another problem are the failure data. There have been several initiatives to establish equipment failure databases of high quality with public access to facilitate QRA. The known ones on data collected in offshore operations are those by HSE UK and OREDA^{29, 30}. Reported failure data often do not include human operational or maintenance error. Moreover, failure frequency of a component is not only because of its individual behavior or operational treatment but also due to cascading or escalating effects by failure elsewhere. To apply with confidence a decision criterion such as As Low As Reasonably Practicable (ALARP), the assessment results must include confidence limits.

During the last decade ‘possibilistic’ and probabilistic techniques such as fuzzy logic, Petri nets, and in particular Bayesian statistics and Bayesian networks (BN) have become widely applied to enable decision making predictive statements about uncertain events involving risks. These methods helped greatly to incorporate expert knowledge, to model relationships among random, often dependent variables; the latter even in a dynamic sense enabling monitoring of slow and fast changing risk levels. BNs are also well suited to map effects of management and human failure on operational performance. Another application of Bayesian statistics is to estimate rare event frequency on the basis of measured frequencies of various types of more commonly occurring precursors of the

event and related events. BNs are also useful for dynamic risk analysis of processes by failure enhancement due to degradation, while in combination with HAZOP results BNs can help operators locate more quickly the most likely causes of an abnormal situation. They then can prioritize actions to reduce risk and lower probability of upset.

Altogether, there is still much work to do to exploit mathematical-statistical methods, reduce value uncertainties and make risk predictions more accurate. An overview and summary of process and plant risk control and management over the years and a further outlook on methods/approaches has been given by Pasman, 2015³¹. A recent perspective article on trends and challenges in process safety is by Mannan et al., 2015³².

1.3. Looking into the future: top-down problem analysis

Major accident hazards and associated risks are still present. Will we be able to provide all needed products by running small decentralized units? Can we avoid large quantities of flammables and toxic materials? No, the future with protection of the climate and requirements of sustainability will probably demand large industrial agglomerations of specialized plants that are dependent on each other for energy, feed stocks, and products. As humanity will further grow in numbers, demand quantities will not decrease, and although final products may be safe, many unavoidable intermediates will not be safe. In addition, the number of new processes applying, *e.g.*, biomaterials, will grow. More sustainable fuels such as hydrogen will in large quantities not be without hazards, to say the least. Process intensification may limit reactor volumes or even result in mini-reactors, and combine unit operations, which will undoubtedly favor safety. But most often the trouble is associated with large quantity; manifolds, purification processes, storages, and transport will still handle large quantities. Hence, complexity will not reduce but probably

grow and lead to failure outcomes with increased frequencies and consequence severities. Will economics relax or will competition and therefore pressure on cost further increase? Probably the latter will occur. Reputation and reliability will be valued. It will ensure that company management cannot afford a major mishap. Anyhow, risk control, risk communication, and risk governance with involvement and education of stakeholders with shared responsibility for major decisions and risk will remain of utmost importance. With this, we arrive at setting the requirements for a High Reliability Organization of which resilience is a fundamental prerequisite³³. Although used so far in the context of organization we intend to expand its meaning to the whole socio-technical system of a technical system within its organization. So, what is exactly meant by resilience, what can we do to assess it and what is a satisfactory level of it?

- The requirement that regulators have to drive forward and provide a just environment within which the taking of short cuts, or adopting strategies with a high risk, is unacceptable.
- Industry then must sign up, enthusiastically, to working to best available current standards and practice - the risk taker has to be made an outcast.
- There then is a requirement to produce safety professionals by providing appropriate education, training, experience and attractive career paths. This will include training so that those in industry are fully up to date with techniques, strategies and skills that they will need to understand and possibly use - *e.g.* the activities of MKOPSC and others, degrees, short courses, distance learning, case studies, safety professional qualifications, safety passport, *etc.*

- At the same time researchers also need to develop new concepts, tools, methodologies, software, *etc.*, so that safety professionals and the field of process safety continues to advance - *e.g.* tools of the future - resilience, blended HAZID, Bayesian network, *etc.*

An important factor that works against improving safety is the usual absence of a comprehensive system approach where all relevant information is analyzed. Another attribute of a system approach is to include the organization and human interface in the measurements, modelling, updates, and management together with the technical system with a chemical process, for example.

Another characteristic of the system approach is to identify and model significant interdependencies, identified from a risk assessment, rather than unrealistically assuming a priori that the individual components behave independently. The system approach also models important time dependencies and the effects of condition ranges on observed data, component behavior, frequency of occurrence, and outcome consequences.

1.4. Research challenges and objectives

As stated earlier, there exist limitations in existing risk assessment and management methods. Primarily, the current methods follow a disintegrated approach. There are two aspects to this, first, there is a disconnection between technical and social factors and second, lack of data sharing between the process simulation, maintenance, and safety. Further, there exists limitations to using data for evaluation and relying on values from literature and without gaining any insights about the plant performance. Additionally, methods need to be developed and implemented that capture meaningful information from weak signals or precursor data and also study impact of uncertainties to major key

performance indicators for the process or business at large. Figure I.16 (original figure by Visser; modified by Knegtering and Pasman) shows the progress or evolution of various methods/policies/developments that have happened over time^{34, 35}. In spite of these, as seen earlier, incidents continue to happen globally. Lack of knowledge can contribute significantly to the cause if the accidents were not each investigated, learned from, and actions taken beyond immediate causes to causes that always implicate and entangle the management, leadership, organizational, and human factors. The next level is to adopt a more comprehensive and holistic systems approach of Resilience towards process safety and risk management.

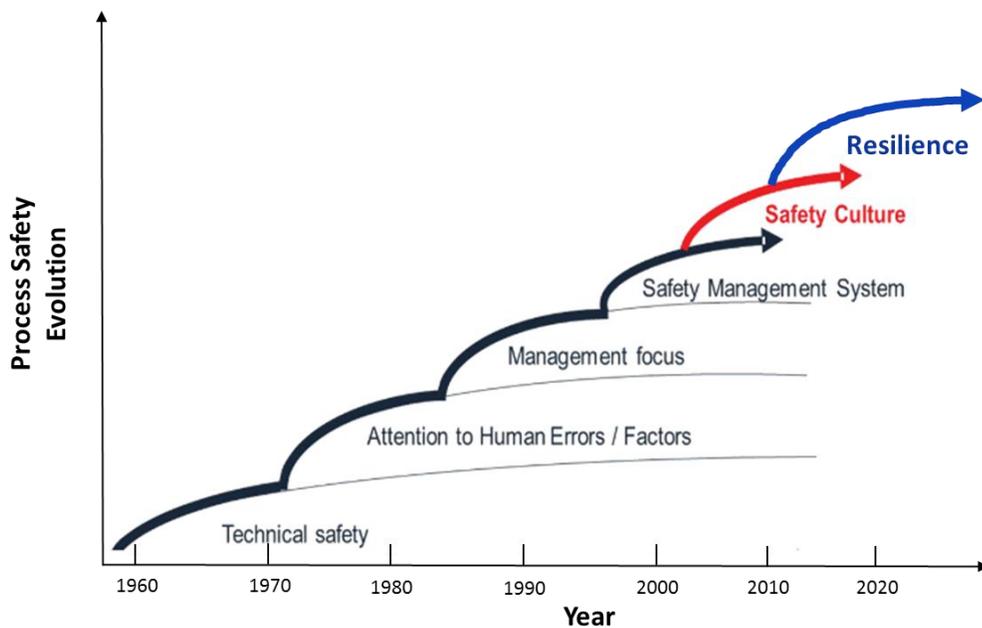


Figure I.16: Evolution in process safety and risk management methods

In order to address the challenges identified, this research has the following three prime objectives:

1. **Predictability:** predict the process upset situations or events and find the maximum bounds of the feasible operational region while satisfying any process, and safety constraints. This would result in stability of process systems under uncertainties and better flexibility and control of the process system under study.
2. **Survivability:** to determine the optimal operations and maintenance strategies by establishing an integrated method to incorporate process, maintenance, and safety models. The impact is improved reliability and maintainability of the process system while a reduction in unplanned shutdown or downtime.
3. **Recoverability:** to establish strategy for emergency response using scenario-based analysis. This would result in reduced severity of consequences, and response time and overall enhanced recovery.

Therefore, Process Resilience Analysis Framework (PRAF), is developed that would help achieve these objectives and hence lead to data-driven, process model-based, cost effective more informed decision making for process design and operations. This would deliver business continuity as well as add business value.

1.5. Summary

In general, it can be concluded that indeed much has been achieved. Many lessons have been cast in regulation, standards, codes, and practices, both in design and operation. But at the same time our methods to identify possible scenarios, to predict abnormal situations arising and with that to prevent mishaps are still far from perfect. However, various methodical avenues can be further explored. For risk control, the complexity and non-linear behaviour of process plant and supporting systems require a system approach.

A detailed research on resilience engineering methods to integrate both technical and social factors based on systems approaches would help to understand process upset/incident situations better and thus support resilience of such socio-technical process systems. Resilience for a system or a leader implies the ability for the system or a leader to anticipate, respond, adapt, and learn from unexpected situations, again showing the need for socio-technical system modeling, management, and resilient leadership. In a sense rather than a new method, the system approach reveals the emphasis that should always have been placed on organizational and human factors, which are sensitively engaged in and influence the underlying causes, root causes, and the concomitant implications, *e.g.*, for acceptable regions of risk rather than acceptable point values of risk. The concept of resilience helps us understand the relationship of complexity, uncertainty, organizational factors, leadership, and system culture, which understanding can increase our optimism about future deliberations to build credibility and confidence in a comprehensive socio-technical approach for optimum decision making and risk management.

Catastrophic incidents and failures of complex infrastructure and systems have led to an increased significance of a systems approach to risk management³⁶. These complex systems can be characterized as a combination of several technical and social sub-systems interacting with each other in specific, usually non-linear patterns. One example of such complex socio-technical systems is the process industry that includes chemical plants, oil and gas platforms, and onshore and offshore installations. The process industry is an indispensable part of today's modern society considering the critical products it provides for consumption, for sustenance of its members, and maintenance of the infrastructure. However, over decades due to disastrous loss of containment³⁷ incidents, augmented risk

and challenges to process safety management of such systems has been acknowledged. Social factors like regulations or policy related matters, human, and organizational factors have been acknowledged to play a crucial role in process safety and also in maintaining the efficiency of technical barriers to prevent high consequence events. Consequently, an interest in an integrated systems based approach of resilience engineering has arisen which considers both technical and social factors in a single methodology and aims to strike a balance between various performance requirements of such systems³⁶. Increased research and application of the resilience engineering concept is evident in various sectors such as ecology, the environment, psychology, *etc.*, in past years. However, process systems resilience has substantial need for a quantified framework to exhibit standardization and development of process resilience aspects and principles³⁸. Typical property of a system is that the whole is more than the sum of its parts, which makes it complex. Process safety incidents emerge due to inability or failure to understand these complex interactions. A resilient process system will be able to survive better when subjected to such unknown and unforeseen threats.

The key contributions of this work are:

- A standard process system resilience framework called *PRAF - 'Process Resilience Analysis Framework'* with a unified taxonomy.
- 24 process system resilience metrics including both technical and social aspects have been developed.
- A PRAF survey has been conducted and survey response has been analyzed to answer the three research questions related to incorporation of the resilience metrics in the risk and/or resilience assessment – what are the

most important metrics for each of the three phases of PRAF – avoidance, survival, and recovery?, are there any differences in viewpoints of various groups of survey respondents?, what are the weights or level of importance for each of the metrics?

- A new resilience-based and integrated systems approach for hazard analysis called *RIPSHA – ‘Resilience-based Integrated Process Systems Hazard Analysis’*.
- A predictability assessment methodology to predict process upset situations and hence have better flexibility and control of process system.
- A Bayesian based method for uncertainty quantification.
- A novel and integrated method of survivability assessment using PRAF. A novel metric called SSI – ‘*System Survivability Index*,’ was incorporated as the system safety threshold to analyze the safety impact costs.
- A summary of concepts of business continuity, sustainability, process system resilience and their relationship based on an incident case study.

Chapter II presents a literature review of the previous developments on which the Process Resilience Analysis Framework (PRAF) concepts and model formulations presented are based. The review covers the previous work carried out in system resilience and resilience engineering, risk and resilience assessment of process systems, and modeling aspects of process system resilience. The foundations of the proposed framework PRAF are formally introduced in Chapter III. In Chapter IV, a novel resilience-based qualitative method for hazard analysis called Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA) has been proposed. A thorough predictability assessment

analysis procedure has been formally proposed in Chapter V, for the identification of the process upset situations or events affecting the flexibility and control of the process system under study. In Chapter VI, a novel method of survivability assessment using PRAF has been presented. The concepts of business continuity, sustainability, process system resilience and their relationships are explored and presented in Chapter VII. Finally, the concluding remarks and recommendations for future work are summarized in Chapter VIII.

CHAPTER II

BACKGROUND: PREVIOUS WORK AND LITERATURE REVIEW*

In this chapter, the literature review is presented, which outlines the concepts and previous developments in areas of resilience, resilience engineering, process resilience, and resilience modeling. First, the concepts of system resilience and resilience engineering are discussed. The fundamentals of resilience are outlined, along with the definitions and various research areas where the concept has been applied. Finally, a literature review of the modeling aspects and resilience concepts in the area of process risk and resilience assessment is provided. This section covers the previous work in the fields of process risk analysis and reduction, systems thinking, early fault detection, and dynamic simulation and optimization. These fields capture the resilience engineering implementation in the process industry.

2.1. System Resilience and Resilience Engineering

In recent years, there has been an increase in research literature on the application of resilience concepts in enhanced risk assessment and management^{39, 40}. For example, book by⁴¹ marked the maturation of a new approach to safety management and the chapters explored different facets of resilience. The work of⁴² and ⁴³ demonstrates the simulation and optimization modeling of technical processes with respect to flexibility and operability. ⁴⁴ analyzed the Columbia disaster using Resilience Engineering concepts, and concluded that resilience perspective will create foresight about the changing patterns of

*Reproduced in part with permission from Jain, P., Pasman, H. J., Waldram, S., Pistikopoulos, E. N., & Mannan, M. S., "Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management," JLPPI, Vol 53, Pages 61-73. Copyright 2018 Elsevier Ltd.

risk before failure and harm occurs. ⁴⁵ introduced the Resilience Analysis Grid to provide a well-defined characterization of a system that can be used to manage the system and specifically to develop its potential for resilient performance. ⁴⁶ proposed six resilience aspects for safety in chemical industry. ⁴⁷ used a survey method to identify deficiencies related to Resilience Engineering by measuring seven safety culture indicators and managerial factors. Francis et al. proposed a resilience analysis framework incorporating absorptive, adaptive, and restorative capacities⁴⁰. ⁴⁸ used the mathematical programming approach to identify the most important factors of integrated managerial and organizational factors.

Various researchers have defined ‘resilience’ in different contexts and viewpoints as presented in Table II.1. The following are some aspects identified from these selected definitions:

- no common definition of resilience or resilience engineering;
- ‘resilience’ is closely related to ‘Robustness’ in various definitions;
- resilience definitions are applied to numerous categories: safety, critical infrastructure, business process, supply chain, organization, and ecological/environmental;

most of the definitions imply post-event analysis.

Table II.1 Resilience definitions

Year	Definition	Research area	Reference
1973	A measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships.	Socio-ecological systems	49
1999	Disaster resilient community is a community that can withstand an extreme event, natural or manmade, with a tolerable level of losses, and is able to take mitigation actions consistent with achieving that level of protection.	Disaster resilience	50
2004	The capacity of a system to absorb disturbance and reorganize while undergoing change so as to still retain essentially the same function, structure, identity and feedbacks.	Socio-ecological systems	51
2006	A balance of stability and flexibility that allows for adaptations in the face of uncertainties without losing control.	Organizational system	52
2006	The capacities for an enterprise to survive, adapts, and grow in the face of turbulent change.	Economic systems	53
2006	The loss and loss recovery required maintaining the function of the system with minimal disruption.	Seismic resilience	54
2006	The ability of an organization to cope with unexpected and unplanned situations and respond rapidly to events, with excellent communication and mobilization of resources to intervene at critical points.	Safety systems	55
2007	The maintenance of positive adjustment under challenging conditions such that the organization emerges from those conditions strengthened and more resourceful.	Organizational system	56
2011	The ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks.	Safety systems	57
2012	The ability to bounce back when hit with unexpected demands.	Safety systems	46
2012	In order to be resilient one needs to learn to ‘bend, but not break,’ and acknowledge that adaptability is more important than hardiness.	Nursing	58
2014	The capacity to cushion stresses and disturbances while maintaining or improving essential properties and functions.	Society-ecology	59
2015	The ability to mitigate hazards, contain the effects of disasters when they occur, and carry out recovery activities in ways that minimize social disruption and mitigate the effects of future disasters.	Business continuity, resource allocation	60

Table II.2 provides information on resilience engineering application areas.

Table II.2: Resilience engineering applications

Year	Application	Description	Reference
2016	Business planning/Entrepreneurship	Effective decision-making to social as well as business costs following an entrepreneurial failure	61
2014	Healthcare	Possible applications of resilience engineering in health care	62
2015	Safety	Explore everyday operations of the Vehicle Traffic Service system to gain insights in how it contributes to safe and efficient traffic movements	63
2013	Healthcare	Improve patient safety	64
2014	Petrochemical	Performance evaluation of integrated resilience engineering	65
2014	Petrochemical	Assess the factors affecting the plant resilient level	66
2016	Seaport systems	Resilience modeling of maritime systems using Bayesian belief networks	67

Main characteristics of selected resilience and resilience engineering studies are summarized below:

- Resilience theory and concepts

Woods grouped the various uses of the word ‘resilience’ into four basic concepts – rebound, robustness, graceful extensibility, and sustained adaptability⁶⁸. In the healthcare industry, Aburn et al. identified the following common themes - rising above, adaptation and adjustment, dynamic process, ‘ordinary magic’ and mental illness⁶⁹. The authors in this research also concluded, ‘there is no universal definition of resilience.’ Within the area of adulthood and psychology, Infurna et al. summarized five tenets characterizing the resilience framework for research, practice,

and policy⁷⁰. Francis et al. summarized the concept of resilience in terms of a triangle with three major capacities of absorptive, adaptive, and recovery/restorative⁴⁰.

- Research areas

Righi et al. identified six research areas based on the systematic review conducted by them⁷¹. These areas are theory of resilience, resilience identification and classification, safety management tools, accidents analysis, risk assessment, and training. Linnenluecke analyzed literature published between 1977 and 2014 and concluded that the resilience research has developed into five research streams⁷². These streams are organizational responses to external threats, organizational reliability, employee strengths, and the adaptability of business models or design principles that reduce supply chain vulnerabilities and disruptions. The other related disciplines that have also been discussed in existing literature are systems engineering, Normal Accidents Theory, and High Reliability Organizations—HRO.

2.2. Process System Resilience Modeling Aspects

The sociotechnical hierarchical structure has also been considered by²⁵ and⁷³ as a basis for analyzing holistic risk control of systems, while the organizational aspect has been emphasized in the resilience engineering initiative⁴¹. It was in 2004 when Hollnagel, Woods, and Leveson introduced the concept, in terms of technological safety, by stating that resilience engineering is a paradigm to safety and can be used to avoid human and organizational failure. The definition by⁷⁴ is closely related to process system resilience.

They define resilience, as “the intrinsic ability of a system to adjust its functioning prior to, during or following changes and the disturbances, so that it can sustain required operations under both expected and unexpected conditions”. This definition obviously comprises the definition of safety, as ‘ability to sustain required operations’ and is equivalent to freedom from unacceptable risks. However, resilience emphasizes the ability to function in both expected and unexpected conditions rather than just to avoid failures. Also, an anticipation element is included with the use of words ‘prior to’ in the definition. Resilience analysis is distinguished from risk assessment in several ways. Principally, conventional risk assessment methods are used to determine the negative consequences of potentially undesired events and to mitigate them. Based on work by Dekker et al.⁷⁵ and Jain et al.⁷⁶ in contrast, the resilience approach emphasizes an assessment of the system's ability to anticipate, survive and recover.

2.2.1. Process Risk: Analysis and Reduction

Reliable risk estimation and assessment is a condition for awareness of the state of affairs and improvement if necessary. As mentioned before, it involves two components; establishing both the probability of the event occurring, and the consequences if the event does occur. The four important components of risk analysis are hazard identification (and if possible reduction or elimination), and then risk assessment, risk management, and risk communication⁷⁷. Historically, primary causes of process incidents are categorized as – process failures, human errors, mechanical failures, instrumentation failures, and external events such as natural calamities. Attention is seldom paid to a) failures related to organizational or management system breakdowns, cognitive failures associated with human fatigue, and lack of training; and b) proactive approaches similar to Inherent Safety

(IS). Some efforts have been made in the direction of integration of such failures into the analysis, however it is still fragmented in nature and not implemented in the industry. The focus needs to be on the seamless integration of both technical and organizational resilience to ensure business continuity and sustainability⁵³. Some work on business continuity management and resilience have been done in recent years^{78, 60}. Also, ideas about Inherent Safety (IS) have been around for millennia and it is widely accepted that the IS concepts were first formalized in a process engineering context by Trevor Kletz in the late 1970s⁷⁹. Examples of some indices developed include Qualitative Assessment for Inherently Safer Designs (QAISD)⁸⁰, a fuzzy logic-based inherent safety index⁸¹, one of the first safety indices for inherent safety called the Heikkila index⁸², and inherent safety assessment based on indicators⁸³. IS concepts can have significant impact in avoiding the hazards. Few efforts have involved in the incorporation of these concepts into design features⁸⁴. Methods, tools and knowledge related to process safety have notably increased over the years⁸⁵. Some of the major contributions in the area are summarized in Table II.3. Today, process safety management is well-implemented in some companies and this has reduced the severity of incidents compared to prior performance⁸⁶. In the aftermath of the Bhopal disaster in 1984, research efforts and regulations for process safety gained new momentum⁸⁷. In the last 30 years, regulatory requirements for process safety management systems have been established and implemented in countries such as the United States, in Europe through the Seveso II and III Directives, Australia, *etc.* However, current risk evaluation still lacks the proactive and the social aspects involved within the process systems and thus often still results in a non-comprehensive risk analysis that can overlook, and therefore cause, some catastrophic incidents.

Table II.3: Selected works on process risk analysis

Authors	Major contributions
88	Bayesian analysis method for treatment of epistemic uncertainties.
89	New technique called Optimal Risk Analysis (ORA).
90	A seven-stage systematic framework for the analysis and improvement of near-miss programs.
91	Comparison of application areas, methodology and relationships for 3 approaches - accident investigations (AI), risk analysis (RA), and safety management systems (SMS).
92	Review of risk analysis tools used by 24 chemical plants in Belgium. Requirement of external domino accident prevention framework.
93	Two different approaches to handle uncertainties in FTA and ETA.
94, 95, 96	Dynamic risk analysis methodology that uses alarm databases to improve process safety and product quality.
20	Blended hazard identification (BLHAZID) methodology blends and automates two different types of HAZID methods: the function-driven and component-driven approaches.
97	Demonstration of discrete-time Bayesian network (DTBN).
98	Comprehensive maturity model for QRA covering potential flaws of risk assessment.
99	Human reliability analysis for the pre-maintenance and post-maintenance activities of a pump (HEART methodology).
100	Two advanced dynamic techniques, DyPASI (hazard identification) and DRA (risk assessment) were coupled.
101	Areas of improvement in risk assessment - dynamic updating of risk to support real-time decision-making. Risk Barometer: a novel method based on indicators.
102	Review of recent contributions on what is currently wrong with QRA and future steps in QRA directions.

2.2.2. Systems thinking

In the process industries, there are numerous factors that can influence the process safety environment, and each factor can affect others, maybe in an immediate and direct manner, or in systems engineering terminology, a tightly coupled manner. Multilevel factors can trigger each other, and thus cannot be described in a simple, isolated, linear fashion. Safety is a non-linear problem, and researchers have proved this in the system safety context^{18, 103, 104}. In the life cycle cost analysis (LCCA) perspective, many routine decisions consider performance-related factors alone, and do not focus on downstream costs such as operation and maintenance support. Therefore, designing a system on the short-term basis alone can lead to much higher costs than a more enlightened long term

approach. At this point, counter-intuitiveness plays a key role in explaining the difference and relationship between long-term and short-term behavior. For example, in the short-term, implementing inherent safety principles in the early stages of design may seem to have an associated cost. On the other hand, in the long-term, it may reduce the total cost by diminishing one or more of maintenance, operation, and training costs, *etc.* Moreover, it can lead to increased worker motivation and process productivity. This is shown in the causal loop model in Figure II.1. System thinking is characterized by its holistic approach to problem solving while analytical methods used in traditional risk assessment can be viewed mainly as linearly reductionist^{2, 105}. With a systems approach focused on resilience, common characteristics of failure that must be addressed in addition to pure technical factors include: organizational deficiencies; ineffective control and communication; poor reliability; disregard of human factors, *etc.*

System characteristics

The following four have been identified as key system characteristics by various researchers:

- Emergence: this implies that the tasks or actions and their results at the system or collective level arise or develop from the individual actions and interactions between the individual components^{106, 107}.
- Hierarchy: this characteristic represents the differences between the various levels of a system across its vertical structure. It relates to the different levels of authority and roles within a system.
- Communication: a reference to the mechanisms for the system to exchange relevant information within itself system (reporting up, instructing down)

and its environment. It provides for the flow of information among the subsystems.

- Control: this characteristic is related to communication and also deals with the level of control to changes in systems behavior, technology, *etc.*

Key concepts of systems thinking

The major concept of systems thinking is the system life cycle presented as a V-model that is an integrated top-down and bottom-up approach¹⁰⁸. This refers to the application of systems engineering to integrate both evaluation of technical and social aspects in risk assessment for the whole life cycle. For a process system, this would include stages such as feasibility study, technology development, detailed design, construction, commissioning, start-up, inspection, operations, and decommissioning. With the V-model application, evaluation would be done at both the individual system level as well as at the level of the whole system with the goal of ensuring perfect integration. This is represented through a simple schematic for a process system life cycle in Figure II.2.

Another important systems concept from the resilience perspective is the understanding and capability of a system to perform and function during abnormal conditions or states^{7, 109}. These abnormal conditions may arise due to known or as yet unknown, expected or unexpected and internal or external events. The third concept is about the dichotomy and trade-off analysis. System characteristics are often treated separately although they not only coexist and interact but also form a complementary relation.

116, 117, 118, and the banking sector^{119, 120}. Some other industrial sectors as well as natural disaster management units like the construction industry, the medical sector, hurricane response teams, and others have research studies where near-miss or similar information has been identified as an early warning signal to forecast major mishaps^{121, 122, 123}. In the process industries, with the introduction of advanced automation and safety management systems, a wealth of possible signals are available and captured. As noted by¹²⁴, this would enable monitoring of the instantaneous risk levels. Near-miss information is considered as a significant precursor data that can be utilized for facilitation of prediction of major process upsets^{90, 125}. Table II.4 presents the notable contributions in early fault detection and warning signals application in the process industries.

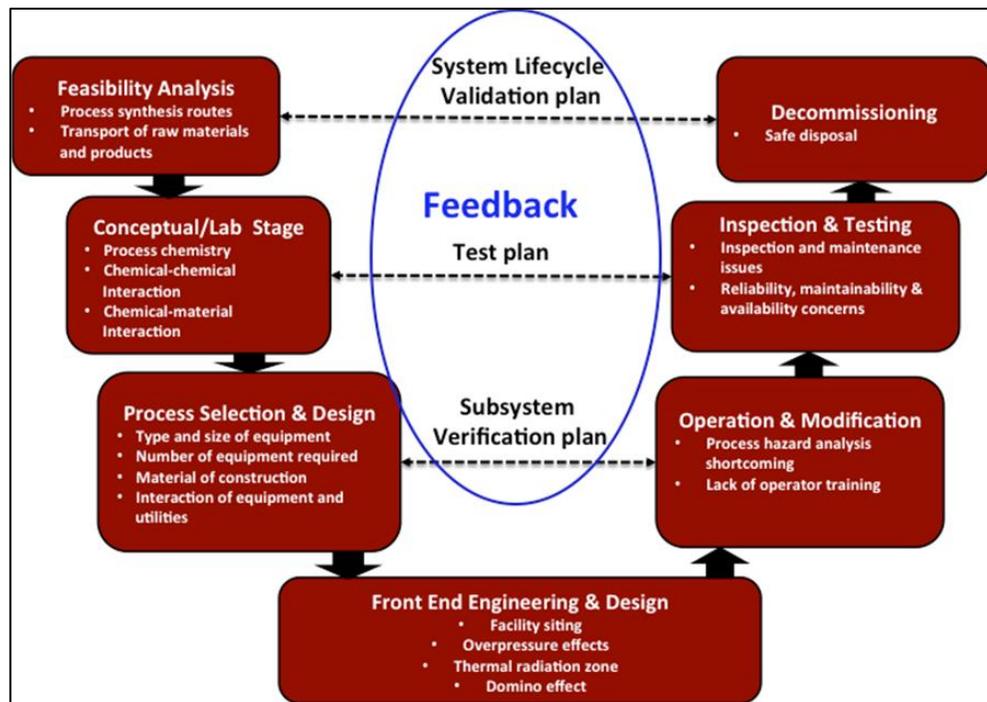


Figure II.2: System life cycle V-model

Table II.4: Selected works on early fault detection

Authors	Major contributions
126	Use of cumulative summation (CUSUM) control charts and artificial neural networks together for fault detection and diagnosis (FDD).
127	An Early Warning Detection System (EWDS) and neural network learning system for early prediction of runaway reaction events.
128	Use of multi-scale principal component analysis (MSPCA) for fault detection and diagnosis.
129	Review of quantitative model based approaches to fault diagnosis and a general framework for analyzing and understanding various diagnostic systems.
130	Review of fault diagnosis methods that are based on historic process knowledge.
131	A real-time expert system for fault diagnosis of chemical processes.
132	System Hazard Identification, Prediction and Prevention (SHIPP) methodology: a process accident model with predictive capabilities, which uses a combination of event and fault tree concepts to model the cause-consequence relationship.
133	Original approach in the comparison between different criteria on the study of the onset of runaway reactions. Results fundamental for the development of an Early Warning Detection System.
134	Non-linear Kernel Gaussian mixture model based inferential monitoring approach for fault detection and diagnosis.
135	Review of current trends of future-oriented prevention management in the chemical-using industry. Two concepts for the next generation of managing prevention within chemical industrial areas are - integrated design-based safety and security; collaboration of several chemical plants to increase sustainable development of their activities and their environment.
136	Comparison of two different methods of development of early warning indicators - The Resilience Based Early Warning Indicator (REWI) method and The Dual Assurance method.
137	New tool - DyPASI for the continuous systematization of information from early signals of risk related to past events and mitigation of deficiencies of the current HAZID techniques in the identification of unexpected potential hazards related to atypical scenarios.

2.2.4. Dynamic simulation, optimization and major events modeling

Dynamic modeling of process systems has been used for many decades. This technology has greatly influenced process industry business and is critical throughout the lifecycle of a plant. It is a systematic method to express all operations of a chemical plant (pumping, flow, mixing, chemical reactions, separation processes and purification, *etc.*) using a unique set of algebraic and differential equations based on fundamental

engineering principles. Such simulation studies result in mathematical models that can be very useful in real-time monitoring and predictions, operator training, verification of operating and safety procedures, decision-making, control of plant during transient operations, investigation of any operational issues, safety and environmental issues *etc.*¹³⁸. These studies have played a crucial role in design of operability and economically profitable and efficient plants. It is an area where numerous methods and tools have been developed for advanced decision-making in the process industry. Various models have been developed in process optimization with respect to design, control, scheduling, maintenance and safety problems^{139, 140, 141}. For example, Thomaidis and Pistikopoulos developed a model for evaluation of undesirable and hazardous conditions via a combined flexibility-reliability-safety analysis¹⁴². Also, several remarkable works have been conducted in the area of process simulation and major events modeling with respect to safety as summarized in Table II.5. The current process resilience analysis framework research utilizes these dynamic simulation and optimization techniques to develop process, safety and cost models. The objective is a design optimization approach to identify and obtain safer operational regions at maximum average profit.

Table II.5: Selected works on resilience and major events modeling

Authors	Major contributions
143	Review of available techniques and future research needs for flexibility, operability and control aspects into the design procedures of process systems.
43	Presents a rigorous framework for handling systematically the objectives of flexibility and dynamic resilience which are major components in plant operability.
144	Analysis method to obtain risk profiles for major adverse events.
145	Significance and challenges of modeling and simulating critical infrastructures and their interdependencies.
146	Discussion on traditional safety models and their limitations, and description of new system-theoretic approaches to the modeling and analysis of accidents in complex systems.

Table II.5 Continued

Authors	Major contributions
45	Presents a graphical approach called The Resilience Analysis Grid (RAG) to measure the resilience of a system.
47	Presents nine categories of challenges in the procedure of building RE and its adaptive capacity in a chemical plant.
147	New method QRAPII (Quantitative Risk Analysis Precursor Incident Investigation) that combines accident investigation and QRA using information from a precursor incident as input to QRA.
148	Systemic Risk Index for the industrial area is determined considering both a safety and security network risk index and a supply chain network risk index.
149	Improved bow-tie analysis to overcome missing data and model uncertainty.
150	A systems view of process safety is quantified via a safeness-index concept.

2.3. Summary

Process safety and risk management, in process industry is unequivocally critical due to potential on-site as well as off-site impacts. As noted in previous sections, there is an abundance of work in areas of risk analysis, early fault detection, major events modeling, *etc.* It is also important to note that process systems are complex socio-technical systems that comprise of various sub-systems and components¹⁵¹. These interconnected components interact in a non-linear pattern and often present trade-off challenges between productivity and safety, risk mitigation measures and costs involved and more. Therefore, it is critical to study process disasters from systems engineering perspective, and conduct a detailed analysis on the interfaces, which involves studying scenarios close to reality for effective risk management. From, systems perspective, the concept of resilience engineering has various features, and the one that makes it distinct from traditional process safety practice is the importance of coping with complexities by learning and adapting to ensure safety as a system undergoes changes, deterioration, hazardous situations and

more⁷⁵. Over the last few years there has been a considerable interest and work carried out in the idea of application of resilience engineering for risk management.

CHAPTER III

PROCESS RESILIENCE ANALYSIS FRAMEWORK*

Hazard identification methods suffer from limitations and are not comprehensive. There is lately much written about it¹⁵². In addition, assessment of risk apart from scenario definition contains other uncertainties adhering to event probability determination as well as that of the severity of consequences. And even, if a particular scenario is foreseen and assessed, there is no guarantee whatsoever that the recommended safeguards have been realized. Suppose the process hazard analysis has been very effective, still an unknown threat may show up.

From the second half of the 1980s, the High Reliability Organization concept developed, *e.g.*, later described in the known work of³³. These authors promoted the basic message of mindfulness to business in general on the principles:

- Preoccupation with failures
- Reluctance to simplify
- Sensitivity to operations
- Commitment to resilience
- Deference to expertise

*Reproduced in part with permission from Jain, P., Pasman, H. J., Waldram, S., Pistikopoulos, E. N., & Mannan, M. S., "Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management," JLPPI, Vol 53, Pages 61-73. Copyright 2018 Elsevier Ltd.
Reproduced in part with permission from Jain, P., Mentzer, R., & Mannan, M. S., "Resilience metrics for improved process-risk decision making: survey, analysis and application," Safety Science, Vol 108, Pages 13-28. Copyright 2018 Elsevier Ltd.

Resilience as a property of an organization became a leading thought making to launch their system oriented resilience engineering initiative, which is specifically focused on the psychological and cultural aspects of humans and organizations with the objective of preventing accident and promotion of safe work⁴¹.¹⁵³ thinks in terms of performance fluctuations with sometimes a high positive or a deep negative “resonance” peak. The unexpected drawback of the latter shall be mitigated by built-in resilience.

Resilience engineering in this social sense makes people continuously anticipate and adapt in a resourceful and resilient way to varying conditions⁴¹. It led to the approach that promoted as Safety-II, in which unlike in traditional Safety-I not is looked and prevented how things go wrong, but in a positive way learning and doing as much as possible to have it go right¹⁵⁴. Safety-I led to do’s and don’ts and even what is called safety bureaucracy, while Safety-II is in the same way as a Quality Management System: doing things with an attitude of trying to improve. Safety-II can be implemented and works out in practice, it is useful to read the White Paper of¹⁵⁵. The two approaches do not clash, but Safety-II enhances safety and productivity. Also, in view of the increase in complexity of socio-technical systems risk assessment through the eyes of Safety-II is seen as trying: “to understand the conditions where performance variability can become difficult or impossible to monitor and control”. Due to complexity and transients, the causality is often not immediately clear and an undesirable event just emerges.

In this chapter, a framework of process system resilience analysis is established and the chapter is organized as follows. Sections 3.1 presents the Process Resilience Analysis Framework (PRAF) along with details of phases, aspects and metrics. Section 3.2 describes the PRAF survey, methodology and analysis results. Section 3.3 provides the

concepts of matrix-based tools for quantification of social aspects with a motivating example. The chapter concludes in Section 3.4 with a summary.

3.1. Process Resilience Analysis Framework (PRAF): basic concepts and structure

Following the concept of resilience, of course, process resilience is related to avoiding, surviving and recovering from disruptions due to both the technical and social factors. The technical and social factors are well aligned with the four dimensions of community resilience—technical, organizational, social, and economic (TOSE)¹⁵⁶. Figure III.1 illustrates the PRAF overview applied to the process systems for effective risk assessment and management.

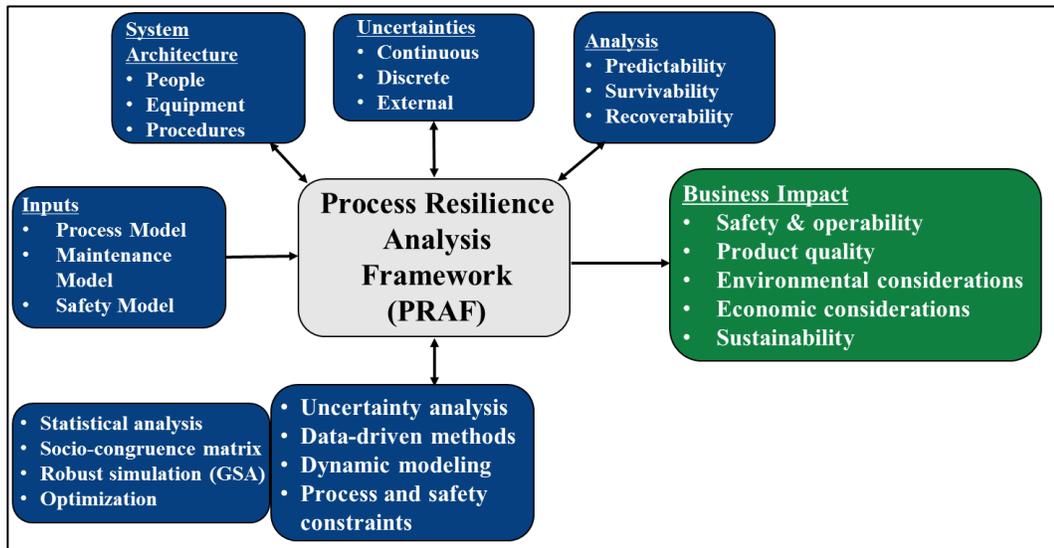


Figure III.1: Process resilience analysis framework overview

With the purpose of establishing an effective methodology, PRAF presents an integrated approach that relies on data-driven, quantitative, and dynamic analysis. The seven characteristics for an effective and comprehensive methodology are:

- Integrated: single approach incorporating both technical and social factors analysis.
- System-based: analysis based on interactions of various system components, sub-components and system characteristics of emergence and hierarchy.
- Quantitative: use of mathematical, statistical and matrix-based models to provide measures of risk and resilience.
- Data-driven: utilization of measured process variables and resilience metrics of the system.
- Dynamic: evaluation in real-time by use of simulation.
- Uncertainty management: use of Bayesian analysis to manage uncertainties in limited historical data.
- Cost-effective: incorporates profitability as one of the objective functions.

A comparative analysis of existing studies vs PRAF is summarized in Table III.1.

It is critical to understand the functioning of such a complex socio-technical system and also the understanding of how it fails. In this context a process system schematic as shown in Figure III.2 depicts the various levels and interactions between sub-systems, components and sub-components. As evident, within these various levels, the process system exhibits the system characteristics of emergence, hierarchy, communication and control.

Table III.1: Comparative analysis of resilience models or studies

Models/studies	Characteristics						
	Integrated	System-based	Quantitative	Data driven	Dynamic	Uncertainty management	Cost-effective
PRAF	✓	✓	✓	✓	✓	✓	✓
42	✗	*	✓	✓	✓	✓	✓
157	✓	✓	✗	✗	*	✗	*
44	*	✓	✗	✗	✗	*	✗
158	*	*	✗	✗	✗	✗	✗
45	*	✓	*	*	*	*	✗
159	✗	✓	*	*	*	✗	✗
46	*	✗	*	*	*	✗	✗
160, 161	✓	✓	*	*	✗	✗	✗
40	✗	*	✓	✗	✓	✓	*
48	✓	✓	✓	*	*	*	*

✗: Low consideration

*: Partial consideration

✓: Complete consideration

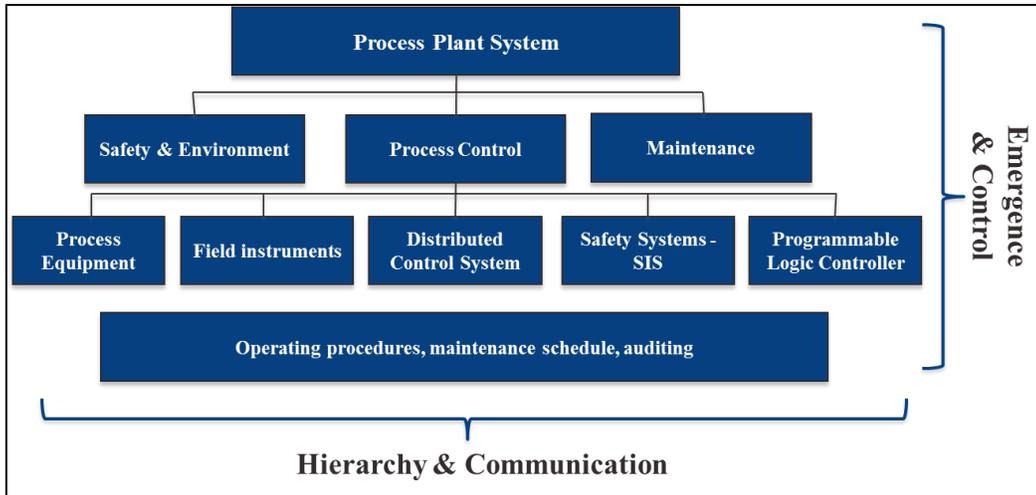


Figure III.2: Process plant system

Primarily, the resilience concept is associated with the post disturbance ability of the system to bounce back, or return, in a low risk manner to a pre-disturbance or normal state. When the notion of resilience is applied to process systems, this definition broadens to include the pre-disturbance state, as well as, change of state from normal to a process upset state as shown in Figure III.3. There are three main system states: normal state, process-upset event state and catastrophic event state. There can be various technical and social failures (regulatory, human, and organizational factors), which may lead to a process upset event and the catastrophic top event incident. In the avoidance phase of PRAF, process upset event is predicted in advance (represented by activity A), and hence, the system remains in the normal operation state. For the survival phase of PRAF, the system state is assumed to be process upset event and PRAF helps the system to survive through the process upset condition (represented by activity B), and hence the system remains in the same state, possibly with a degraded performance. Finally, in the recovery phase, the system is assumed to be in the catastrophic event state and PRAF helps to prioritize

emergency barriers to enable reduction in severity of consequences and response time (represented by activity C), and leading to eventual resumption of the normal operation state.

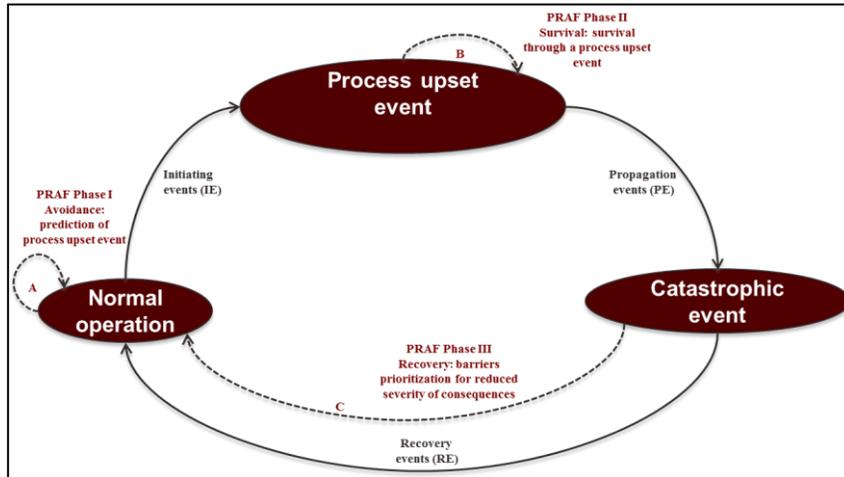


Figure III.3: System transition diagram

3.1.1. Four aspects of process resilience

The four cornerstones of resilience engineering as identified and developed by ¹⁰³ are anticipation, monitoring, response and learning. The four aspects to be considered in the process resilience analysis framework (PRAF) have been identified based on these four cornerstones of a resilient system. These four aspects are early detection; error tolerant design including inherently safer design; plasticity also characterized as resistive flexibility, and recoverability¹⁶² and are illustrated in Figure III.4.

Early detection (ED) refers to the recognition of a system’s ‘weak’ signals that could be precursors of an undesired abnormal event. Weak signals will be from a variety of sources. There will be the usual enterprise resource planning¹⁶³ information, *e.g.*, System analysis And Program development (SAP) data, which will be comprehensive on the company business processes (accountancy, client orders, suppliers, maintenance schedules,

logistics). Further, there will be the process control data, and additional data on plant performance, such as equipment energy consumption, pump vibration, the state of corrosion, maintenance activities, unusual internal traffic, and temporary personnel concentrations. Also, an important source of signals will be lagging and leading indicator information. Additionally, there will be external signals on weather, environmental conditions such as an earthquake, flooding, utility disturbances, possible strikes, cyber and terrorist threat. The processing of all these data, followed by data mining and analytics to extract trends or to obtain coming event warnings, can provide valuable insights however, shall be a major effort¹⁶⁴. Due to randomness and interdependencies, this will require artificial intelligence developed methods within the Big Data and Analytics application trend. Process safety and resiliency can ‘piggy-back’ on this contemporary development as important side-benefits. In case alarming information is discovered another aspect is to present it in a convincing way to management for a decision on the action¹⁶⁵.

Error tolerant design (ETD) presents the inherently safer features of a system and process such that undesired, and perhaps even unknown, external influences will not cause the system to fail in any significant way. Processes should still function well (but maybe at reduced efficiency and marginally increased risk). *Error tolerant design* encompasses quite a few aspects as well. It starts with the design process itself. Not without reason, ¹⁸ added a design pillar in parallel to the original process industry socio-technical system representation pillar of ²⁵. A large fraction of major accidents is due to or co-caused by design errors. Also, the design organization is for its product quality dependent on its management virtues with all the derived characteristics as competence level, cultural behavior, and error-avoiding performance. But actually, error tolerant design means that

designs are such that an operator in its interaction with procedure and equipment cannot easily make an error, or if the operator makes an error, it will not immediately lead to complete failure, or if the machine is faulty, it will not lead to an immediate process upset. The latter is a feature that reminds of the inherent safer plant but also of good system ergonomics. Error tolerance shall hold too for the organizational structure and procedures. It should be such that it will not bring staff in a situation of making an error easily, and it should motivate staff positively. The latter will be in line with the Safety-II idea to approach things from the positive side and to seek conditions to produce sound work and wherever possible improvement.

Recoverability (R) indicates how quickly the system can recover back to a normal state of operations in the case of an abnormal event. Recovery starts with an emergency response operation. For an effective functioning of this response, preparation and capabilities are required. An Emergency Command Center is a basic requirement. Also, this pillar has to rely on risk assessments. For preparation, representative scenarios are selected and with this scenario-analysis is performed. This consists of determining which of the functions of firefighting, medical support or keeping order, is at what location needed most, and what should be their capabilities. Scenario-analysis will also serve to find out at what stage assistance and extra capabilities must be demanded. Resiliency, however, requires too a whole series of other provisions and contingencies, so that the company activity is disturbed only minimally. Because all investment is limited, the risk assessment results will provide a basis of how to distribute resources for the best final result and the best chance of business continuity. Where emergency response may take days or weeks, recovery as a whole may take a much longer time.

Finally, Plasticity (P) refers to how well an organization and people would behave, how small the effects are and how well it will resist the undesired disturbances by implementing planned measures and improvising others, when a seamless transition from a normal state to an upset state occurs and shall be reversed. *Plasticity* is the openness of mind to recognize possible threats and changes, devise ways to cope with it without generating risk elsewhere. Again, it is a way of behavior that has to come from the top and be anchored in the culture. It also requires competence comprising knowledge, and insight and experience. Like in designing, plasticity will need the support of process simulation techniques, and risk assessment methods. As in case of an aircraft pilot or a command cell, it is very useful to have simulator training for crisis situations and to have been exposed to scenarios. Although the presence of mind and staying cool in a pressure situation is a general requirement, to have experienced a scenario and recognizing its features is of a great help.

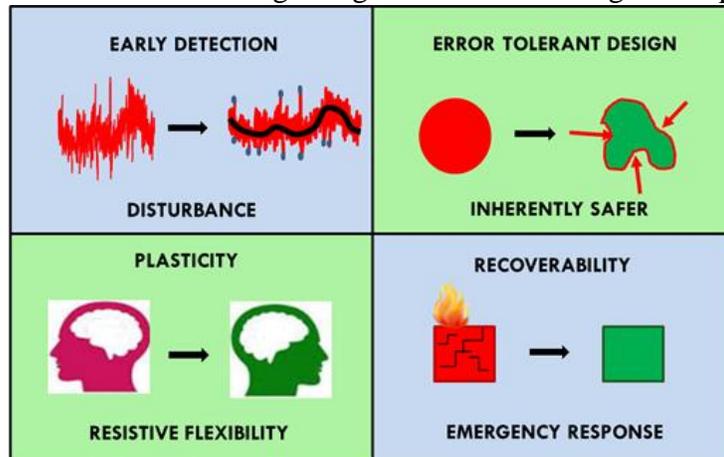


Figure III.4: Resilience aspects under PRAF

3.1.2. Three-phase analysis

With an objective to study the complete failure process of any complex system such as critical civil infrastructure systems, spaceflight, financial services organizations, and energy, the resilience approach has been segregated into actions or impacts prior to,

during or after disturbance^{36, 74, 109-110, 166}. These actions and impacts for a system are covered in the ‘avoidance’; ‘survival’ or ‘recovery’ phases based on the disturbance time. The National Response Plan implemented by the Department of Homeland Security in the United States, and related plans in other countries, comprising of Prevention and Preparedness and Response and Recovery steps contain similar phases for an intentionally caused incident. In order to cover the whole anatomy of a process safety incident, the three phases are distinguished as presented in Table III.2.

Table III.2: Different phases of process resilience

Phase	Description	Available data (from indicators)	Available time to respond	Financial impact
Avoidance	Includes actions or efforts targeted to identify threats or vulnerabilities based on weak signals or inference by analysis of system observations to prevent an upset condition or predict a LoC scenario ³⁷ .	more	more	less
Survival	Includes actions or efforts to understand the upset condition and identify resources and prioritize them to reduce likelihood of further impact.	medium	medium	medium
Recovery	Includes actions or efforts required to return to a normal state by reducing response time and hence strongly reducing likelihood of severe consequences.	less	less	more
*Loss of containment: An unplanned or uncontrolled release of material from containment, including non-toxic and non-flammable materials (<i>e.g.</i> , steam, hot condensate, nitrogen, compressed CO ₂ or compressed air) ¹⁶⁷ .				

In the case of a looming threat, three phases are distinguished:

Avoidance phase – includes actions or efforts targeted to identify threats or vulnerabilities based on weak signals or inference by analysis of system observations to prevent an upset condition.

Survival phase – includes actions or efforts to understand the upset condition and identify resources and prioritize them to reduce likelihood of further impact.

Recovery phase – includes actions or efforts required to return to a normal state by reducing response time and hence strongly reducing likelihood of severe consequences.

It is explicit from Figure III.5 that there is - more information available from metrics, more time to react to a disruption or threat, fewer resources or lower cost involved in the avoidance phase as compared to the survival and recovery phases.

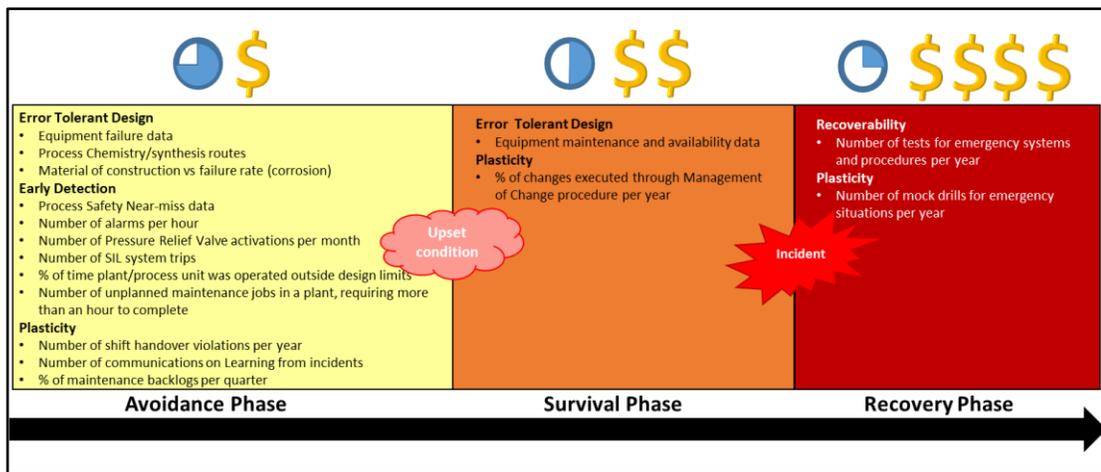


Figure III.5: Resilience analysis diagram in three stages with aspects and metrics

3.2. Resilience metrics

With respect to resilience engineering, risk and safety management of a process facility is a top-level system requirement and cannot be considered in isolation. In order to analyze the impact of different sub-systems, components, sub-components and their interaction as a whole it is critical to monitor and measure. This has been already explained and practiced by monitoring the effectiveness of the safety management system by means of indicators¹⁶⁸. Hence, one of the other key tasks is to develop metrics specifically for

process resilience. These metrics, or indicators, will be critical in the quantification of overall process resilience and will also provide the essential information for senior management to make informed risk related decisions. These decisions will be guided by the top-level requirements of the process system, and their purposes could be wide-ranging, multi-dimensional and sometimes have conflicting immediate objectives similar to the trade-off analysis concept. In such situations, performance monitoring indicators or metrics will give insights into the time dependent prediction, survival and recovery analysis and can help track the overall resiliency of the system. For Process Resilience Analysis Framework (PRAF), metrics have been developed considering the performance indicators established by API RP 754¹⁶⁹ and also based on the process resilience aspects of early detection (ED), error tolerant design (ETD), recoverability (R) and plasticity (P). These have been categorized into technical (ED, ETD, R) and social resilience (P). At present there are a total of 24 resilience metrics identified under the three phases of process resilience. The avoidance phase for predicting a process upset event included metrics such as alarm rate (ED), unplanned maintenance jobs (ED), process safety near miss data (ED), and learning from incidents (LFI) communication (P). The survival phase for surviving a process safety or LoC event comprises of metrics such as changes executed through Management of Change procedure (ETD), safety critical equipment inspection (ETD), maintenance backlogs (P), and shift handover communication (P). The recovery phase for recovering from a process upset or catastrophic condition comprised of metrics such as tests of emergency systems and procedures (R), mock drills for emergency situations (R), and review/revision of required procedures. (P). Metrics are significantly needed to make predictions about disruptions, assist in decision-making, and take corrective actions.

Additionally, it is important to assign weights to these metrics in order to obtain the contribution of each of the three phases to overall resilience. For this purpose, a survey questionnaire called ‘Process Resilience Analysis Framework’ has been circulated to a wide variety of practitioners and response was analyzed.

The use of metrics in risk assessment and management of chemical process systems is a well-known area of research. There are numerous sources, which provide a comprehensive list of such metrics categorized into leading or lagging and technical or social. It is only since the BP Texas City Refinery incident in 2005, that the need for process safety indicators has gained momentum. Primarily two types of process safety metrics have been defined in literature – leading and lagging. Recent investigations discovered that consideration of only lagging indicators over leading indicators is not a good practice. Lagging indicator data might be useful for organizational benchmarking purposes, however, it lacks the potential of enlightening the management on the true process safety statistics and safety culture. Several works have been undertaken to develop approaches using metrics. ¹⁷⁰discussed an approach for the inherent safety metric and demonstrated its application through comparison of LNG regasification technologies. ¹⁷¹established the risk-based process performance indicators for improving the existing safety performance indicators. There are numerous sources, which provide a comprehensive list of such metrics categorized into leading or lagging and technical or social. Table III.3 summarizes some of the selected works on process safety or risk management metrics existing in the literature. It is important to note that resilience emphasizes human and organization aspects, as well as technical aspects. Table III.4 lists

some of the models or studies, which have developed resilience metrics, principles, and elements.

Table III.3: Selected list of works on process safety or risk management metrics

Sources	Process safety or risk management metrics
172	Guidelines to develop process safety indicators
173	Description and use of Process Safety Leading and Lagging Metrics
174	Comprehensive document providing guidance to assist industry, public authorities, and communities to prevent and prepare for chemical accidents
169	Standard API RP 754: Process Safety Performance Indicators for the Refining and Petrochemical Industries
175	Report on Process Safety: Recommended Practice on Key Performance Indicators
176	New normalization factors for process safety lagging metrics
177	Two categories for major hazard risk indicators within the oil and gas industry: precursor events and barrier elements
178	Various indicators are reviewed to answer which indicators qualify to provide insight and knowledge in levels of safety of processes or business

These metrics are critical in the quantification of overall process resilience and also provide the essential information for senior management to make informed risk decisions. However, not many researchers have attempted to cover all aspects of resilience for augmented risk management or assigned weights to the resilience metrics. In the current study, the motivation is to obtain the relative significance of metrics and the contribution of each of the three phases to overall resilience based on the Process Resilience Analysis Framework (PRAF)^{162, 182}. Therefore, a survey called ‘Process Resilience Analysis Framework’ survey was conducted. The research questions,¹¹⁰ addressed in this study are:

- RQ1: What are the most important metrics for each of the three phases of PRAF – avoidance, survival, and recovery?
- RQ2: Are there any differences in viewpoints of various groups of survey respondents?
- RQ3: What are the weights for each of the metrics?

Table III.4: List of works on resilience metrics

Authors	Metrics or principles or elements of resilience
158	Seven themes of Highly Resilient Organizations (HROs): Top-level commitment, just culture, learning culture, awareness, preparedness, flexibility, and opacity
179	Four cornerstones of Resilience Engineering (RE): Anticipate, monitor, respond, and learn
110	Four principles: Top management commitment, flexibility, learning, and awareness
180	Eight Contributing Success Factors (CSFs): Risk understanding, anticipation, attention, response, robustness, resourcefulness/rapidity, decision support, and redundancy
181	Three elements for emergency management: Proactive emergency management through early risk anticipation, emergency management’s adaptation to new and future work practices such as distributed actors, and emergency management’s adaptation to new and future work practices such as new technology
46	Six principles: Flexibility, controllability, early detection, minimization of failure, limitation of effects, and administrative controls/procedures
65	Integrated Resilience Engineering Factors: Self-organization, teamwork, redundancy, and fault-tolerant
162, 182	Process Resilience Analysis Framework Four resilience aspects: Early detection, error tolerant design, recoverability, and plasticity Twenty four process system resilience metrics

In order to answer these questions, a Process Resilience Analysis Framework (PRAF) survey questionnaire was prepared based on the resilience metrics.

The metrics include both technical and social factors. For example, the technical factors include process or equipment related parameters such as alarm rate, vibration analysis of mechanical equipment, and demands on safety system. Social factors include human and organization related aspects such as current and accurate procedures, training completed on schedule, shift-handover communication, and completion of process safety corrective actions.

This section presents the resilience metrics developed for PRAF with description and significance to make process systems resilient and safer to operate^{162, 168-169, 182}. These are categorized in three phases of PRAF:

3.2.1. Phase I – Avoidance

Alarm rate

It is defined as the number of alarms per hour. In a process unit, the alarm is annunciated if the value of one of the measured process parameters such as pressure, temperature, or level is outside the set point limits. A higher number of alarms in a particular process unit indicates a problem with the normal operation of the process operation and can escalate to an abnormal condition in case the operator does not take appropriate action¹⁶⁵.

Equipment pieces operated outside fitness-for-service rating

It is defined as the “number of equipment pieces found to have operated outside fitness-for-service rating per 100 or 1000 inspections or tests”¹⁶⁹. Such inspection results will indicate potential failure of primary containment.

Unplanned maintenance jobs

It is defined as the number of unplanned maintenance jobs in a plant, requiring more than an hour to complete. If some process equipment in a plant is faced with a higher number of major unplanned maintenance, it is a clear indication of a mechanical integrity problem.

Mechanical database

It is defined as the data gathered from mechanical equipment, and it is categorized primarily as the number of rotatory equipment pieces (*e.g.*, compressor, and agitator) found

to have operated outside vibration rating limits and number of pump or seal leaks observed from mechanical equipment.

Process safety near miss data

It has been considered as one of the most important leading metrics in literature¹⁷³. This metric is defined as the number of process safety near misses reported in the plant. Near miss has been defined as “any significant release of a hazardous substance that does not meet the threshold for a process safety incident lagging metric, or a challenge to a safety system”¹⁷³. An increased number of near miss events can be an indicator of a higher potential for a significant LoC event.

Unplanned shutdowns per year

It is defined as the number of unplanned shutdowns per year in a process unit/plant. If there are frequent events of emergency and/or unplanned shutdowns in a process unit, this is an indicator of a potential problem in the plant. This metric contributes to the avoidance phase by providing an important history of various setbacks in the plant history.

Learning from incidents (LFI) communication

It is defined as the number of communications on learning from company and industry incidents. It is evident from literature that this is an important indicator for improved process safety and risk management. The literature on failure to learn from process safety incidents has highlighted how some of the disastrous events could have been avoided¹⁸³. It is one of the vital metrics in avoidance phase as communications on learning from incidents could help the process operations team identify additional challenges or hazards thus supporting prediction of events.

Process hazard evaluations completion

It refers to the various hazard identification and evaluation studies for a process plant. It is calculated as the percentage of studies completed on time vs scheduled.

Process safety action item closure

It refers to the different kinds of recommendations and action items generated from process safety studies such as incident investigations, hazard identification and evaluations or compliance audits. It is calculated as the percentage or number of past-due action items.

3.2.2. Phase II– Survival

Demands on Safety system

This is categorized into the following three metrics, which form important metrics for the survival phase.

Trips (SIF/ESD system activation): “A safety instrumented system is considered to have been activated when called upon to function by a valid signal regardless of whether or not the SIS responds”¹⁶⁹. It is measured as the number of trips (ESD/SIF system activations) per month.

Pressure relief: “A pressure relief valve is considered to have been activated when the system pressure reaches the device set point whether or not the pressure relief device performs as designed”¹⁶⁹. It is measured as the number of activations of pressure relief valve/bursting disk per month.

Mechanical device shutdown: “A mechanical shutdown system is considered to have been activated when called upon to function by a valid signal, regardless of whether or not the mechanical shutdown system responds”¹⁶⁹. It is measured as the number of mechanical trip activations per month.

Plant/process unit was operated outside design limits

It is defined as percentage of times process unit was operated outside the safe operating limit (SOL) applicable to the phase of operation.

Changes executed through Management of Change MoC procedure

It is defined as the percentage of changes executed through Management of Change procedure per year. This metric measures how well a process plant/unit recognizes changes that require use of the MoC procedure of the company and actually makes use of the procedure prior to implementing changes.

Work permit compliance

It is defined as the “percentage of sampled work permits that meet all requirements”¹⁶⁹. The examples may be hot work, lockout/tagout, *etc.* It forms a critical metric for surviving through process-upset events.

Safety critical equipment (SCE) inspection

This metric is defined as the percentage of inspections of SCE completed on time. This may include pressure vessels, storage tanks, piping systems, pressure relief devices, pumps, instruments, control systems, interlocks and emergency shutdown systems, mitigation systems, and emergency response equipment.

Safety critical equipment (SCE) deficiency management

It is defined as the management response to the inspection findings of SCE deficiency (*e.g.*, non-functional pressure relief devices and safety instrumented systems - SIS's). “This may include proper approvals for continued safe operations, sufficient interim safeguards, and timeliness of repairs, or replacement, or rerate”¹⁶⁹.

MoC and Pre Start-up Safety Review (PSSR) Compliance

It is defined as the percentage of the sampled MoC s and PSSRs that meet all the requirements of the standards and procedures.

Fatigue risk management

It presents the human aspect of the process plant. It can be calculated based on various measures such as percentage of overtime, number of open shifts, number of extended shifts, number of consecutive shifts worked, *etc.*¹⁶⁹

Maintenance backlogs

It is defined as the percentage of maintenance backlogs per quarter in a process plant. This reflects the lack of effective implementation of the mechanical integrity program in the plant.

3.2.3. Phase III– Recovery

Tests for emergency systems and procedures

It is defined as the percentage of successful tests for emergency systems and procedures per year. It is an important metric for effective response and recovery from a catastrophic incident.

Mock drills for emergency situations

It is defined as the number of mock drills for emergency situations per year. It can be measured as the percentage of emergency response drills completed as scheduled. This is an important metric to assess the difficulties and time factor during actual response.

3.2.4. Common metrics

Shift handover communication

It is defined as the number of shift handover communication violations per year for the process unit. Human or plant operator is a critical and integral component of the process system in any operational activity. Therefore, this metric is common to all three phases of avoidance, survival and recovery.

Process safety required training sessions completed

It is defined as the “percentage of process safety required training sessions completed with skills verification”¹⁶⁹. This metric is conducive in robust and effective operators’ actions and response in the process plant. The operators in the plant are required to use various procedures such as operating, maintenance, and emergency and training for these is important. Hence, this is an important metric for both survival and recovery phases.

Required procedures reviewed/revised

It is defined as the percentage of required process safety related procedures reviewed or revised¹⁶⁹. This metric is conducive to robust and effective operators’ actions and response in the process plant. The operators in the plant are required to use various procedures such as operating, maintenance, and emergency and it is critical that these are revised and updated. Hence, this is an important metric for both survival and recovery phases.

3.3. PRAF survey

In this section, we are reporting on the statistical analysis of the resilience metrics survey conducted within the process industry. The survey respondents present a wide

variety of experience and employment sectors. This study aims to answer the following three research questions related to resilience metrics– what are the most important metrics for each of the three phases?; are there any differences in viewpoints of various groups of survey respondents?; and what is the relative level of importance for each of the metrics? Answers to these research questions are critical in the quantification of overall process resilience and also provide the essential information for senior management to make informed risk decisions. Therefore, a PRAF survey based on Likert type questionnaire was conducted, which produced categorical responses. Methods and techniques such as ordinal alpha, Kruskal-Wallis test, and polychoric correlations, relevant to analyze categorical responses have been used in the programming language R.

3.3.1. Survey content and methodology

The survey questionnaire comprises two parts, Part-I has 30 items with four possible responses graded from 4 to 1: 4 -essential; 3- important; 2- helpful; 1- unnecessary (Likert-type format). These 30 items were questions covering the 24 resilience metrics and three phases of process resilience in three sections. For avoidance phase, 11 items; survival phase 14 items; and recovery phase 5 items were asked respectively. The avoidance phase included items on metrics for predicting a process upset or LoC event. The survival phase comprised of items on metrics for surviving a process upset or LoC event. The recovery phase comprised of items on metrics for recovering from a process upset or catastrophic condition. Part-II is the ‘Glossary’ that contained definitions for the 15 terms used within the survey to assist the respondents with the domain terminology. This was done with the objective to maintain consistency in the respondents’ understanding of the survey questions. In order to ensure the quality and rationality of the questions, inputs and

suggestions from industrial experts and academic researchers in the area were incorporated in the final survey questionnaire.

The Qualtrics platform was used to conduct the survey. It was distributed via email after approval from the Texas A&M University Institutional Review Board - (IRB Number: IRB2016-0327D, IRB Approval Date: 09/22/2016, IRB Expiration Date: 09/15/2017). The PRAF survey is based on Likert type questionnaire, which produced categorical responses. Methods and techniques such as ordinal alpha, Kruskal-Wallis test, and polychoric correlations, relevant to analyze categorical responses have been used in the programming language R¹⁸⁴. The statistical analysis presented in this section made use of various packages within R such as rcompanion, psych, lattice, FSA, Rcmdr^{185, 186, 187, 188, 189}.

3.3.2. Survey respondents

The type of respondents for this survey had a pivotal role to answer the questions asked. The survey respondents were primarily identified from chemical process, and oil and gas fields with knowledge of process safety, risk assessment, and process operations. The survey was distributed to industry and academia and personal contacts of the authors. All survey responses were collected electronically and were anonymous. The survey results indicate that a total of 251 responses were recorded. Regarding the missing data, it should be noted that the answers do not always add up 251 because not all respondents answered all the survey questions.

The respondents' experience ranges from Process operations, Process safety to Other fields such as business, accounting, and purchasing departments. Industry, Academia, and Government are the various employment sectors representing the survey

respondents. Figures III.6 and III.7 present an overview of survey respondents by area of experience and employment sector. It is apparent from Figure III.6 that the majority of the respondents (72% of the total respondents) have spent most of their careers in process safety field. Figure III.7 shows that the respondents primarily work in industry (85%).

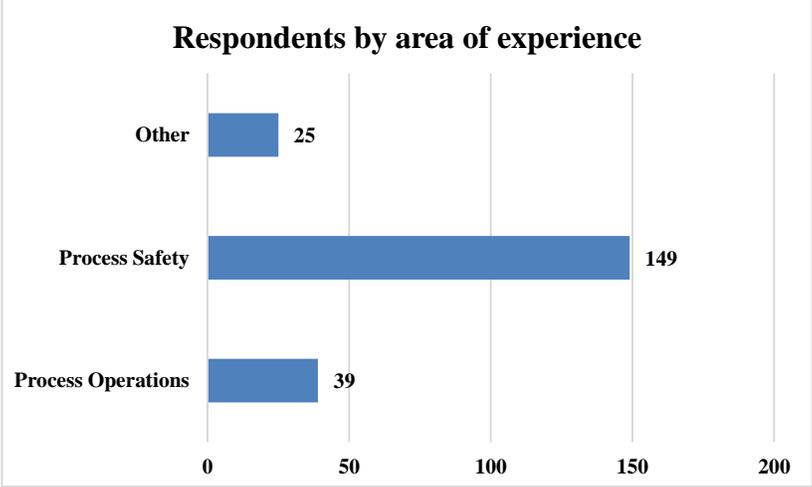


Figure III.6: Respondents by area of experience

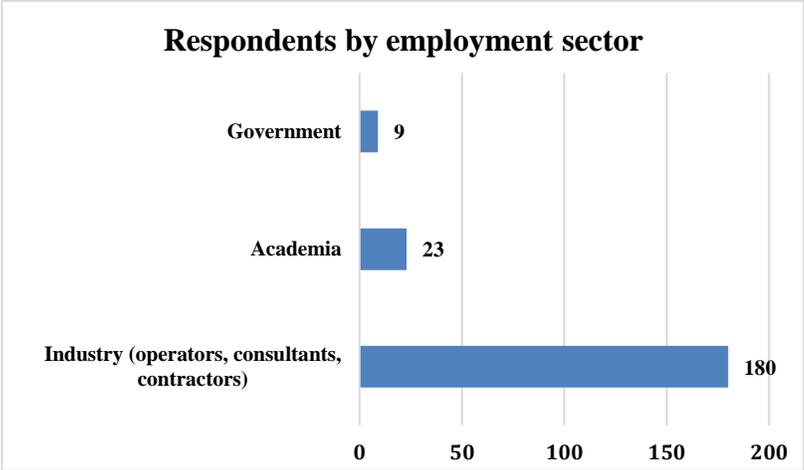


Figure III.7: Respondents by employment sector

3.3.3. Survey quality and analysis

The reliability of the survey questionnaire is fundamental to get accurate and good results. The literature on reliability has highlighted that if the alpha of the questionnaire is greater than 0.7, it has high internal consistency¹⁹⁰. This survey questionnaire was tested for reliability for the three different phases – avoidance, survival, and recovery. There is a large volume of published studies describing the role of Cronbach’s alpha as frequently used reliability index^{191, 192}. However, the first analyses of ordinal alpha as reliability index emerged in 2001, which proves to be a more accurate index for Likert-type formats^{191, 193}. Tables III.5, III.6 and III.7 report the ordinal alpha (based on the Polychoric correlation matrix) and Cronbach’s alpha (raw and standardized based on Pearson covariance and correlation matrices respectively) for the three PRAF phases.

Table III.5: Ordinal alpha and Cronbach’s alpha for Avoidance phase metrics

Item	Description	Ordinal alpha (Polychoric correlation matrix)	Raw/Cronbach alpha (Pearson covariance matrix)	Standardized alpha (Pearson correlation matrix)
Q1	Alarm rate	0.77	0.74	0.74
Q2	Equipment pieces operated outside fitness-for-service rating	0.76	0.73	0.73
Q3	Unplanned maintenance jobs	0.77	0.73	0.73
Q4	Rotatory equipment pieces operated outside vibration rating	0.76	0.73	0.73
Q5	Seal leaks	0.76	0.73	0.72
Q6	Process safety near-misses	0.76	0.73	0.73
Q7	Unplanned shutdowns	0.76	0.72	0.72
Q8	Communications on learning from incidents	0.76	0.72	0.72
Q9	Process hazard evaluations completion	0.74	0.70	0.69

Table III.5 Continued

Item	Description	Ordinal alpha (Polychoric correlation matrix)	Raw/Cronbach alpha (Pearson covariance matrix)	Standardized alpha (Pearson correlation matrix)
Q10	Past-due process safety actions	0.74	0.71	0.7
Q11	Shift handover communication violations	0.74	0.71	0.71

As can be seen from Table III.5 for the avoidance phase, all except the standardized alpha for item Q9 are ≥ 0.7 , hence all alpha values are acceptable and internally consistent and reliable.

Table III.6: Ordinal alpha and Cronbach's alpha for Survival phase metrics

Item	Description	Ordinal alpha (Polychoric correlation matrix)	Raw/Cronbach alpha (Pearson covariance matrix)	Standardized alpha (Pearson correlation matrix)
Q12	ESD/SIF system activations	0.83	0.81	0.81
Q13	Pressure relief valve/bursting disk activations	0.85	0.82	0.82
Q14	Mechanical trip activations	0.84	0.81	0.81
Q15	Process unit operation outside design limits	0.84	0.82	0.82
Q16	Changes executed through the Management of Change procedure	0.84	0.82	0.82
Q17	Work permits that met all requirements	0.84	0.82	0.82
Q18	On-time safety critical equipment (SCE) inspections completion	0.84	0.81	0.81
Q19	Management response to the inspection findings of safety critical equipment (SCE) deficiency	0.84	0.81	0.81

Table III.6 Continued

Item	Description	Ordinal alpha (Polychoric correlation matrix)	Raw/Cronbach alpha (Pearson covariance matrix)	Standardized alpha (Pearson correlation matrix)
Q20	Management of Change (MOC's) and Pre Start-up Safety Review (PSSR's) that met all requirements	0.83	0.80	0.80
Q21	Human factor related to fatigue risk management	0.84	0.81	0.81
Q22	Maintenance backlogs	0.83	0.80	0.80
Q23	Process safety required training sessions completed	0.83	0.80	0.81
Q24	Process safety required operations and maintenance procedures reviewed or revised as scheduled	0.84	0.81	0.81
Q25	Shift handover communication violations	0.83	0.80	0.80

From Table III.6, survival phase, all alpha values are ≥ 0.8 , hence are good and internally consistent and reliable.

Table III.7: Ordinal alpha and Cronbach's alpha for Recovery phase metrics

Item	Description	Ordinal alpha (Polychoric correlation matrix)	Raw/Cronbach alpha (Pearson covariance matrix)	Standardized alpha (Pearson correlation matrix)
Q26	Successful tests for emergency systems and procedures	0.75	0.73	0.73
Q27	Mock drills for emergency situations	0.76	0.72	0.72
Q28	Process safety required training sessions completed	0.69	0.66	0.66
Q29	Process safety required operations and maintenance procedures reviewed or revised as scheduled	0.7	0.66	0.67
Q30	Shift handover communication violations	0.74	0.71	0.71

Lastly, from Table III.7, for recovery phase, most of the items have ordinal alpha (more relevant for Likert type data analysis) ≥ 0.7 , hence are acceptable and internally consistent and reliable. Item Q28 has an ordinal alpha of 0.69~0.7. Overall, it can be concluded that the survey quality is good and acceptable as the questionnaire items are found to be statistically reliable and internally consistent.

3.3.4. Results

RQ1: what are the most important metrics for each of the 3 phases of PRAF – avoidance, survival, and recovery?

The following sections present the results for three different phases of avoidance, survival, and recovery.

Descriptive statistics

Tables III.8, III.9, and III.10 illustrate the descriptive statistics such as mean, median, skewness, kurtosis and the standard error of the questionnaire items for avoidance, survival and recovery phases, respectively.

As can be seen in Table III.8, most items except Q2, Q6, and Q10 have skewness between -0.5 and 0.5, which implies response distributions are fairly symmetrical or in other words, most responses (essential, important, helpful, and necessary) to various metrics occur at regular frequencies. Items Q2 and Q10 have a skewness of -0.79 and -0.61 respectively, which means response distribution is moderately negatively skewed or a higher percentage of responses for these two metrics fall in the essential or important categories. For item Q6, skewness < -1.0 , which implies distribution is far from symmetrical with a long tail on the left or most of the responses for this metric fall in the essential or important categories. Negative kurtosis for most items reflects flatter

distribution except for item Q2 with a positive kurtosis meaning slightly more peaked distribution than Gaussian, which means for Q2, the responses are more clustered around the mean value (3.49) and have a smaller standard deviation. This corroborates the analysis of the skewness value for item Q2.

Table III.8: Descriptive statistics (Avoidance phase)

Avoidance						
Item	Description	Mean	Median	Skewness	Kurtosis	Standard error
Q1	Alarm rate	2.68	3	-0.06	-0.62	0.06
Q2	Equipment pieces operated outside fitness-for-service rating	3.49	4	-0.79	0.43	0.04
Q3	Unplanned maintenance jobs	2.79	3	-0.13	-0.5	0.05
Q4	Rotatory equipment pieces operated outside vibration rating	3.04	3	-0.14	-0.81	0.05
Q5	Seal leaks	3.14	3	-0.37	-0.59	0.05
Q6	Process safety near-misses	3.54	4	-1.18	0.68	0.05
Q7	Unplanned shutdowns	2.98	3	-0.28	-0.65	0.06
Q8	Communications on learning from incidents	2.40	2	0.39	-0.58	0.06
Q9	Process hazard evaluations completion	2.84	3	-0.33	-0.69	0.06
Q10	Past-due process safety actions	3.27	3	-0.61	-0.34	0.05
Q11	Shift handover communication violations	2.95	3	-0.14	-0.97	0.06

Table III.9 represents skewness between -0.5 and 0.5 for most items except Q12, Q13, Q15, and Q19. This implies that the response distributions are fairly symmetrical, or in other words, most responses (essential, important, helpful, and necessary) to various metrics occur at regular frequencies.

Table III.9: Descriptive statistics (Survival phase)

Survival						
Item	Description	Mean	Median	Skewness	Kurtosis	Standard error
Q12	ESD/SIF system activations	3.18	3.00	-0.59	-0.42	0.06
Q13	Pressure relief valve/bursting disk activations	3.43	4.00	-1.02	0.17	0.05
Q14	Mechanical trip activations	3.05	3.00	-0.27	-0.23	0.05
Q15	Process unit operation outside design limits	3.46	4.00	-1.08	0.49	0.05
Q16	Changes executed through the Management of Change ¹⁹⁴ procedure	2.63	2.50	0.06	-1.1	0.07
Q17	Work permits that met all requirements	2.65	3.00	-0.09	-0.9	0.07
Q18	On-time safety critical equipment (SCE) inspections completion	3.30	3.00	-0.48	-0.9	0.05
Q19	Management response to the inspection findings of safety critical equipment (SCE) deficiency	3.50	4.00	-0.79	-0.39	0.04
Q20	Management of Change (MOC's) and Pre Start-up Safety Review (PSSR's) that met all requirements	2.94	3.00	-0.15	-0.88	0.06
Q21	Human factor related to fatigue risk management	3.08	3.00	-0.12	-1.04	0.05
Q22	Maintenance backlogs	2.83	3.00	-0.31	-0.36	0.06
Q23	Process safety required training sessions completed	2.83	3.00	-0.03	-0.86	0.06
Q24	Process safety required operations and maintenance procedures reviewed or revised as scheduled	2.81	3.00	-0.06	-0.7	0.06
Q25	Shift handover communication violations	2.85	3.00	-0.1	-0.86	0.06

Items Q12 and Q19 have a skewness of -0.59 and -0.79 respectively; which means response distribution is moderately negatively skewed or a higher percentage of responses for these two metrics fall in the essential or important. Also, skewness < -1.0 for items Q13 and Q15 that implies distribution is far from symmetrical with a long tail on the left or most of the responses for this metric fall in the essential or important categories. Negative kurtosis for most items reflects flatter distribution except for items Q13 and 15 with a positive kurtosis meaning more peaked distribution than Gaussian, which means for Q13 and Q15, the responses are more clustered around the mean value (3.43, 3.46 respectively) and have a smaller standard deviation. This validates the analysis of the skewness value for items Q13 and Q15.

Table III.10: Descriptive statistics (Recovery phase)

Recovery						
Item	Description	Mean	Median	Skewness	Kurtosis	Standard error
Q26	Successful tests for emergency systems and procedures	3.23	3.00	-0.76	0.06	0.06
Q27	Mock drills for emergency situations	3.03	3.00	-0.13	-0.9	0.05
Q28	Process safety required training sessions completed	2.88	3.00	-0.18	-0.93	0.06
Q29	Process safety required operations and maintenance procedures reviewed or revised as scheduled	2.68	3.00	-0.11	-0.7	0.06
Q30	Shift handover communication violations	2.51	2.00	0.07	-0.99	0.07

It is clear from Table III.10 that skewness is between -0.5 and 0.5 for most items, implies response distributions are close to symmetrical, or in other words, most responses (essential, important, helpful, and necessary) to various metrics occur at regular

frequencies. Item Q26 has a skewness of -0.76, which means response distribution is moderately negatively skewed or a higher percentage of responses for these two metrics fall in the essential or important. Item Q30 has a positive skewness that means it has a slightly long tail to the right or most of the responses for this metric fall in the helpful or unnecessary categories. Negative kurtosis for most items reflects flatter distributions except for item Q26 with a positive kurtosis meaning more peaked distribution than Gaussian, which means for Q26, the responses are more clustered around the mean value (3.23) and have a smaller standard deviation. This supports the analysis of the skewness value for item Q26.

Metrics significance based on respondents' perception

All survey respondents were asked to rank the metrics in each of the three phases according to their effectiveness. The results are presented in Figures III.8, III.9, and III.10.

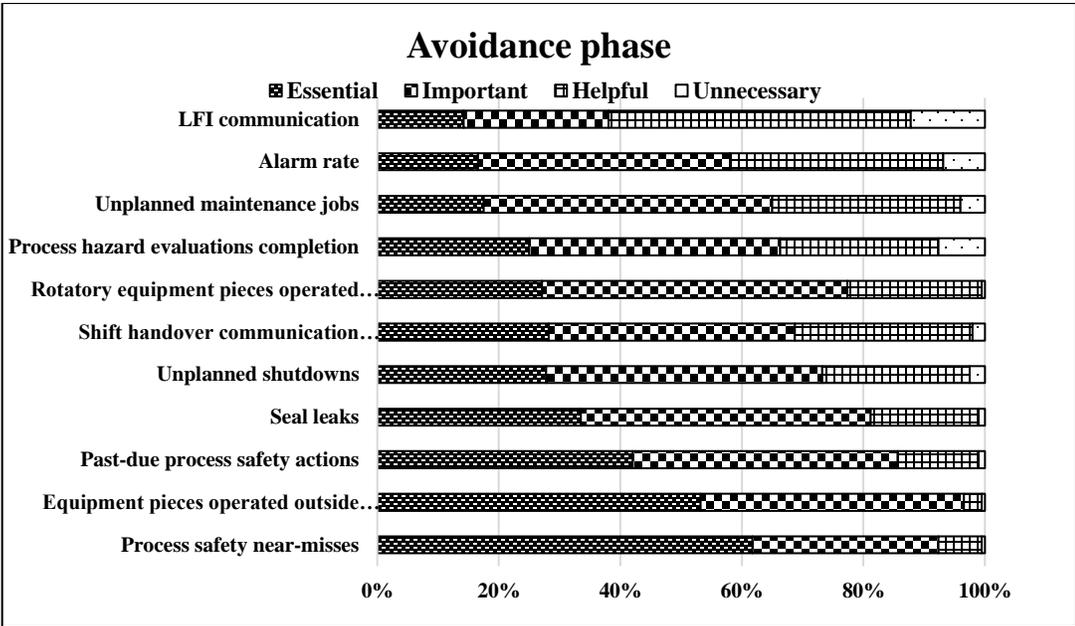


Figure III.8: Avoidance phase metrics and respondents perception on effectiveness

Some conclusions that can be drawn from Figure III.8 are as follows:

- Most of the metrics except LFI communication are either essential or important to >75% of respondents on average.
- Process safety near misses was the metric perceived most as the essential metric to predict a process upset event by most respondents.
- Equipment pieces operated outside fitness-for-service rating, and the past due process safety actions are considered to be other essential metrics after near misses for prediction of process upset events.
- LFI communication is considered to be helpful by most respondents, yet >10% of responses found it unnecessary for predicting process upset. Further analysis is done to see variations between different groups based on area of experience and employment sector.
- It is surprising to note that alarm rate was found to be unnecessary in the prediction of process upset events by ~7% of respondents. It would be interesting to learn more about the respondents' background to gain more insights on the same.

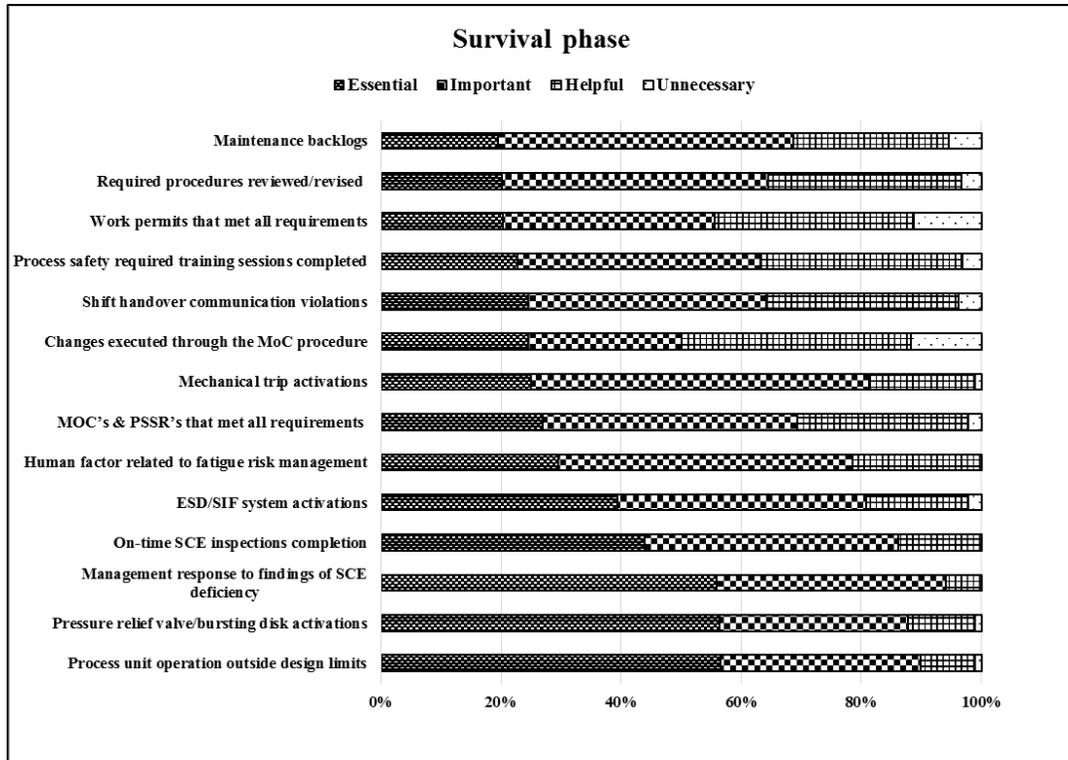


Figure III.9: Survival phase metrics and respondents perception on effectiveness

Following are some of the interesting conclusions from Figure III.9:

- A higher number of respondents found Process unit operation outside design limits, Pressure relief valve/bursting disk activations and Management response to findings of SCE deficiency as the essential metrics to prevent LoC events; markedly more than other metrics.
- Mechanical trip activations and Maintenance backlogs are considered to be important metrics in the survival of LoC events. The response to the first six metrics look very similar, within an accuracy of the analysis.
- The majority of the respondents found some of the social factors such as Procedures revised and updated, Process safety related training sessions

completed important and useful. Human factor related to fatigue risk management is the most important metric based on the results. This provides an indication of strong significance of social metrics in the risk and resilience assessment.

- On-time SCE inspections completion, Management response to findings of SCE deficiency, and the Human factor related to fatigue risk management were found to be necessary by all respondents.
- It is surprising to find that ~11% of responses considered robust work permit system and changes executed through MoC as unnecessary to survive a LoC event.

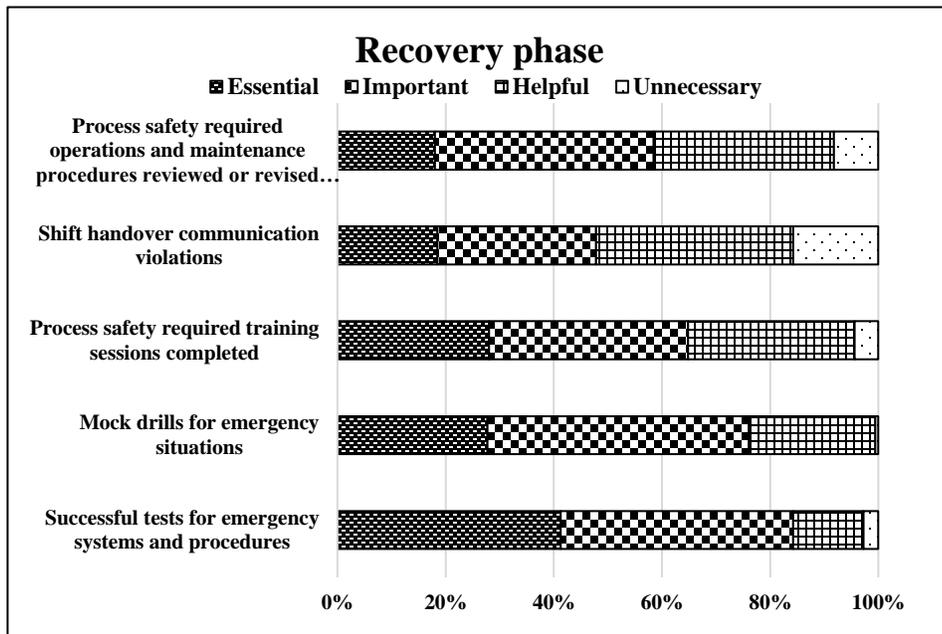


Figure III.10: Recovery phase metrics and respondents perception on effectiveness

From Figure III.10, the following can be concluded:

- Of the five metrics, a higher number of respondents found Successful tests for emergency systems and procedures as the essential metric to recover from a process upset/LoC event.
- Though not thought as essential Mock drills for emergency situations was most important metric and had least counts as an unnecessary metric.
- Some of the social factors such as procedures revised and updated, and shift handover communication violations were perceived to be important and helpful by the majority of the respondents but not essential. The authors believe there is still some unexploited potential and is an area for improvement.

Correlation analysis

The rule of thumb is if $r > 0.8$ or $r < -0.8$, variables correlate too highly and if $-0.3 < r < 0.3$, they correlate too lowly with other variables. If the variables relate too highly, it means that it is difficult to determine how the variables contribute uniquely to the factor¹⁹⁵. If the variables relate too lowly, it means that they measure different underlying construct as the other variables.

As seen from Table III.11, most of the correlations (underlined) are too low ($-0.3 < r < 0.3$). This implies they measure different underlying construct as the other metrics. It is evident from Table III.12, most of the correlations (underlined) are too low ($-0.3 < r < 0.3$). This implies that most of the metrics measure different underlying construct as the other metrics.

Table III.11: Polychoric correlation matrix (Avoidance)

Correlation matrix (Polychoric), Avoidance											
	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Q1	1	<u>0.24</u>	<u>0.08</u>	<u>0.21</u>	<u>0.17</u>	<u>0.18</u>	<u>0.22</u>	<u>0.13</u>	<u>0.2</u>	<u>0.17</u>	<u>0.15</u>
Q2	<u>0.24</u>	1	<u>0.19</u>	0.31	<u>0.16</u>	<u>0.27</u>	<u>0.16</u>	<u>0.13</u>	<u>0.25</u>	<u>0.21</u>	0.32
Q3	<u>0.08</u>	<u>0.19</u>	1	<u>0.12</u>	<u>0.17</u>	<u>0.14</u>	<u>0.29</u>	<u>0.23</u>	<u>0.25</u>	<u>0.19</u>	<u>0.28</u>
Q4	<u>0.21</u>	0.31	<u>0.12</u>	1	<u>0.29</u>	<u>0.15</u>	<u>0.18</u>	<u>0.13</u>	<u>0.25</u>	<u>0.17</u>	<u>0.28</u>
Q5	<u>0.17</u>	<u>0.16</u>	<u>0.17</u>	<u>0.29</u>	1	<u>0.2</u>	<u>0.17</u>	<u>0.2</u>	0.32	<u>0.28</u>	<u>0.2</u>
Q6	<u>0.18</u>	<u>0.27</u>	<u>0.14</u>	<u>0.15</u>	<u>0.2</u>	1	<u>0.29</u>	<u>0.14</u>	<u>0.23</u>	0.33	<u>0.24</u>
Q7	<u>0.22</u>	<u>0.16</u>	<u>0.29</u>	<u>0.18</u>	<u>0.17</u>	<u>0.29</u>	1	<u>0.24</u>	<u>0.26</u>	<u>0.28</u>	<u>0.23</u>
Q8	<u>0.13</u>	<u>0.13</u>	<u>0.23</u>	<u>0.13</u>	<u>0.2</u>	<u>0.14</u>	<u>0.24</u>	1	0.43	<u>0.29</u>	0.31
Q9	<u>0.2</u>	<u>0.25</u>	<u>0.25</u>	<u>0.25</u>	0.32	<u>0.23</u>	<u>0.26</u>	0.43	1	0.62	0.42
Q10	<u>0.17</u>	<u>0.21</u>	<u>0.19</u>	<u>0.17</u>	<u>0.28</u>	0.33	<u>0.28</u>	<u>0.29</u>	0.62	1	0.44
Q11	<u>0.15</u>	0.32	<u>0.28</u>	<u>0.28</u>	<u>0.2</u>	<u>0.24</u>	<u>0.23</u>	0.31	0.42	0.44	1

Table III.13 shows that few of the correlations (underlined) are too low ($-0.3 < r < 0.3$). Most of the correlations are < 0.8 . This implies that most of the metrics contribute uniquely to the recovery factor as they are neither correlated highly nor lowly.

Table III.12: Polychoric correlation matrix (Survival)

	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25
Q12	1	0.54	0.61	0.3	<u>0.15</u>	<u>0.15</u>	<u>0.29</u>	<u>0.24</u>	<u>0.29</u>	0.53	0.3	0.3	<u>0.21</u>	<u>0.27</u>
Q13	0.54	1	0.66	0.4	<u>0.05</u>	<u>-0.02</u>	<u>-0.02</u>	<u>0.23</u>	<u>0.12</u>	<u>-0.23</u>	<u>0.2</u>	<u>0.15</u>	<u>0.05</u>	<u>0.22</u>
Q14	0.61	0.66	1	0.32	<u>0.09</u>	<u>0.1</u>	<u>0.22</u>	0.32	<u>0.28</u>	<u>0.2</u>	<u>0.29</u>	0.31	<u>0.19</u>	<u>0.22</u>
Q15	0.3	0.4	0.32	1	<u>0.2</u>	<u>0.1</u>	<u>0.06</u>	0.52	<u>0.18</u>	<u>0.25</u>	<u>0.09</u>	<u>0.21</u>	<u>0.14</u>	<u>0.29</u>
Q16	<u>0.15</u>	<u>0.05</u>	<u>0.09</u>	<u>0.2</u>	1	0.49	<u>-0.02</u>	<u>0.14</u>	0.41	<u>0.24</u>	0.3	<u>0.25</u>	0.32	0.33
Q17	<u>0.15</u>	<u>-0.02</u>	<u>0.1</u>	<u>0.1</u>	0.49	1	<u>0.25</u>	<u>0.24</u>	0.5	<u>0.25</u>	<u>0.25</u>	0.33	0.32	<u>0.26</u>
Q18	<u>0.29</u>	<u>-0.02</u>	<u>0.22</u>	<u>0.06</u>	<u>-0.02</u>	<u>0.25</u>	1	0.46	0.55	<u>0.24</u>	0.47	0.37	0.33	0.3
Q19	<u>0.24</u>	<u>0.23</u>	0.32	0.52	<u>0.14</u>	<u>0.24</u>	0.46	1	0.37	0.38	0.35	<u>0.27</u>	<u>-0.01</u>	<u>-0.01</u>
Q20	<u>0.29</u>	<u>0.12</u>	<u>0.28</u>	<u>0.18</u>	0.41	0.5	0.55	0.37	1	0.37	0.40	0.46	0.52	0.36
Q21	0.53	<u>-0.23</u>	<u>0.2</u>	<u>0.25</u>	<u>0.24</u>	<u>0.25</u>	<u>0.24</u>	0.38	0.37	1	0.35	0.43	<u>0.23</u>	<u>0.26</u>
Q22	0.3	<u>0.2</u>	<u>0.29</u>	<u>0.09</u>	0.3	<u>0.25</u>	0.47	0.35	0.40	0.35	1	0.48	0.37	0.54
Q23	0.3	<u>0.15</u>	0.31	<u>0.21</u>	<u>0.25</u>	0.33	0.37	<u>0.27</u>	0.46	0.43	0.48	1	0.47	0.5
Q24	<u>0.21</u>	<u>0.05</u>	<u>0.19</u>	<u>0.14</u>	0.32	0.32	0.33	<u>-0.01</u>	0.52	<u>0.23</u>	0.37	0.47	1	0.43
Q25	<u>0.27</u>	<u>0.22</u>	<u>0.22</u>	<u>0.29</u>	0.33	<u>0.26</u>	0.3	<u>-0.01</u>	0.36	<u>0.26</u>	0.54	0.5	0.43	1

Table III.13: Polychoric correlation matrix (Recovery)

Correlation matrix (Polychoric), Recovery					
	Q26	Q27	Q28	Q29	Q30
Q26	1.00	0.50	0.35	0.32	<u>0.26</u>
Q27	0.50	1.00	0.40	0.30	<u>0.21</u>
Q28	0.35	0.40	1.00	0.64	0.49
Q29	0.32	0.30	0.64	1.00	0.57
Q30	<u>0.26</u>	<u>0.21</u>	0.49	0.57	1.00

RQ2: are there any differences in viewpoints of various groups of survey respondents?

Kruskal-Wallis test was used to understand whether survey response to metrics, where responses are measured on an ordinal scale, differed based on area of experience and employment sector. One metric that showed surprising or unexpected results from each of the three phases was chosen. These metrics are- LFI communication from avoidance phase, Work permits that met all requirements from survival phase, and Mock drills for emergency situations from recovery phase. For the area of experience, the dependent variable is "survey response to metrics", measured on a 4-point scale from "essential" to "unnecessary", and the independent variable is "area of experience", which has three independent groups: "process safety", "process operations" and "other". For the employment sector, the dependent variable is "survey response towards metrics", measured on a 4-point scale from "essential" to "unnecessary", and the independent variable is "employment sector", which has three independent groups: "industry", "academia" and "government".

Table III.14: Kruskal-Wallis test results

	Area of experience			Employment Sector		
	Q17: Work permits that met all requirements	Q27: Mock drills for emergency situations	Q8: LFI Communication	Q17: Work permits that met all requirements	Q27: Mock drills for emergency situations	Q8: LFI Communication
Chi-square	0.065	2.33	0.009	4.34	0.522	7.36
DF	2	2	2	2	2	2
p-value	0.968	0.312	1	0.114	0.770	0.03

Following are some conclusions based on Table III.14:

- A Kruskal-Wallis test showed that there was a statistically significant difference in LFI communication metric response between the different groups based on employment sector, $\chi^2 = 7.36$, $p = 0.03$ ($p < 0.05$). This result is consistent with the mosaic plot analysis.
- Items Q17: Work permits that met all requirements, Q27: Mock drills for emergency situations, and Q8: LFI Communication were not statistically different based on the area of experience.
- Items Q17: Work permits that met all requirements, Q27: Mock drills for emergency situations were not statistically different based on employment sector.

RQ3: what are the weights for each of the metrics?

The weights are calculated based on the survey response using the following equation.

$$\frac{N_e*W_e+N_i*W_i+N_h*W_h+N_u*W_u}{N_{total}} \quad (3.1)$$

The scaled weights are calculated by dividing with the maximum weight within that phase.

The weights for the avoidance, survival and recovery phases range from 2.4 to 3.53; 2.61 to 3.49; and 2.49 to 3.22 with an average weight of 3.01; 3.04; and 2.86, respectively. The table is quite revealing in several ways:

- Avoidance phase: Process safety near-misses metric has the highest weight (3.53 or scaled weight of 1), followed by Equipment pieces operated outside fitness-for-service rating (3.49 or scaled weight of 0.99) and Past-due process safety actions (3.27 or scaled weight of 0.93). The two metrics with lowest weights are LFI communication (2.4 or scaled weight of 0.68) and alarm rate (2.68 or scaled weight of 0.76).
- Survival phase: Management response to the inspection findings of safety critical equipment (SCE) deficiency has the highest weight (3.49 or scaled weight of 1), followed by Process unit operation outside design limits (3.47 or scaled weight of 0.99) and Pressure relief valve/bursting disk activations (3.44 or scaled weight of 0.98). The two metrics with lowest weights are Changes executed through the Management of Change procedure (2.61 or scaled weight of 0.75) and Work permits that met all requirements (2.65 or scaled weight of 0.76).
- Recovery phase: Successful tests for emergency systems and procedures has the highest weight (3.22 or scaled weight of 1), followed by Mock drills for

emergency situations (3.02 or scaled weight of 0.94). The metric with lowest weight is Shift handover communication violations (2.49 or scaled weight of 0.77).

Additional results

Relationship analysis using mosaic plots

A mosaic plot is a graphical display that allows you to examine the relationship between two or more categorical variables. In this section, three mosaic plots are presented in Figures III.11, III.12, and III.13 and results from each plot are summarized.

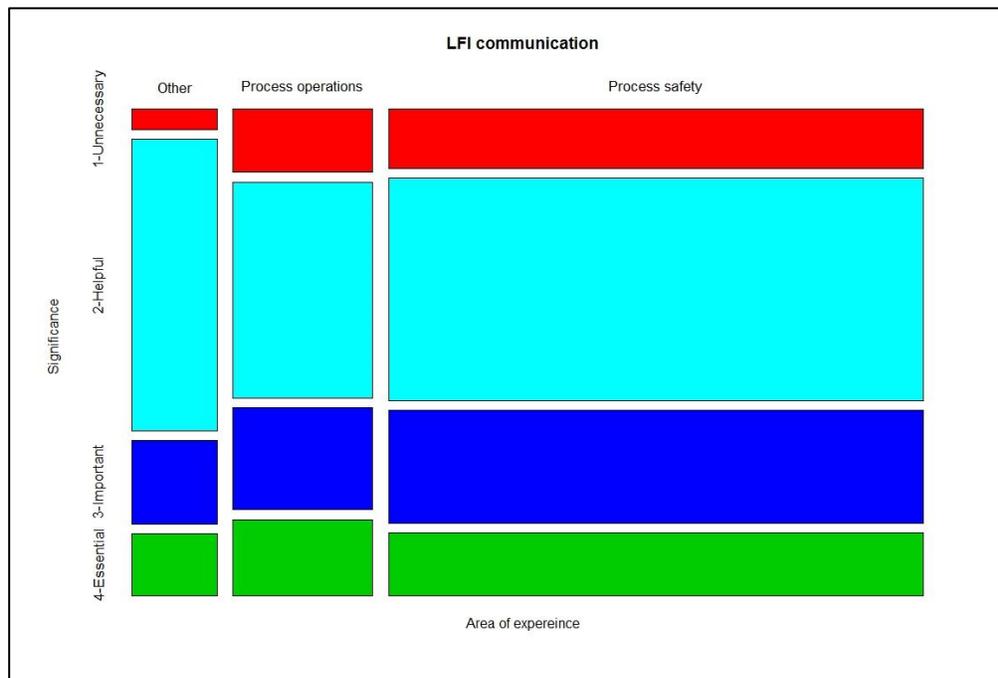


Figure III.11: Relationship between experience areas (LFI communication metric)

This is a mosaic plot looking at the relationship between the area of experience group (process safety, process operations, and other) and significance (essential, important,

helpful, and unnecessary) of the LFI communication metric. From Figure III.11, we can note the following:

- The respondents from process safety and process operations categories have approximately equal percentages of significance as important, helpful, and unnecessary.
- The other category respondents have a higher percentage of significance as helpful.
- The process operations category respondents have a slightly higher percentage of significance as essential.

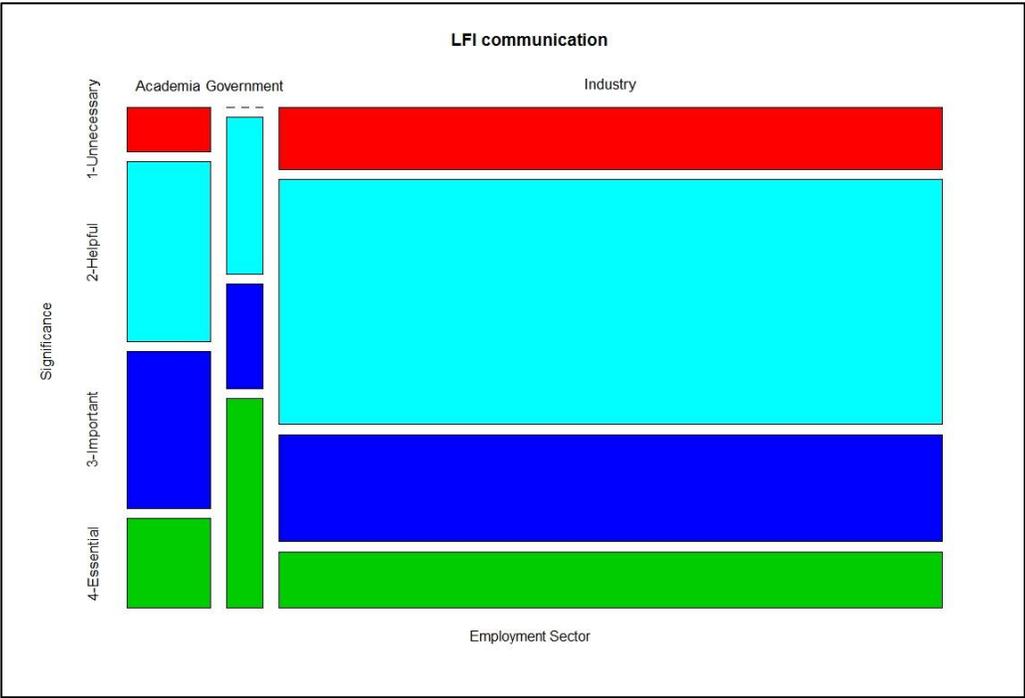


Figure III.12: Relationship between employment sectors (LFI communication metric)

This is a mosaic plot looking at the relationship between employment sectors (industry, academia, and government) and significance (essential, important, helpful, and unnecessary) of the LFI communication metric. It is apparent from the Figure III.12 that:

- The respondents from all three employment sector categories have varying proportions for various significance levels.
- A higher percentage of unnecessary significance is observed for industry sector respondents. Also, a higher percentage of helpful significance is recorded for industry sector.
- A higher percentage of essential significance is observed for government sector respondents. Also, no respondents from the government sector perceived LFI communication as unnecessary.

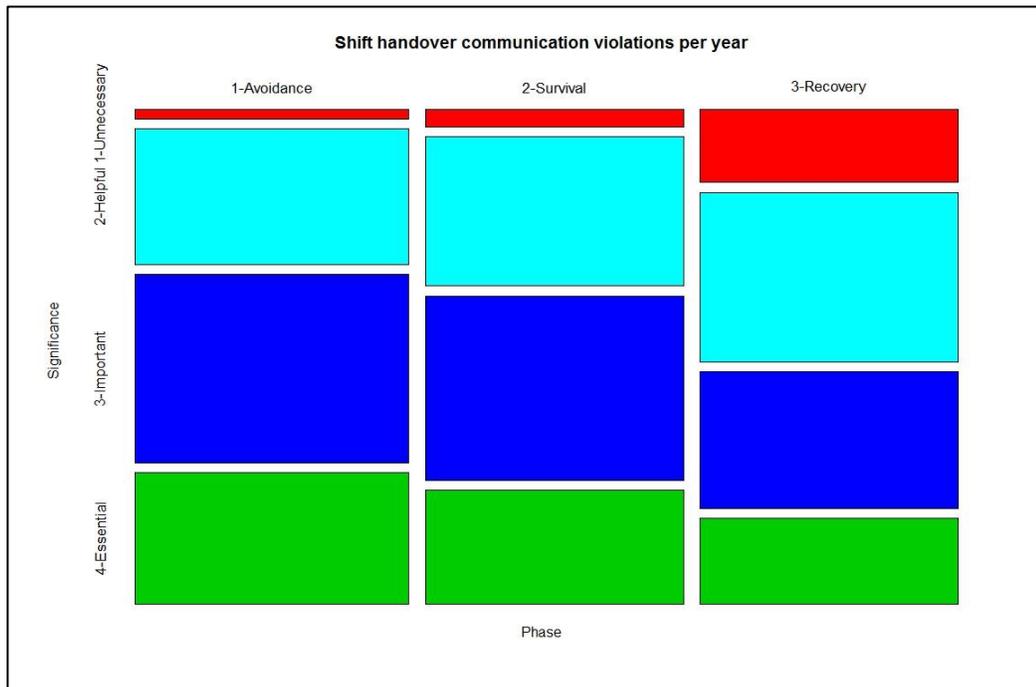


Figure III.13: Relationship between phases and significance

This is a mosaic plot looking at the relationship between three PRAF phases (avoidance, survival, recovery) and significance (essential, important, helpful, and unnecessary) of the shift handover communication violations metric. It can be seen from Figure III.13 that:

- A larger percentage of essential significance for avoidance phase.
- All phases have approximately equal percentages of helpful significance level.
- A slightly higher percentage of unnecessary significance level is recorded for recovery phase.

Observations

During the survey response data analysis, following observations were made:

- No data-driven or validated method was followed to determine the phase/s of application of each metric. The allocation of metric phases was based on limited literature sources on the topic and professional experience of the authors. For example, some experts suggested that Management of Change (MOC's) and Pre Start-up Safety Review (PSSR's) that met all requirements to be far more significant metric in avoidance phase than in survival phase.
- It would be interesting to test the level of significance of some of the metrics such as LFI communication, Changes executed through the Management of Change procedure based on all three phases. This could be one of the potential reasons that these metrics were reported as unnecessary for a particular phase.

- For Shift handover communication violation metric, further analysis in way of interviews with experts in the field to understand the reasons for finding that this metric was most significant in avoidance phase, than survival and recovery would be advantageous.
- Another remarkable contribution would be to find the relative level of significance of three phases – avoidance, survival, and recovery in the overall risk and resilience assessment.

3.3.5. Application

Risk and resilience assessment

Within the PRAF, the uncertain variables for an actual scenario in resilience assessment can be described in the form of a probability distribution function. The posterior values of the statistical parameters of these uncertain variables would be inferred based on the prior, and likelihood function formed from the resilience metrics information. This would reduce the uncertainty in the measured process parameters. It will be erroneous to give equal weightage to all metrics in the assessment. Hence, in order to have a comparatively accurate analysis, resilience metrics weights obtained in the current study would be utilized instead of equal weights.

General purpose

Another application of the results obtained in this study can assist an organizations' senior management in the process industries in identification of the most significant metrics. For example, it is evident from the analysis that the Process safety near-misses, Management response to the inspection findings of safety critical equipment (SCE) deficiency, and Successful tests for emergency systems and procedures metrics are the

most significant for avoidance, survival and recovery phases respectively. These results can be applied to various risk, safety, and resilience assessment studies. This would be conducive in making decisions on optimal allocation of resources such as financial, and manpower towards the metrics management system (collection of data, measurement of metrics, trending analysis, making recommendations or having corrective actions) within their organizations. Also, it would be beneficial for small and medium level organizations to initiate the implementation of a metrics management system. The current study can be extended to develop correlations with the use of actual data on these metrics and process upsets and/or incidents.

3.4. Quantification of social aspects (DSM)

As established in previous chapters, process systems are complex socio-technical systems and this characteristic makes them vulnerable to upset conditions or in the worst case scenario disastrous incidents. Many incidents in literature have been reported to occur due to lack of understanding of social factors (human and organizational) impact or both individual and mutual contribution and their quantification. Considering the significance of these social aspects in process system risk and resilience analysis, there is a need to develop quantification methods for these aspects. Some efforts have been focused in this direction in the past years, however, these are limited in their approach or are not applied to the process systems analysis. One of the prior research has been applied in the software and healthcare industry to study the expected and actual interactions between the engineering and emergency care teams. This study builds on that previous research method and develops it for the process industry. A case study of reactor charging is used to demonstrate the methodology. An overlay of expected and actual interactions in the form

of a matrix is built which is utilized to calculate the socio-technical congruence metric. Analysis and quantification of social aspects demonstrate that merely engaging the right stakeholders such as operators, shift supervisors in the process, the MDM can itself lead to performance improvement. This type of analysis sets the basis for future studies on quantification of these social aspects such as training, operating procedures, learning from incident communication *etc.* in the process systems risk and resilience assessment.

3.4.1. Motivating example

Congruence analysis is conducted to quantify the interactions within the socio-technical system^{196, 197}. In order to do so, we consider the reactor charging procedure and construct a multi-domain matrix (MDM) to model the two domains involved in this procedure—process and people—and the interactions across them.

The steps in the reactor charging procedure make up the process domain, and the personnel performing those steps make up the people domain. Thus, the MDM contains four quadrants, two design structure matrices (DSMs) representing interactions within the two domains and two domain mapping matrices (DMMs) representing dependencies across the domains. A schematic of the quadrant model representing the hierarchical MDM is shown in Figure III.14.

In the Figure III.14, the upper left quadrant of the MDM, is the process architecture DSM depicting the technical system—the general steps of the reactor charging procedure. Similarly, the lower right quadrant, is the organization architecture DSM representing either actual or reported communication among the members of the team. The upper right and lower left, respectively, are the two domain mapping matrices in that they map entities

in the technical domain (the process steps) to those in the social domain (the team members) and vice versa.

The upper right quadrant is termed the “trigger task matrix” because it represents the activities that “trigger” a team member to perform his/her task. That is, a marking in a cell within this quadrant indicates that the person listed in the corresponding column is triggered to complete some task by the completion of another task listed in the corresponding row. This signaling is termed “trigger communication.” The lower left quadrant represents a much simpler relationship, the tasks for which each team member is responsible.

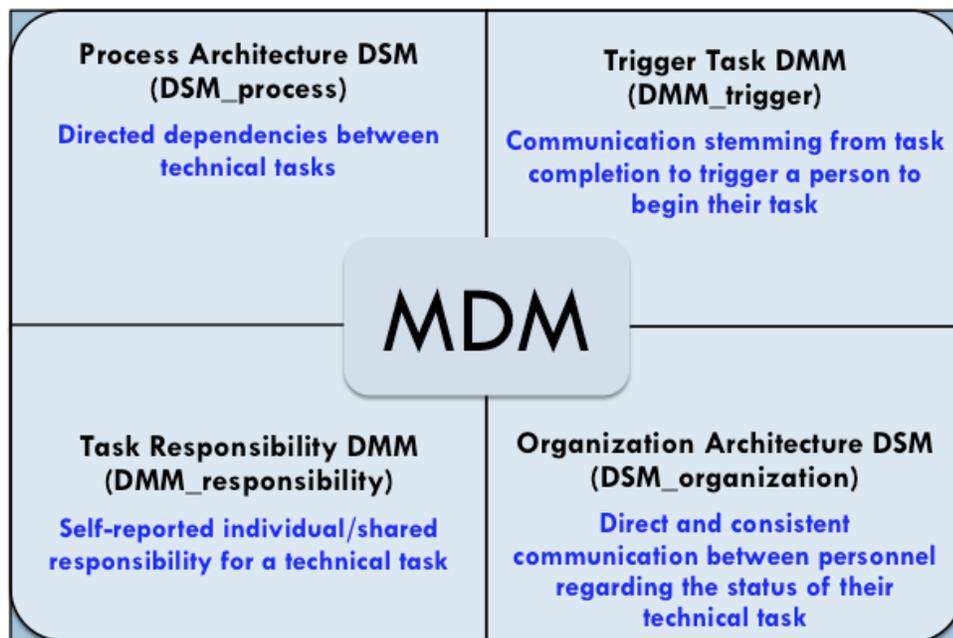


Figure III.14: The four quadrants of a two-domain MDM for reactor charging

The integrated analysis of these matrices leads to a process map of reactor charging procedure as shown in the Figure III.15. This process map represents the reactor charging procedure and is derived from the MDM and is based on the ISA 88 standard¹⁹⁸. It is a

sequence of steps that need to be followed in the reactor charging procedure and has the triggers and checks that can be both manual and automated. Using this, congruence matrix is constructed which is discussed in the results section.

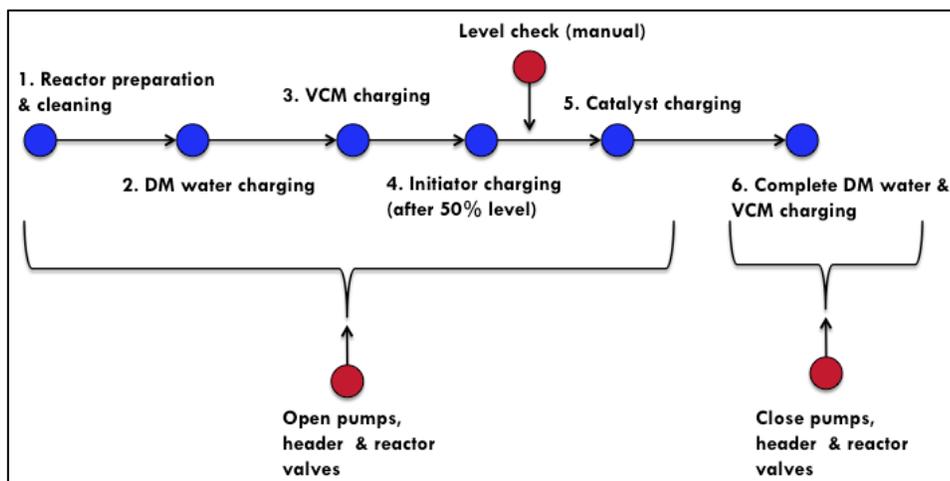


Figure III.15: Reactor charging procedure

The expected and reported interactions in the reactor charging procedure were compared by overlaying the two matrices according to the framework, which is based on a formalism originally developed by¹⁹⁹. Avnet expanded the formalism and called the result the congruence matrix²⁰⁰

The result, which is referred to here as the congruence matrix, can be used to highlight four distinct cases in mapping expected to reported communication: # (interactions expected and take place), X (interactions expected but does not take place), O (interactions not expected but take place), and <blank> (interactions neither expected nor happened). A congruence matrix comparing reported interactions to the expected interactions is shown in Figure III.16.

	Control room operator	Field operator	Previous shift operator	Shift Operator	Previous shift supervisor	Shift supervisor
Control room operator		X		#		O
Field operator	X			#	O	O
Previous shift operator				X	#	
Shift Operator	#	#	X			
Previous shift supervisor		O	#			#
Shift supervisor	O	O			#	

Figure III.16: Reactor charging procedure: congruence matrix

Along with the congruence matrix, a summary of the statistics for the counts of the cell values is given in Figure III.17. These counts are used to calculate the socio-technical congruence metric (C_{st}) by Eq. (3.2). The value of congruence belongs to the [0,1] interval that represents the proportion of coordination requirements that were satisfied through some type of coordination activity or mechanism.

	NO	X	Blank
Actual interactions	16	4	12
	YES	#	0
	14	8	6
		YES	NO
		12	18
		Required interactions	

Figure III.17: Summary statistics

$$C_{ST} = \frac{0.7N_{\#} + 0.3N_{Blank}}{N} \quad (3.2)$$

where N is the number of team members depicted in the matrix

$$C_{st} = 0.26$$

The higher value close to 1 implies good performance of the socio-technical system. This result based on plant specific data is utilized in the statistical analysis to derive an improved uncertainty probability distribution.

3.5. Summary

In general, systems based resilience theory has gained momentum and has recently been applied by organizations to various critical infrastructure elements which are subjected to internal and external, as well as known and unknown, disruptions⁷. Resilience engineering is an idea that cannot at present be regulated and it is the ingenuity and responsibility of the organization and society to understand the business case for resilient systems and organizations thus promoting overall business resilience – and in the long

term profitability. The concepts of process system resilience and a unified taxonomy for a common reference framework are proposed in this chapter. Further, a novel, integrated, time dependent, quantifiable framework for process resilience termed PRAF - 'Process Resilience Analysis Framework' is presented in the context of improved risk and safety management. As illustrated, the key aspects of process system resilience are early detection (ED), error tolerant design (ETD), recoverability (R), and plasticity (P). In application, use of these aspects to conduct predictability, survivability and recoverability analysis for a process system is not trivial. Nonetheless, the proposed resilience metrics including both technical and social resilience indicators would in principle allow for system optimization to develop effective risk management strategies in design and operations of such systems. With this process resilience analysis framework (PRAF), three major issues in the field of risk management in the process industry will be addressed: reduced LoC events, reduced consequences from failures and quicker recovery.

In the resilience metrics study, for the avoidance phase, the process safety near-miss metric has the highest weight (3.53 or scaled weight of 1), the LFI communication (2.4 or scaled weight of 0.68) has the lowest weight, of the eleven metrics examined. For the survival phase, management response to the inspection findings of safety critical equipment (SCE) deficiency has the highest weight (3.49 or scaled weight of 1), changes executed through the Management of Change ¹⁹⁴ procedure (2.61 or scaled weight of 0.75) has the lowest weight, of the fourteen metrics examined. For the recovery phase, successful tests for emergency systems and procedures has the highest weight (3.22 or scaled weight of 1) and the shift handover communication violations (2.49 or scaled weight of 0.77) has the lowest weight, of the five metrics examined. Some of the detailed findings of this

study, provided additional insights such as that shift handover communication violation metric had a lower percentage of ‘essential’ significance for the recovery (18%) phase vs survival (24%) and avoidance (28%) phases. Some other additional results extended our knowledge on the different perception of the respondents based on their area of experience and the employment sector for LFI communication metric. The results of the reliability analysis have shown that the survey questionnaire is reliable and has internal consistency. Additionally, the correlation analysis of the metrics in the avoidance and survival phases was correlated too lowly and the metrics measured different underlying constructs as the other metrics. For the recovery phase, variables were neither correlated highly nor lowly. This implied that the metrics contributed uniquely. Overall, the information based on the results from the metrics study is useful for various risk assessors and decision makers. For example, the weights of the metrics can be applied to different process safety, risk assessment, and resilience studies for enhanced decision-making. Using these weights and not using equal weights for these metrics would accomplish this. The results of this study also indicate potential improvement for further research areas such as extending the survey to determine the most appropriate phase of the metric, additional analysis to test the level of significance of some of the metrics based on all three phases, find the relative level of significance of three phases, significance of social metrics in risk and resilience assessment, and establish correlations by using actual data.

Furthermore, a matrix-based approach was developed for the quantification of social aspects for the process industry and was demonstrated for the reactor charging procedure.

CHAPTER IV

QUALITATIVE ASSESSMENT: RESILIENCE BASED INTEGRATED PROCESS SYSTEM HAZARD ANALYSIS (RIPSHA)*

Essential initial steps in process safety and risk management of any facility are hazard identification and hazard analysis. A large volume of work can be found in the literature on different hazard identification and analysis techniques and advanced methodologies, as summarized in section 4.1.^{201, 202}. However, these methods have been considered inadequate in identifying and analyzing the hazards involved in most incidents^{5, 203}. This is because these techniques require competence to overcome incompleteness in identifying potential technical causes and ignored the contribution of human, procedures or organizational elements that affected the analysis results^{19, 204, 205}. Traditional methods for process hazard analysis focus primarily on process hazards and ignore the social aspects, such as management policies on resource allocation, spare parts deficiency/availability, training of operators and more. Most traditional methods use a linear approach and a single cause-consequence pair³⁷. These methods are not complete and lack a comprehensive assessment approach for the system. According to Zhao et al., humans work with technology, social structures, and environment, which can be designated complex systems.

*Reproduced in part with permission from Jain, P., Rogers, W. J., Pasman, H. J., Keim, K. K., & Mannan, M. S., "A Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA) approach: Part I plant system layer," *Process Safety and Environmental Protection*, Vol 116, Pages 92-105. Copyright 2018 Institution of Chemical Engineers. Published by Elsevier B.V.

Reproduced in part with permission from Jain, P., Rogers, W. J., Pasman, H. J., & Mannan, M. S., "A resilience-based integrated process systems hazard analysis (RIPSHA) approach: Part II management system layer," *Process Safety and Environmental Protection*, Vol 118, Pages 115-124. Copyright 2018 Institution of Chemical Engineers. Published by Elsevier B.V.

In case of an accident system interdependencies must be addressed, and to prevent such accidents, the complete sociotechnical system must be evaluated²⁰⁶. Therefore, a socio-technical systems perspective covering proper and adequate hazard identification including both technical and social factors is paramount in development of preventive measures for catastrophic incidents. The socio-technical systems theory has been developed and explored by numerous researchers in the past^{207, 208, 209, 25}. A socio-technical system is characterized as a complex organization with interaction among its elements of human and technology/equipment.

In this research, a systems-based approach is further developed by including resilience engineering aspects. This results in creation of a holistic view of the hazard identification and analysis process called Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA). This approach is applicable to different modes and subsystems of the process system. A bi-layered system approach is described covering the process system resilience aspects, multi-modes, and detailed methodology. This chapter provides the guidewords based on the sub-systems (plant system layer - human, procedures, and process equipment; management system layer – process safety culture and leadership, process safety systems, and operational discipline) and associated worksheets. Using the examples of liquefied natural gas (LNG) process system and a tank explosion, detailed analysis is demonstrated.

4.1. Overview of existing hazards identification and analysis techniques

There are a number of hazard evaluation techniques used by the process industry as a systematic method to identify influences or causes that may result in incidents or process upsets. ²¹⁰ presented a review of the eight most commonly used hazard analysis techniques. These included checklists, what-if analysis, safety reviews, preliminary hazard analysis, failure mode and effect analysis (FMEA), fault tree analysis ¹¹³, event tree analysis (ETA), and hazard and operability study (HAZOP).

It was found that earlier researchers focused mainly on the conventional methods of hazard analysis^{211, 212, 213}. Later, researchers extended the work to include new types of deviations, automating the methods, or exploring the development of expert systems^{214, 215, 216, 217, 218}. Considering batch processes as more critical, some authors focused their work in this area to identify and analyze hazards by developing advanced methods^{219, 220, 221, 222, 194}. Also, researchers established hybrid approaches by combining HAZOP with dynamic simulation²²³. Furthermore, a comprehensive function based, systems framework approach called Blendid HAZID including system components as plant components, procedural aspects, and people was introduced^{224, 225, 226}. A summary of selected hazard identification and analysis methods is presented in Table IV.1 highlighting system/human/process based approach.

Summarizing, it can be concluded that a considerable amount of work has been conducted through exploring and applying various methods. Some examples of these methods are knowledge bases, combined with process models, such as Petri nets, signed digraphs, and dynamic simulation, with focus on improving and semi-automating hazard identification. Nevertheless more research focused on systems thinking is needed for more

comprehensive hazard identification and loss prevention control. Of the various methodologies to identify and analyze hazards, particular consideration has been given to HAZOP. The HAZOP methodology is relatively convenient to implement and has been used by the risk assessors in process industry for very long time²⁴¹.

Table IV.1: Hazid and Analysis Methods

S.no.	Year	Author/Organization/ Institution	Hazard identification and analysis method	System (S) or Process (P) or Human (H)
1	1974	Lawley	Operability Studies And Hazard Analysis ²¹³	P
2	1995	Vaidhyanathan and Venkatasubramanian	HAZOP Digraph (HDG) Model ²²⁷	P
3	1997	Liu and Chiou	The use of Petri Nets for failure analysis ²²⁸	P
4	1997	Jens Rasmussen	Accimap ²⁵	S
5	1998	Kennedy and Kirwan	SCHAZOP—safety culture hazards and operability study ²²⁹	S
6	1999	Redmill <i>et al.</i>	System Safety: HAZOP and Software HAZOP ²³⁰	S
7	2002	Baybutt	LOPA-HF—an application of LOPA for human failure analysis ²³¹	H
8	2003	Baybutt	Major Hazards Analysis (MHA) ²³²	P
9	2006	Leveson <i>et al.</i>	Resilience Engineering ²³³	S
10	2007	Kariuki and Lowe	Integrating human factors into process hazard analysis ²³⁴	S
11	2007	Scott Jackson	System resilience ²³⁵	S
12	2009	Seligmann <i>et al.</i>	Blended HAZID ²³⁶	S
13	2009	Leveson <i>et al.</i>	STAMP or Systems- Theoretic Accident Modeling and Processes ²³⁷	S
14	2013	Paltrinieri <i>et al.</i>	DyPASI tool ¹³⁷	P
15	2013	Khakzad <i>et al.</i>	Dynamic safety analysis by mapping bowtie into Bayesian network ²³⁸	S
16	2015	CA Ericson	System safety hazard analysis techniques ²³⁹	S
17	2017	Xin <i>et al.</i>	Dynamic hazard identification using Bayesian network ²⁴⁰	S

4.2. Overview of existing evaluation studies for the management layer

There are a few studies that cover the analysis of a management layer in hazard identification. Table IV.2 presents a brief summary of works on evaluation studies for the management layer.

Table IV.2: Works on evaluation studies for the management layer

Authors	Major contributions
242	The Management Oversight and Risk Tree ⁶⁵ technique uses a predefined qualitative fault-tree approach to show the possibly failing inter-relationship of management systems with safety.
25-26	Accimap accident investigation method based on socio-technical system includes six organizational levels and has the ability to link factors both within and across these levels.
229	SCHAZOP—safety culture hazards and operability study.
243	System-theoretic process analysis (STPA) by probing for failure all control loops in the system.
91	Comparison of application areas, methodology and relationships for 3 approaches - accident investigations (AI), risk analysis (RA), and safety management systems (SMS).
20	Blended hazard identification (BLHAZID) methodology blends and automates two different types of HAZID methods: the function-driven and component-driven approaches.
137	DyPASI reduces deficiencies of the current HAZID techniques by querying accident data bases and building a bowtie.
244	Strategies Analysis for Enhancing Resilience (SAfER) based on a task analysis and a decision ladder.
245, 246	Using FRAM to model complex socio-technical systems, defining functions, analyzing the structure while portraying the functional links between human and equipment and guiding to performance variability parameters.
240	Dynamic hazard identification using Bayesian network.

Some details and limitations of the most common methods such as Accimap, System-theoretic process analysis (STPA), Blended Hazid (BLHAZID), and Dynamic Procedure for Atypical Scenarios Identification (DyPASI) are summarized below.

4.2.1. Accimap

²⁵⁻²⁶introduced the concept of the socio-technical system (STS) existing since the 1950s, to investigate and describe accident causation. An STS consists of six organizational levels: government policy and budgeting; regulatory bodies and associations; local area government planning and budgeting; technical and operational management; physical processes and actor activities, and equipment and environment. Causes are considered failing factors, components, and connections across the overall system, including higher governmental and regulatory levels. The diagrams show the cause-consequence links.

4.2.2. System-theoretic process analysis (STPA)

Leveson et al. applied the socio-technical system concept too and considered the function of each level as a control^{73, 243}. For an STS, safety is an emerging outcome and the layers can be depicted as control loops consisting of process, sensor, processor, and actuator. Each loop can be queried for presence, correctness, and timely activation of control action. It is claimed that completeness of scenario identification is obtained. The result of an analysis is shown as a causal flow diagram. Due to the current lack of supporting software the effort of an analysis on all layers is relatively large.

4.2.3. Blended Hazid (BLHAZID)

²⁰developed on the basis of the Functional Systems Framework approach a highly digitized hazard identification and scenario definition method. The method blends two different types of HAZID methods: the function-driven HAZOP and component-driven FMEA. The scenarios describe triplets of cause, process deviation, and implication. Failure

can be in the plant, people, and procedures. The scenarios are stored in a compact fashion and due to the digitization, IT support is high.

4.2.4. Dynamic Procedure for Atypical Scenarios Identification (DyPASI)

¹³⁷ developed a method that mitigates deficiencies of the current HAZID techniques by querying accident databases applying a similarity algorithm, and so identifying atypical scenarios. Scenarios are presented in a bowtie form, also enabling seeing the location of preventative and protective safeguards in the causation trees. For human and organizational factors DyPASI is dependent on the representation of these factors in accident descriptions.

4.3. Systems hazard analysis vs process hazard analysis

Process Hazard Analysis (PHA) is a methodical identification, assessment, and documentation of potential process hazards and incident scenarios related to a process plant. It is the most common and easy to implement method used by process industry. It can be performed by using various techniques, such as HAZOP, What-if analysis, safety review, and more.

It has been documented that numerous incidents in the process industry including the chemical, petrochemical, and offshore oil and gas platforms occurred as a result of multiple causes or interdependent failures. The incidents occurred because of breakdown of various system components, such as organizational behavior, human errors, or procedural elements^{247, 234, 229, 248, 25}. Hence, it is critical to understand and analyze the human, procedures, and other social factors along with the technical factors like process parameters. It has been observed that PHA has a significant limitation where it lacks social and organization factors associated with the operations in a single approach²⁴⁹.

Various research works have been carried out in field of system safety. The concept of safety culture and its relation to the system property has been explained²⁵⁰. Researchers have proposed different accident models demonstrating the influence of human, organizational, and managerial factors^{73, 251, 252}. Furthermore, aspects such as design, risk analysis informed anticipation, early detection, learning from incidents, and emergency response time are critical to prevent catastrophic incidents. Previous research has demonstrated the importance of these aspects^{253, 254}.

The highly complicated and hazardous launching and landing operations at U.S. Navy aircraft carriers emphasize on tracking and monitoring small failures, less oversimplification, sensitivity towards operations, ensuring resilience capabilities (such as adaptive, absorptive, restorative *etc.*) and taking benefit of shifting locations of expertise. Inspired by the smoothness of U.S. Navy aircraft carrier operations several researchers have proposed the High Reliability Organization²⁵⁵ concept. Weick & Sutcliffe, 2011 described the concept in extension and explained the Principle of “Preoccupation with Failure”, which focuses on several small errors that conditionally can lead to a bigger disaster. Hence, by reducing smaller errors a catastrophic incident could be prevented³³.

As defined by Stephans, “System safety analysis is the formal analysis of a system and interrelationships among its various parts (including plant and hardware, policies and procedures, and personnel) to determine real and potential hazards within the system and suggest ways to reduce and control those hazards”²⁵⁶. Unlike PHA, systems hazard analysis (SHA) focuses on the complex combinations of subcomponents acting together. Macro-ergonomics is one of the proposed top-down approaches for systems hazard analysis of a socio-technical system^{208, 257}.

4.4. RIPSHA: Resilience-based Integrated Process Systems Hazard Analysis

The majority of the largest incidents in the process industry are a result of human, organizational, management, mechanical, and operational failures^{258, 259}. The process industry can benefit from learning from other industrial sectors such as transportation, nuclear, shipping, and aviation^{260, 261}. Current methods for hazard identification and analysis have focused on process hazards and researchers have explored isolated methods for human error analysis. Further, most methods lack the anticipation element and also the full anatomy of incident – initiation, propagation, and termination. The key methods used today in the industry follow a univariate analysis and are limited in their approach to consider multiple factors, complex interactions among system components and their relationships²⁵⁹. The hazard analysis method for a complex socio-technical system such as a process plant should have the following characteristics: consideration of all system components (processes, human operations, equipment, instruments, control systems, *etc.*), all plausible deviations, a multi-disciplinary team, and proper documentation. Further, the concept of resilience engineering has been identified as one of the vital aspects in process safety⁸⁵. RIPSHA is a novel hazards analysis approach based on resilience engineering concepts that incorporates both technical and social factors within a single analysis method. It has been found that HAZOP is the most widely used PHA method. Therefore, HAZOP is selected as the base methodology for RIPSHA but enhanced with resilience thinking. This means that the resilience concept, in its totality, should leave fewer overlooked deficiencies and make up for ones still remaining. The RIPSHA methodology for hazard analysis includes the following features: applicable to the life cycle of the

process system, dynamic in nature, emphasis on social factors, such as organizational behavior and management system.

Several authors have developed methods based on monitoring and analysis of trends or variations in parameters^{262, 263, 264}. However, these parameters have been primarily limited to the process. The RIPS HA methodology is based on parameters and guidewords developed based on resilience metrics from four aspects. This approach follows the well-established HAZOP technique and covers technical as well as social aspects of the process system. Therefore, as we shall see the RIPS HA methodology provides the following benefits:

- Analyzes both internal and external disruptions
- Considers static and dynamic states covering design and various operational modes

4.5. Bi-layered system approach

The system approach refers to both the vertical and the horizontal layers. The vertical layers comprise of sub-layers such as Engineering, Safety & Security, Procurement, Construction, and Contracting activity that form the Management System Layer. The horizontal layers consist of an operational plant/facility including components such as process equipment, operators (people/human) and procedures. The RIPS HA methodology proposes a bi-layered approach that takes into account the two distinct layers, as shown in Figure IV.1. RIPS HA consists of two types of analysis – management system layer and plant system layer. There are two major inputs that come from safeguards and resilience metrics assessment, which are shown by dashed arrows. This analysis will have two deliverables – RIPS HA worksheet, and report.

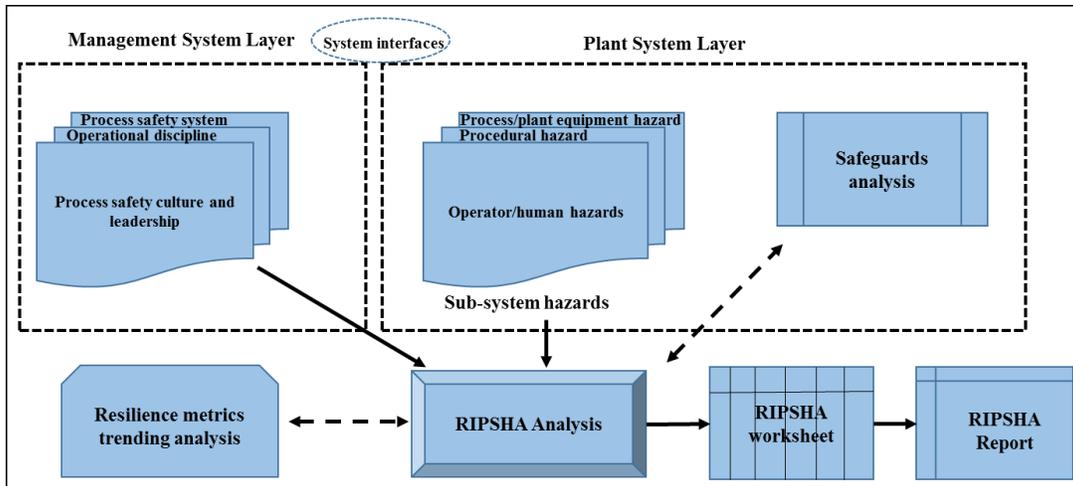


Figure IV.1: RIPS HA: bi-layered approach

4.5.1. Management system hazard analysis

This is the first layer called the management system, and it can be further broken down into three rational sub-systems for analysis: process safety culture and leadership; operational discipline, and process safety systems. It has been observed that deficiencies in these sub-systems lead to weaknesses of the whole system potentially causing disastrous consequences such as BP Texas City refinery²⁵⁵, William Olefins explosion²⁶⁵, and the Esso Longford gas explosion^{266, 267}. An important or critical example of a hazard due to organizational factors is lack of trade-off analysis between production and safety given business priorities and pressures. This hazard can result in reduced vigilance to maintain barriers and a degradation of organizational resilience.

Effectiveness of a management system has to be measured applying indicators.²⁶⁸ described the benefits of resilience metrics to achieve progress towards being more resilient and stressed the need for leading indicators for resilience as opposed to lagging ones. Metrics can further help to link organizational resilience with high competitiveness

and will contribute to demonstrate a business case for resilience investments. More specifically, Øien et al., 2010 proposed indicators for organizational resilience¹⁸⁰. A Management system layer is the first layer in the RIPSHA approach. It consists of three rational sub-systems for analysis - process safety culture and leadership; operational discipline, and process safety systems.

Process safety culture and leadership

Investigation studies of some of the catastrophic incidents such as Piper Alpha disaster, Longford gas plant explosion and more have identified common process safety culture weaknesses. Hence, building, maintaining, and nurturing a strong process safety culture and leadership has been identified as critical to consistent and satisfactory process safety performance. Within the 20 elements of RBPS by CCPS, Process Safety Culture is listed as the first element under Commit to Process Safety²⁶⁹. ²⁷⁰presents an idealistic framework for Best-in-Class process safety management for high reliability organizations. The framework consists of ten attributes to evaluate the safety performance of organizations – leadership; culture and values; goals; policies and initiatives; organization and structure; employee engagement and behaviors; resource allocation and performance management; systems, standards and processes; metrics and reporting; continually learning organization; and verification and audit. Four characteristics of a good safety culture are suggested as commitment, communication, resilience and flexibility, vigilance²⁷¹. Researchers have conducted several safety culture assessments and evaluation studies²⁷², ²⁷³, ²⁷⁴. Strong leadership along with good process safety culture is essential to provide consistent support for process safety programs and confirm the commitment from all levels of management. In summary, without a way to assess process safety culture and

leadership, an organization will have no meaningful basis for making and measuring improvements. Table IV.3 lists the guidewords for process safety culture and leadership sub-system based on resilience aspects and metrics.

Table IV.3: Process safety culture and leadership: suggested guidewords

Process safety culture and leadership: suggested guidewords			
Resilience aspect	Resilience metric	Parameter	Guideword
Early Detection	ED ₅ , ED ₆ , ED ₇	Indicators analysis and actions	Missing
			Inadequate
Plasticity	P ₁ , P ₂	Safety studies	Untimely
			Ineffective
Plasticity	P ₁₂	Communication	Skipped
			Ineffective
Plasticity	P ₂	Communication of recommendations to management	Missing
			Inadequate
Plasticity	P ₁ , P ₂	Identification of external signals such as flood, security threats	Missing
			Inadequate
Plasticity	P	Benchmarking	Missing
		Data collection	
		Involvement/Awareness/Participation	More
			Less
		Safety training/coaching/retraining	Missing
			Inadequate
	Skipped		
	Inadequate		
Plasticity	P	Management commitment	Missing
Plasticity	P	Safety promotion strategies	Unavailable
			Inadequate
			More
			Less
Plasticity	P ₇	Resource allocation	Inadequate
Recoverability	R ₁ , R ₂	Emergency Response Plans	Missing
			Unavailable
			Ineffective
Early Detection	ED	Metrics and Reporting	Missing
			Inadequate

Operational discipline

Many researchers both from academia and industry have addressed the aspect of operational discipline. DuPont has defined Operational Discipline (OD) as “the deeply rooted dedication and commitment by every member of an organization to carry out each task the right way every time”²⁷⁵. Another definition of OD is “the performance of all tasks correctly every time.” According to ²⁷⁶, both organization and individuals contribute to an effective OD program. Some of the attributes of an effective OD program mentioned in literature are - equipment is properly designed, operated, and maintained, management systems are properly executed, and errors and deviations are consistently addressed.²⁷⁷ model of OD cover three elements – management discipline, operational discipline, and engineering discipline.²⁷⁸ defines risk is an inverse function of an OD program. Also, it has been stated that the effectiveness of Process safety and risk management systems is dependent on the company’s implementation and support for operational discipline (OD)-related programs. These OD programs depend on data collected from the operations from various sources such as plant historian, audit reports *etc.* to get insights about the operating metrics and explore the opportunities for improvement in safety¹⁶⁴. Some of the tragic events that highlighted failures in the operational discipline are BP Texas City, Seveso disaster, Gulf of Mexico *etc.* It is therefore critical to identify hazards based on OD to recognize, monitor, track, and learn from near misses. Table IV.4 provides the guidewords for operational discipline sub-system based on resilience aspects and metrics.

Table IV.4: Operational discipline: suggested guidewords

Operational discipline: suggested guidewords			
Resilience aspect	Resilience metric	Parameter	Guideword
Recoverability	R ₂	Resources, proper plans	Unavailable
			Inadequate
			Missing
Plasticity	P ₇	Inventory	Less
			Inadequate
Plasticity	P ₃	Training	Missing
Plasticity, Early Detection	P ₁₀ , ED ₃	Maintenance	More
			Less
			Inadequate
Plasticity, Early Detection, Error Tolerant Design	P, ED, ETD	Observations tracking and trending	Missing
			Unavailable
Plasticity	P ₁₂	Observations communication	Missing
			Unavailable
			Untimely
Error Tolerant Design	ETD	Deviations	Ignore
Plasticity	P ₉	Worker fatigue	More
Error Tolerant Design	ETD ₂	Safe operating limits	Missing
			Unavailable
Plasticity	P ₁	Hazard evaluation	Skipped
			Inadequate
Error Tolerant Design, Plasticity	ETD ₃ , P ₈	Management of Change	Unavailable
			Missing

Process safety systems

Many researchers have identified the social or management barriers. For example, ²⁷⁹ has classified barriers as physical, procedural or administrative, or human action. ²⁸⁰ have classified barriers as technical, human, or human/organizational. ²⁵² classifies barrier systems as physical, technical, or human factors-organizational systems. ²⁸¹ also distinguishes between the physical and management barriers. This indicates the

significance of social aspects of barriers or process safety systems in hazard identification and analysis and also overall risk assessment. Also, in literature, several features have been identified that characterize safety systems or barriers. Some of the features recorded by ²⁸² are - functionality/effectiveness, reliability/availability, response time, robustness, and triggering event or condition. ²⁸³ summarized the following criteria as aspects for barrier quality – efficiency/adequacy, resources required, robustness (reliability), delay in implementation, and applicability to safety-critical tasks, availability, evaluation, and dependence of humans. These characteristics of safety systems are critical for identification of hazards and their analysis. Furthermore, an effective process safety system such as a good alarm management program helps process operations closer to the optimal levels and hence lead to safer operations¹⁶⁵.

Table IV.5: Process safety systems: suggested guidewords

Process safety systems: suggested guidewords			
Resilience aspect	Resilience metric	Parameter	Guideword
Error Tolerant Design	ETD ₁₋₁	Activations	More Less
Error Tolerant Design	ETD ₁₋₂	Activations	More Less
Early Detection	ED ₄	Vibrations, corrosion, leaks	More Less
Plasticity	P ₆ , P ₇	Safety critical equipment/barrier	Inadequate
			Unavailable
			Reliable
		Robustness	More
			Less
		Inspection	Non-routine
Routine			
Safety barrier design	Limited		
	Inadequate		

Table IV.5 provides the suggested guidewords for process safety systems sub-system that are developed based on technical and social resilience metrics.

4.5.2. Plant system hazard analysis

This is the second layer called the plant system and is further broken down into the three rational sub-systems for analysis (human/people, procedures, and plant equipment). This layer supports capture of deviations arising from each of the sub-systems and also their interactions.

Human

Humans or the operators in the plant form an important sub-system as they recognize actions to be taken based on standard operating procedures and information from the control systems panel.²⁸⁴ raised concern related to the minimal use of human error analysis in the petroleum, petrochemical, and chemical industries. An error analysis method was proposed to identify error causes, which are helpful in defining preventive measures incorporating human reliability techniques into the design. Human error is considered to be responsible, directly or indirectly, for 50-90% of the operational risk^{201, 231}.

Procedures

Standard operating and maintenance procedures play a crucial role in process safety²⁸⁵. These provide information for operators to perform various tasks sequentially in complex plant settings. Researchers have mentioned that hazards analysis application to procedures would help predict potential deviations, failures in procedures, and human errors that could help prevent catastrophic incidents²⁴⁸.

Process/Plant equipment

Process hazards have been well-covered by the traditional HAZOP guidewords. Regarding plant equipment based on the RIPSHA approach, as attributes of a socio-technical system, reliability, availability, and maintainability of plant equipment is essential for high organizational resilience, but each is highly influenced, both directly and indirectly, by organizational factors. Design decisions involving these attributes greatly affect system life-cycle costs (direct and indirect) including costs of components, costs of failure events, and costs of maintenance. The true probability of failure on demand of a system component, which is of paramount importance for reliance on safeguards and which is not currently recognized by the majority of industry, is composed of three contributions due to 1) random failure of a component, 2) failure due to component offline for testing, maintenance or replacement, and 3) excessive supply and administrative delays that increase MTTR (mean time to repair) due to organizational factors. Unavailability on Demand, QOD, where Q is unavailability (complement of availability) is more realistic than probability of failure on demand, PFD, in capturing the overall failure uncertainty and component failure probability due to the sum of:

- Component random failure, PFD, for failure rate \sim constant, λ (Exponential behavior), or time dependent, $\lambda(t)$, (Weibull distribution, for a shape parameter $\beta = 1$, Weibull is Exponential, $\lambda(t) = \lambda$),
- Component test and maintenance, MTTR, for renewal or minimal repair,
- Organizational delays and supply delays: SAD is excessive supply and administration delays, which for an organization with resilient leadership, $SAD \sim 0$, for reduced uncertainty of MTTR within an acceptable range.

It is significant to note that organizational factors and associated hazards, enter both directly with SAD and indirectly with quality of training/retraining for testing and maintenance, quality and time of testing and maintenance, quality and time of maintenance and replacement.

Furthermore, an important point to note is that unavailability failure probability on demand, QOD, is a component resilience expression. This is because following conversion of MTTR time and SAD time to probabilities (divide by mission time), it is composed of the three parts of the overall probability of component failure on demand. It further includes restoration of a component that has been tested, maintained, or replaced following failure or detection of failure. On a point value basis, Q, unavailability, is a failure probability composed of the sum of three failure probabilities: PFD, MTTR/T, and SAD/T, where T is the mission time. Tables IV.6 and IV.7 list the selected guidewords for operator/human and the procedures sub-systems based on resilience aspects and metrics.

Table IV.6: Operator/human: suggested guidewords

Operator/Human: suggested guidewords			
Resilience aspect	Resilience metric	Parameter	Guideword
Plasticity	P ₉	Operator	Missing
Plasticity	P ₉	Action	Missing
			Mistimed
			Wrong
Plasticity	P ₄	Procedure	Mistimed
Plasticity	P ₃	Training	Missing
Plasticity	P ₉	Supervision	Ineffective
Early Detection	ED ₁	Alarm	Skipped
Plasticity	P ₁₁	Detail	More
			Less
			Other than
Plasticity	P ₁₁	Communication	Shift changeover, Who should know (verbal/written)

Table IV.7: Procedure: suggested guidewords

Resilience aspect	Resilience metric	Operations	Parameter	Guideword
Plasticity Error Tolerant Design	P ₅ ETD ₃	Permit to work	Isolation (covering adequacy, type and location of isolations)	None
				Inadequate
				Wrong
			Tagging (valves, electrical, fire and gas, panels, utility systems)	None
				Inadequate
			Safety Equipment (extinguishers, fire blankets, cover drains, safety watch)	Not specified
				Inadequate for location
			Special Instructions (list of blinds, tag list, ESD locations)	None
				Inadequate
			Maintenance Procedures	Not made available
				Inadequate
Plasticity	P ₄	Maintenanc e preparation	Process isolation	Inadequate
				Wrong location
				Wrong type
			Electrical isolation	Inadequate
				Location
			Mechanical isolation	Inadequate
				Wrong type
				Not to line/equipment specification
				Wrong location
			Instrument	Wrong location
				No back-up
				Interlock (trip) disconnected
			Depressurizing	Wrong location
				Too rapid
				Inappropriate
				None
			Gas testing	Inadequate
				Wrong location
			Purging	None
				Inadequate
				Wrong location
				Wrong medium
				Inadequate
				Shift changeover

Table IV.7 Continued

Resilience aspect	Resilience metric	Operations	Parameter	Guideword
Plasticity	P ₄	Maintenance	Maintenance Procedures	Unavailable to crew
				Inadequate
Early Detection	ED ₃		Inspections	None
				Incomplete
Recoverability	R ₁		Special Instructions (list of blinds, tag list, ESD locations, specific emergency instructions)	Process emergency
Plasticity	P ₁₁		Communication	Who should know (verbal/written)?
				Shift changeover
Plasticity	P ₇		Spares	Crew changeover
		Wrong Specification		
Plasticity	P ₈	Reassembly (misalignment, wrong installation, temporary blinds not removed)	Incorrect	
Recoverability	R ₂	Mock drills	Availability of critical spare components	Missing Inadequate
Plasticity	P ₈	Handback and restart	Isolation (relief valve, blowdown, temporary blind)	Not checked
			Tags	Not removed
			Logic (trips)	Not restored
			Pressure testing	None
				Inadequate
			Electrical connection	Wrong
				Premature
Housekeeping (blocked drains, foreign objects, work area)	Wrong			
	None			
			Inadequate	

4.6. Multi-mode approach

The RIPSHA approach is developed such that it can be applied to various modes in a process system. These modes are design, normal operations, simultaneous operations and transient operations.

Design: Traditional HAZOPs are primarily conducted on the design and its verification in *e.g.*, the commissioning stage. Hence, there is no doubt it is paramount for safety. However, human and procedural elements and in rare cases also the technical elements are often missed during the conventional methods. There has been consideration given to this aspect^{286, 287}. Hence, RIPSHA includes this as one of its modes for analysis.

Normal operations: This mode is the one that has been studied or analyzed well over the years. The RIPSHA approach would follow the conventional HAZOP process for this mode.

Simultaneous operations: These operations can be defined as two or more activities that by interaction may impact their safety or the performance of emergency response and planning procedures and are executed by different functional groups in the same location at the same time^{288, 289}. In process units, specific activities such as construction, commissioning, start-up, and process operations require particular attention to look for additional hazards that may be created during execution of such operations. A study to review incidents world-wide concluded that even though hazards were known, operational inadequacies resulted in incidents²⁹⁰. Hence, this area of simultaneous operations has been found as an improvement area for PHAs²⁹¹.

Transient operations: A process plant in its life cycle will experience other modes of operation besides its continuous or batch process operation. Changing from one mode to

another is called transition. Start-up, shutdown, catalyst changing and regeneration are common examples of transient operations^{292, 241, 293}. It has been found in the literature that these operations are relatively rare but involve high human intervention²⁹². A large number of incidents have been reported to occur during transition operations^{294, 293, 292}. However, less attention has been paid to these operations. Therefore, it is critical to consider such operations in the RIPS HA methodology.

4.7. Methodology

The RIPS HA methodology has the following steps as part of the hazard identification and analysis:

Step1: Team formation

The RIPS HA team composition and experience requirements are similar to those for a traditional HAZOP with the following additional requirements or exceptions or features for design, simultaneous operations and transient operations modes:

Design: design engineer who designs the function of the system; engineer who designs the human-machine interface HMI; human factor engineer who determines the procedural elements, and an experienced representative from the operators group of a similar plant.

Simultaneous operations: project manager, discipline specialists from construction and/or commissioning, contractors, subcontractors, and vendors who can provide the detailed schedule so that the team can identify relevant hazards and verify the adequacy of additional control measures²⁸⁸.

Transient operations: an experienced operations representative with a sound knowledge of transient operations, their critical nature, field operations, and controls

through HMI; and a process design and technology expert with specific knowledge of the equipment and the process under review²⁹².

Step 2: Charter preparation

The RIPS HA leadership team must prepare and issue a charter to define the responsibilities, tasks, and objectives of the team. It should also include the unit/operation selection, process boundaries, and any special objectives.

Step 3: Data and documents collection

The RIPS HA team should collect the information (preferably electronic versions) as described for conventional HAZOP studies²⁹⁵. Additionally, effort should be made to gather relevant information such as operating and maintenance procedures, standard operating conditions (safe operating limits), management of change documents (since prior PHA), learning from incident and near miss reports - from other similar processes within the company or industry (since prior PHA), resilience metrics information, and prior RIPS HAs (within the same boundaries).

The RIPS HA team should review the documents and information for the system to be studied and ensure that it is sufficiently accurate for conducting the analysis. Any minor errors should be corrected. If there are serious deficiencies, the RIPS HA team must stop work, report the problem to the RIPS HA team leadership, and request that the information be updated. The RIPS HA team, if during the course of conducting the analysis, determines any inconsistency with the plant's designation of safety critical components; equipment or procedures, must document that finding as a recommendation.

Step 4: Sub-systems procedural review

The sub-systems procedural review should be carried out in a similar way as with a regular HAZOP. The sample RIPSHA worksheets for management and plant system layers are shown in Tables IV.8 and IV.9. This worksheet has been created similar to the conventional HAZOP worksheet, and there are two major differences. First, the RIPSHA worksheet has a section called 'Mode'. The 'Mode' section would help capture the four different modes - design, normal operations, simultaneous operations, and transient operations described in Section 4.6. Second, this worksheet has sections for three sub-systems of human, procedures, and plant equipment or three sub-systems of process safety culture and leadership, operational discipline, and process safety systems depending on the analysis layers. This is to ensure that scenarios are not missed. The input from resilience metrics is based on the plant performance under study, and this input provides information for safeguard assessment and results in more informed and accurate decision making. The credit for safeguard can be taken in the assessment based on the resilience metrics trending analysis. Guidewords or process/plant equipment are not presented here as these are similar to the conventional HAZOP.

Table IV.8: RIPS HA Worksheet: Plant system layer

Project/Plant:		Rev. no:					Date:					Page: of		
Team members:														
System description:														
Mode:														
Node (P&ID):														
<i>Subsystem: Process/Plant equipment</i>						Subsystem intention								
					Risk without any safeguards			Risk with safeguards						
Parameter	Guideword	Deviation	Cause	Consequence	Severity (S)	Likelihood (L)	Risk (R)	Safeguards	S	L	R	Recommendations	Responsible entity	
<i>Subsystem: Operator/human</i>						Subsystem intention								
					Risk without any safeguards			Risk with safeguards						
Parameter	Guideword	Deviation	Cause	Consequence	Severity (S)	Likelihood (L)	Risk (R)	Safeguards	S	L	R	Recommendations	Responsible entity	
<i>Subsystem: Procedure</i>						Subsystem intention								
					Risk without any safeguards			Risk with safeguards						
Parameter	Guideword	Deviation	Cause	Consequence	Severity (S)	Likelihood (L)	Risk (R)	Safeguards	S	L	R	Recommendations	Responsible entity	

Table IV.9: RIPS HA Worksheet: Management system layer

Project/Plant:			Rev. no:			Date:						Page: of			
Team members:															
System description:															
Mode:															
Node (P&ID):															
<i>Subsystem: Process safety culture and leadership</i>															
						Subsystem intention									
					Risk without any safeguards				Risk with safeguards						
Parameter	Guideword	Deviation	Cause	Consequences	Severity (S)	Likelihood (L)	Risk (R)	Safeguards	S	L	R	Recommendations	Remarks	Responsible entity	
<i>Subsystem: Operational discipline</i>															
						Subsystem intention									
					Risk without any safeguards				Risk with safeguards						
Parameter	Guideword	Deviation	Cause	Consequences	Severity (S)	Likelihood (L)	Risk (R)	Safeguards	S	L	R	Recommendations	Remarks	Responsible entity	
<i>Subsystem: Process safety systems</i>															
						Subsystem intention									
					Risk without any safeguards				Risk with safeguards						
Parameter	Guideword	Deviation	Cause	Consequences	Severity (S)	Likelihood (L)	Risk (R)	Safeguards	S	L	R	Recommendations	Remarks	Responsible entity	

Step 5: Documentation of findings

While documenting the findings, the RIPSHA team should address or reference the specific findings in the hazard analysis worksheet and use precise wording. The accountability for each finding or recommendation should be assigned to an individual.

Step 6: Recommendations

After hazard analysis, following key points should be followed while making recommendations:

- recommendations must be made to provide additional safeguards where appropriate,
- clear connection with the process/human/procedure hazard,
- related to degree of risk
- consider the integrity and adequacy of safeguards such as degree of independence, dependability, resilience, auditability

The RIPSHA team should ensure that the findings, including the actions taken, are communicated to all employees whose work assignments are in the facility/system or who are affected by the recommendations or actions including any workers responsible for procedure or task execution where the risk moves to the unacceptable region if failure of that procedure or task occurs. Also, the results should be communicated to the emergency response (ER) team so that the ER team has the information needed to develop effective responses.

Step 7: Closure of recommendations and corrective actions

The management should review the recommendations from the RIPSHA study. The response from management must be documented to each recommendation, either accepting as is, accepting as modified, or rejecting. A completion date should be assigned to each accepted/modified recommendation. An electronic system should be followed to track the recommendations. Management system hazard analysis will be used to ensure corrective actions are taken and recommendations are closed timely.

4.8. Management system hazard analysis example: Tank Explosion

An example of a tank explosion incident that happened during an operation trying to remove a plug with a compressed air flow, is selected as the case study as illustrated in Figure IV.2. This incident resulted in blowing off of one end of a horizontal cylindrical tank due to the physical explosion and led to two fatalities. The major cause identified for this incident was the formation of a solid plug in the vent of this tank due to faults in steam tracing or insulation. The tank stored a liquid product at 100°C melting point, kept hot by a steam (7 bar) coil²⁹⁶.

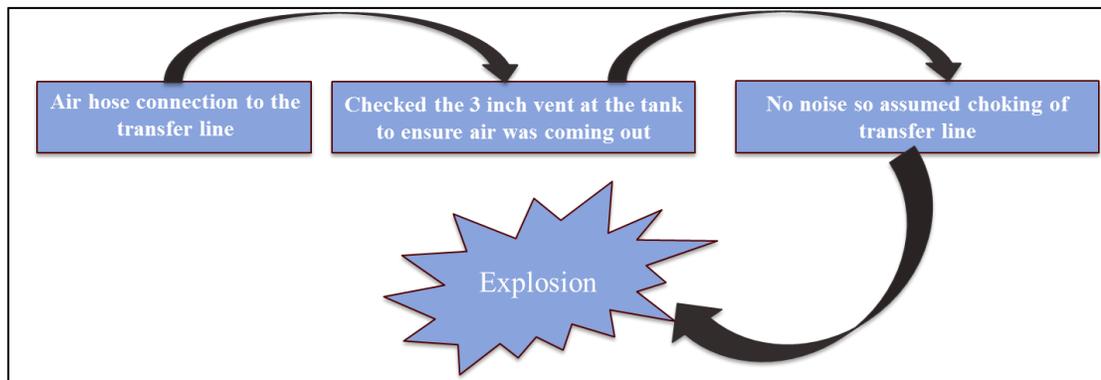


Figure IV.2: Tank explosion accident timeline

Based on the RIPS HA methodology²⁹⁷, a team is formed of members with knowledge about the tank operations. The charter is prepared to define the scope of the study within the operations for this example. Information for each hazardous substance, in this case the chemical, stored and handled, is collected. The information is expected to include similar information required under 29 CFR 1910.119(d)²⁹⁸, such as physical and chemical properties, combustibility, flammability, and explosiveness, toxicity, reactivity, and corrosiveness^{299, 300}. In addition, the vessels and piping containing these materials and associated process conditions are identified on drawings, such as process flow diagrams, piping and instrumentation diagrams, and plot plans. Furthermore, any near-miss or incidents reports and information from metrics that relate to management system layer are gathered.

The authors believe that the RIPS HA approach would have identified some of the hazardous situations developed in this scenario that led to the tank explosion and instigated measures that would have avoided it. For example, the primary cause of this incident was identified as the plugged vent due to not following the management of change process. Another factor was lack of communication concerning previous incidents to identify and be aware of such a scenario. Furthermore, there was lack of resource allocation in terms of the emergency blow-off panel for the choked vent. With the RIPS HA method, potential hazards in this tank explosion incident would have been recognized under the three sub-systems: process safety culture and leadership, operational discipline, and process safety systems. An illustrative RIPS HA analysis using this example is provided in Table IV.10.

Table IV.10: RIPS HA worksheet management system layer analysis – Tank explosion

Project/Plant: XYZ		Rev. no: 0			Date: 12-April-2017			Page: 1 of 1	
Team members:	A, B, C, D, E								
System description:	Blowing operation on a tank								
Mode:	Under maintenance								
Node (P&ID):	101								
<i>Subsystem: Process safety culture and leadership</i>									
					Risk without any safeguards				
Parameter	Guideword	Deviation	Cause	Consequences	Severity (S)	Likelihood (L)	Risk (R)	Recommendations	Responsible entity
Communication	Skipped	No LFI communication of previous incident	Poor management communication	Similar incident happened	S2	L2	R2	Strong LFI communication process	Incident Investigation & Learning Manager
Emergency Response	Unavailable	Absence of emergency blow-off panel for choked vent	Lack of resource allocation	End of tank blown off	S3	L2	R2	Provide emergency blow-off panel based on evaluation	Emergency Response & Planning Lead
<i>Subsystem: Operational discipline</i>									
					Risk without any safeguards				
Parameter	Guideword	Deviation	Cause	Consequences	Severity (S)	Likelihood (L)	Risk (R)	Recommendations	Responsible entity
Management of Change	Missing	No authorization for modification from 6 inch vent to 3 inch	Permit to work & Management of Change not followed	Vent plugged	S4	L1	R3	Carry out a systematic management of change process based on calculations	Process Safety Manager
Training	Skipped	No formal training on compressed air/choked vent hazards	Poor management commitment	No understanding of power of compressed air and how hazardous choked vents can be	S2	L2	R2	Train/retrain all employees involved on hazards choked vent and compressed air pressure	Learning Center Lead
<i>Subsystem: Process safety systems</i>									
					Risk without any safeguards				
Parameter	Guideword	Deviation	Cause	Consequences	Severity (S)	Likelihood (L)	Risk (R)	Recommendations	Responsible entity
Inspection	Non-routine, inadequate	Vent not registered for regular inspection	Lack of management commitment and operational discipline	Replacement of the vent by a 3 inch hole with no calculations and documentation	S2	L2	R2	Inspect vent frequently to check it is clear	Inspection/Maintenance Engineer

As the next step, a sub-system procedural review is carried out using the sample worksheet and guidewords. Table IV.10 illustrates the RIPSHA worksheet, providing a brief sample of the management system layer analysis carried out for the tank explosion for a blowing operation on a tank. The operation mode is ‘under maintenance’. In this analysis, different potential hazards with respect to three sub-systems – process safety culture and leadership (communication and emergency response), operational discipline (management of change and training), and process safety systems (inspection) have been identified. The potential severity levels considered are catastrophic (S4), critical (S3), moderate³⁰¹, and minor (S1). The probability of occurrence is categorized as frequent (L4), occasional (L3), remote (L2), and unlikely (L1). Among all the hazard scenarios highlighted, one scenario was identified as the most dangerous one and four scenarios were identified as the medium risk. The main advantage of the RIPSHA approach is that it captures potential hazardous scenarios related to management layer sub-systems. Another advantage of the RIPSHA method is the ability to analyze various modes of operation, like in this example under maintenance.

4.9. Plant system hazard analysis example: a liquefied natural gas (LNG) facility

A typical LNG process system consists of the following process sections: gas production, pipeline transmission, liquefaction plant, shipping, unloading, regasification, and send-out³⁰². The LNG storage tanks are common to all the LNG facilities, such as import/export terminals and the peak-shaving facilities. Therefore, a LNG storage tank area is selected for the RIPSHA analysis.

Natural gas is composed primarily of methane and contains minor amounts of ethane, propane, butane, nitrogen, and carbon dioxide. The major hazards associated with

LNG are its cryogenic temperature, flammability (flammability range in air is between 5% and 15% by volume), and vapor dispersion properties. Figure IV.3 represents the simplified piping and instrumentation diagram for the LNG storage tank. The LNG storage tank used in this example is a double containment type. The transient operations mode is considered as an example in which tank start-up is studied and demonstrated.

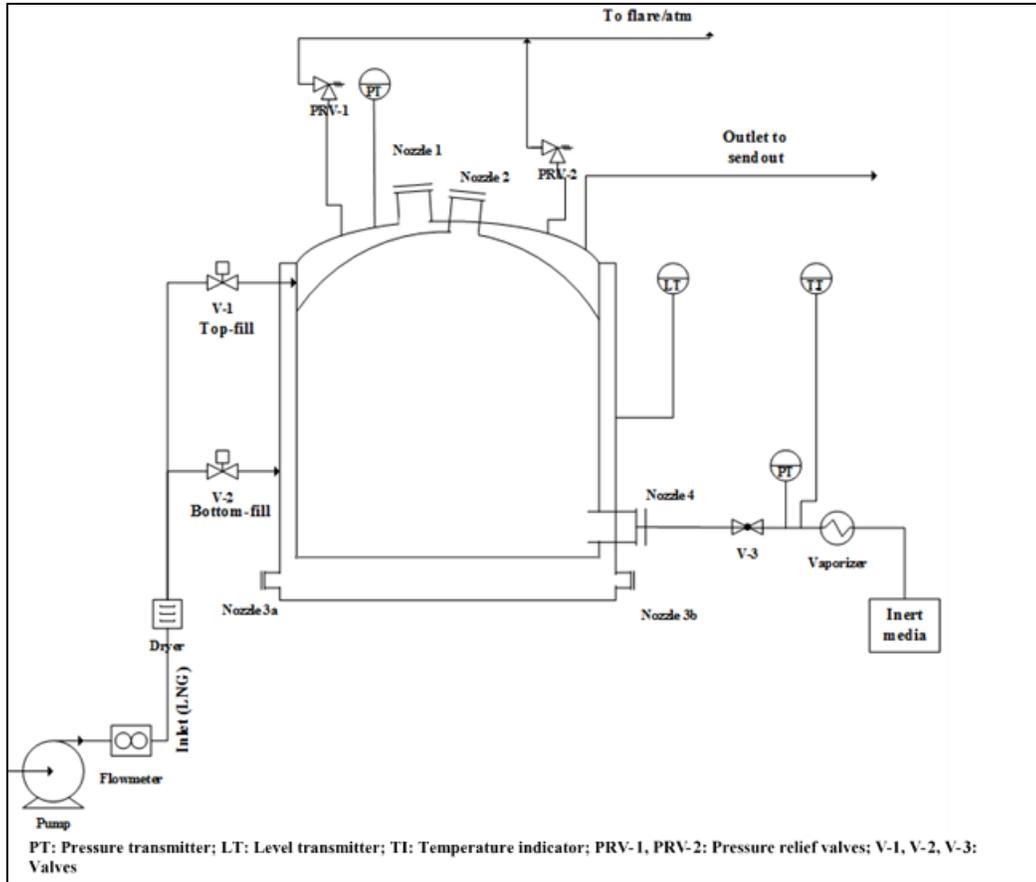


Figure IV.3: LNG storage tank P&ID

Based on the RIPSHA methodology, a team is formed of members with knowledge about the tank start-up operations. The charter is prepared defining the scope of the study within the operations for this example. Information for each hazardous substance, in this case LNG, stored, handled, and processed onsite is collected. The information is expected to include similar information required under 29 CFR 1910.119(d)³⁰³, such as physical and

chemical properties, combustibility, flammability, and explosiveness, toxicity, reactivity, and corrosiveness. In addition, the vessels and piping containing these materials and associated process conditions are identified on drawings, such as process flow diagrams, piping and instrumentation diagrams, and plot plans. Furthermore, any near-miss or incidents reports also are gathered. An example of this is shown in Table IV.11.³⁰⁴

Table IV.11: Incidents in LNG facilities

Year	Ship/Facility Name	Location	Reference
1944	East Ohio Gas LNG tank	Cleveland, Ohio, US	³⁰⁵
1979	Columbia Gas, LNG Terminal	Cove Point, Maryland, US	^{306, 307}
1985	LNG Peakshaving facility	Pinson, Alabama, US	³⁰⁷
1989	Tellier	Algeria	³⁰⁷
1989	LNG Peakshaving facility	Thurley, United Kingdom	³⁰⁶
1993	Indonesian liquefaction facility	Indonesia	³⁰⁷
2002	LNG Ship, Norman Lady	East of the Strait of Gibraltar	³⁰⁷
2004	Skikda	Algeria	³⁰⁵
2010	LNG Edo	Nigeria	³⁰⁷
2014	Williams Partners, Plymouth	Plymouth /Benton County, WA	³⁰⁸

The RIPSHA approach would have identified some of the hazardous scenarios developed in the facilities mentioned in Table IV.11 that led to the incidents. For example, the primary cause of the Plymouth incident was identified as the substandard purge performed, which led to the auto-ignition of the flammable gas mixture during the start-up. Inadequate procedure (wrong start-up sequence), and incorrect operation were recorded as some of the contributory causes of the incident³⁰⁸. Another example is the Skikda gas-

liquefaction plant incident. Inadequate emergency preparedness and hiring and management policies were ascertained for higher number of casualties³⁰⁹. With RIPSHA method, the potential hazards in the Plymouth incident would have been recognized under the ‘procedure’, and ‘operator’ sub-systems using resilience metrics such as P3 and P4. Additionally, for the Skikda incident, application of recoverability metrics such as R1, R2 in RIPSHA approach would have identified potential gaps in emergency response plans and procedures.

As the next step, a sub-system procedural review is carried out using the sample worksheet and guidewords. Table IV.12 illustrates the RIPSHA worksheet, providing a brief sample of the plant system layer analysis carried out on the LNG storage tank for a transient operation, start-up. In this analysis, different potential hazards with respect to three sub-systems – ‘procedure’ (start-up procedure), ‘plant equipment’ (storage tank), and ‘operator’ (field/control room operator) have been identified. The potential severity levels considered are catastrophic (S4), critical (S3), moderate S2, and minor (S1). The probability of occurrence are categorized as frequent (L4), occasional (L3), remote (L2), and unlikely (L1). Among all the hazard scenarios highlighted, one scenario was identified as the most dangerous one; three scenarios were identified as medium risk and two scenarios as low risk. The main advantage of the RIPSHA approach is that it captures the potential hazardous scenarios related to sub-systems ‘procedure’, and ‘operator’. Another advantage of the RIPSHA method is the ability to analyze various modes of operation, like in this example transient operations. Furthermore, with the use of this method safeguard analysis is incorporated effectively in the worksheet.

Table IV.12: RIPSHA worksheet plant system layer analysis – LNG storage tank

Project/Plant: XYZ		Rev. no: 0					Date: 28-Dec-16			Page: 1 of 1			
Rev. no:	0												
Team members:	A, B, C, D & E												
System description:	LNG storage tank (start-up)												
Mode:	Transient operations												
Node (P&ID):	101												
Subsystem: Procedure	Start-up procedure			Subsystem intention			To ensure a safe and effective commissioning and transition to operations.						
					Risk without any safeguards				Risk with safeguards				
Parameter	Guideword	Deviation	Cause	Consequences	S	L	R	Safeguards	S	L	R	Recommendations	Responsible entity
Piping & equipment clean-up inspection	Incomplete	Incomplete piping/equipment clean-up	Specific clean-up procedure not followed	Damage of in-line equipment (pumps, valves) resulting in total failure	S3	L2	R2	Low point drains; end caps on piping	S2	L1	R1	Ensure proper cleaning procedures are followed, foreign particles are removed during installation	Commissioning & Construction engineer
Drying-out	Improper	Improper drying out	Poor/hurried planning and preparation	Water/water vapor can freeze in valves/pumps/low points in the piping; damage to valve seats; delay in start-up schedule; increased costs	S3	L2	R2	Accurate & detailed procedures; recordkeeping	S2	L1	R1	not required	–
Purging	Wrong medium	Wrong medium in purging	Lack of knowledge	Freezing of purge gas under cryogenic temperatures	S3	L1	R2	no safeguards	S3	L1	R2	Compatibility check of the purge gas (temperature & dryness)	Process engineer
Cooling down	Inadequate	Inadequate cooling down	Lack of cool down criteria analysis	Piping stress	S3	L2	R2	no safeguards	S3	L2	R2	Cool down large bore LNG piping using cryogenic vapor flow	Commissioning engineer
Subsystem: Process/Plant equipment	Storage tank			Subsystem intention			To store the cryogenic LNG liquid safely.						
Parameter	Guideword	Deviation	Cause	Consequences	S	L	R	Safeguards	S	L	R	Recommendations	Responsible entity
Flow	High	High flow to tank	Operator inadvertently starts normal & spare pump	Overfilling	S4	L1	R3	High level alarm; pressure indication	S3	L1	R2	Provide interlock to avoid dual pump operation	I&C engineer
Subsystem: Operator/human	Field/control room operator			Subsystem intention			To follow the procedure and communicate effectively.						
Parameter	Guideword	Deviation	Cause	Consequences	S	L	R	Safeguards	S	L	R	Recommendations	Responsible entity
Communication	Skipped/mis sed	Skipped/miss ed communication between field/CR operator	Procedures not followed; faulty communication equipment	Problems in cleaning-up or purging	S4	L2	R3	no safeguards	S4	L2	R3	Establish & follow communication protocol; ensure checklist, documentation is completed	Operations & Commissioning team

4.10. Summary

A review of current hazard identification and analysis methods was presented. It is observed that existing methods do not follow an integrated systems approach, and hence a new resilience-based RIPS HA method has been proposed. This method follows the resilience metrics to develop guidewords for hazard identification and analysis. The approach is an integration of two layers – management system (process safety culture and resilient leadership; operational discipline, and process safety systems) and plant system (process/plant equipment, operator/human and procedures). A significant feature of RIPS HA methodology is that it covers four different modes of analysis – design, normal operations, simultaneous operations, and transient operations to be applied throughout the life cycle of a facility. The life cycle approach allows for the identification of issues early enough in the design phase to incorporate design changes and mitigate hazards more economically, and, at the same time, allows for the review still to be valid through detailed design. Continuing the review throughout detailed design, construction, commissioning, and throughout operation during the life-cycle of the facility ensures that the original siting analysis conducted remains valid for the life of the facility, and that the facility is constructed, tested, and operated in a manner consistent with the original siting analysis.

The RIPS HA methodology is applied to a tank explosion and a LNG case study. This provides an example of a comprehensive and systematic method to identify and analyze hazards for the management system and plant system layers. The study results illustrate that the resilience-based approach is useful for identification of unknown scenarios from human and organizational perspective.

CHAPTER V

QUANTITATIVE ASSESSMENT: PREDICTABILITY ANALYSIS*

There are uncertainties involved in the risk assessment of process systems operations. Also, systems are complex and deteriorate gradually with time or due to exposure to expected or unexpected disturbances/events. Questions such as, what is the frequency of a process upset?; can we predict incidents?; what are the safe operational limits for the process?, are yet to be explored and answered. With the use of Process Resilience Analysis Framework (PRAF), this chapter presents a resilience-based approach to manage uncertainties to better predict process upsets and determine the feasible operational region. The application of the predictability assessment for uncertainty management, flexibility analysis, and optimization is demonstrated using a batch reactor process system. Three types of uncertainties: medium temperature, agitator failure and reactor charging are considered. These uncertain parameters are analyzed using Global Sensitivity Analysis (GSA) using the gPROMS platform and exchanging information with MATLAB through goMATLAB. As a next step, uncertainty analysis is conducted using the Monte Carlo Markov Chain (MCMC) models to find out the actual operation bounds. Further dynamic feasibility and optimization provides the maximum operational bounds and economic optimization results. It is concluded that with the use of resilience metrics data, robust process simulation, and uncertainty management, the variance of statistical parameters can be updated leading to high probability regions of the parameter space

*Reproduced in part with permission from Jain, P., Chakraborty, A., Pistikopoulos, E.N., & Mannan, M. S., "Resilience-Based Process Upset Event Prediction Analysis for Uncertainty Management Using Bayesian Deep Learning: Application to a Polyvinyl Chloride Process System," *Industrial & Engineering Chemistry Research*, Vol 57 (43), Pages 14822-14836. Copyright 2018 American Chemical Society

responsible for the observed data. This helps the risk assessors to ascertain the critical parameters impacting the key performance indicators, determine the maximum feasibility, and thus make more accurate and informed process risk decisions.

5.1. Background

Process systems are complex socio-technical systems that are susceptible to catastrophic incidents as there are certain process or mechanical or instrumentation or human hazards in the plant⁸⁹. Uncertainty management in the risk assessment has a pivotal role to predict any process upsets or prioritize safeguards to survive through upsets or minimize emergency response time to reduce the severity of consequences.

The avoidance phase of PRAF deals with the objective of predicting process upsets for better flexibility and control of the process systems. The primary objective of the predictability assessment is to predict the process upsets to avoid the propagation of event to the catastrophic incident state and achieve better flexibility and control of the process system. With this study, it is aimed to:

- integrate the social factors analysis in a single approach rather than having a separate human risk analysis while covering any missed scenarios in HAZOP studies,
- move from traditional point values for occurrence of loss of containment events (used in QRAs) to a range similar to the Probabilistic Risk Assessment (PRA) methods,
- manage the uncertainties in the limited historical database on frequency or failure rates by using resilience metrics and thus incorporating the process plant performance data of the plant under study,
- and determine the feasible operational region.

In order to demonstrate the application of the methodology, batch reactor operation has been selected as the principal example. Table V.1 presents the statistical data on the prime causes of batch reactor incidents^{163, 310, 311}.

Table V.1: Major causes of batch reactor incidents

	1962 - 1984	1962 - 1987	1986 - 1990	1988 - 2013
Incident cause	(%)	(%)	(%)	(%)
Thermo-reaction chemistry	21.4	20.1	14.8	-
Raw material quality	7.9	8.9	9.803	10
Maintenance factors	22.3	21.3	22.2	13.3
Temperature control	22.2	18.9	13.9	-
Loss of agitation	9.5	10.1	13.1	13
Mischarging of reactants	16.7	20.7	26.2	16.7

5.2. Predictability assessment methodology

The predictability assessment method develops on the idea of combining robust process simulation and statistical methods by using the plant data for prediction of process upsets and achieve improved flexibility and control of the process system under study. The major contribution of the proposed approach is the establishment of accurate and integrated method to predict process upset situations by virtue of a MCMC formulation, GSA, and flexibility optimization backed by process resilience concepts. The overall predictability assessment methodology is illustrated in Figure V.1.

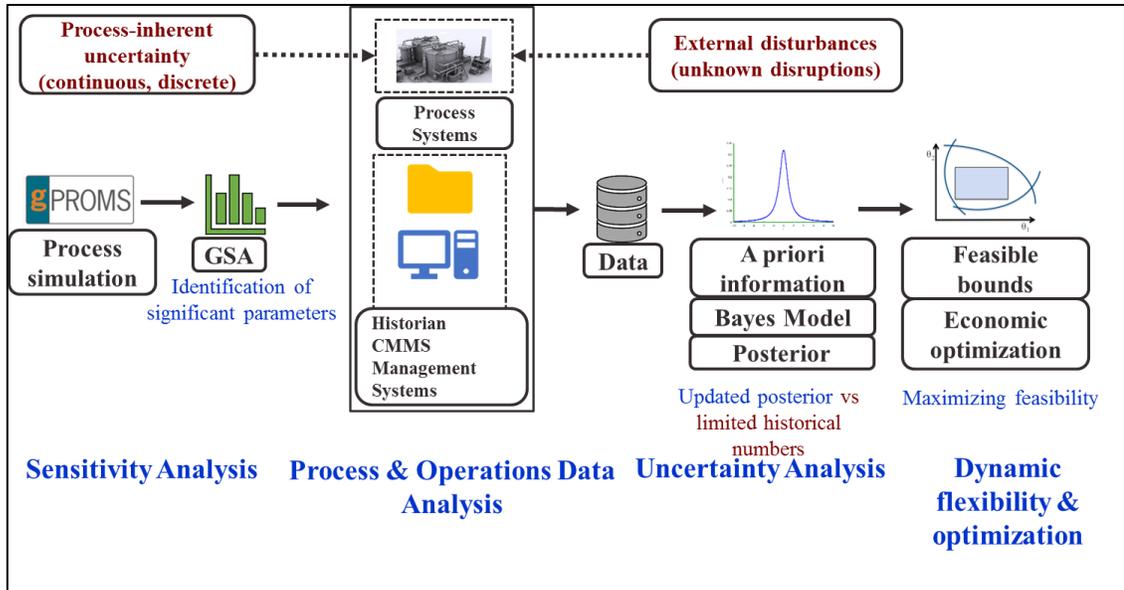


Figure V.1: Predictability assessment

Process systems have process -inherent uncertainties and external/unknown disruptions. This method addresses both of these uncertainties. The prime goal is to use the data from the operations to determine operational limits that would lead to expected production capacity under the process and safety constraints and hence maximum profitability.

Further, the posterior values of statistical parameters are inferred in the Bayesian analysis step based on the prior and resilience metrics information (plant performance data) to obtain the ranges of significant parameters. The incorporation of the relevant resilience metrics information in the analysis enables the use of various data collected in the plant and more importantly, the analysis is more accurate as it is based on the performance of the process system or plant under study and thus helps us to understand effects on the Key Performance indicators (KPIs).

This methodology has the following main steps of 1) Scenario analysis, 2) Process simulation, 3) Global Sensitivity Analysis, 4) Bayesian analysis, and 5) Dynamic optimization. The scenario analysis comprises of identification of triggers or events that may cause the system to transit to the process upset state from the normal operations state.

Robust process simulation is conducted that comprises of sensitivity analysis using global methods to explore the process decision space rapidly and effectively. GSA is a tool used to quantify the significant model parameters and their ranges with regards to the model output. For example, for the runaway reaction scenario, impact of three uncertainties (or model parameters) would be studied on the reactor temperature (model output). The posterior values of statistical parameters are inferred in the Bayesian analysis step based on the prior, resilience metrics information (plant performance data) and congruence analysis (social aspects quantification) results. The incorporation of the relevant resilience metrics information in the analysis enables the use of various data collected in the plant and more importantly, the analysis is more accurate as it is based on the performance of the process system or plant under study. Within the resilience metrics, some are social metrics and in cases of mutual impact of such social metrics, it is important to quantify them before including them in the model. A matrix-based method called congruence analysis as explained in Chapter III, is used to quantify the individual and mutual effects of these social metrics³¹². For example, mutual impact of social metrics such as procedures revised and updated and trainings completed on procedures is combined with observations such as shift handover communication violations to obtain a socio-technical congruence metric (C_{st}). This metric is then utilized in the assessment. Figure V.2 illustrates the flow diagram

consisting of the procedural steps, which are taken to calculate the posterior distribution of parameters using Bayes theorem.

The step 5 of this methodology is optimization. In this step, flexibility optimization and optimization for maximum profitability is conducted. The economic optimization step is employed to assess the maximum profitability of the system under process and safety constraints within the feasible operational region.

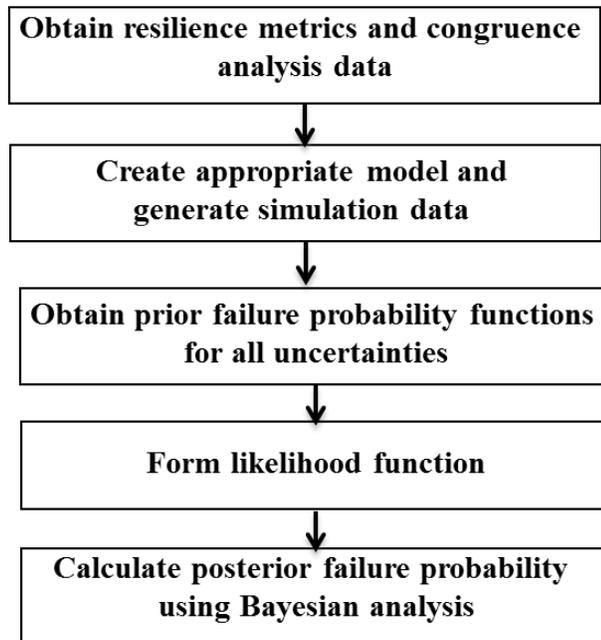


Figure V.2: Bayesian analysis for uncertainty management

5.2.1. Bayesian methods

The two formal statistical methodologies are frequentist and Bayesian. The Bayesian methodology uses Bayes' theorem. It is based on the idea that there might be prior information (knowledge or belief) about the distribution of a parameter value before taking a sample of observations. The Bayesian methodology provides a way to update our prior information about the model parameters using sample information. Generally, the

prior information is summarized in the form of a probability rule called the prior distribution of the model parameters. The posterior distribution of the parameters is proportional to the product of the likelihood and the prior distribution³¹³.

Recently, safety assessment methods based on Bayesian analysis have been extensively developed and used in the chemical process industry. It has been realized that techniques such as hierarchical Bayesian analysis and Bayesian network are effective to overcome limitation of conventional techniques like fault tree in lack of application to dynamic safety analysis³¹⁴. The paper by³¹⁵ summarizes some of the recent progresses in the process systems engineering field such as Bayesian Q learning, Bayesian-adaptive Markov Decision Processes, and Bayesian reinforcement learning. Some examples of work on the Bayesian network methods include the work of³¹⁶ on Bayesian network method for vulnerability assessment of chemical facilities to intentional attacks, another Bayesian network model extended to dynamic Bayesian network based on Dynamic Operational Risk Assessment³¹⁷. Additionally, there are other application methods developed such as Bayesian–LOPA methodology for the LNG industry³¹⁸ and new algorithm using the Bayes' rule for diagnosis of known, multiple and unknown faults³¹⁹.

5.2.2. Sensitivity Analysis

Sensitivity Analysis (SA) is the investigation of how sensitive the output of a model is to variation in the values of its input parameters. Parameters that are non-consequential, quantified by a Sensitivity Index (SI), are fixed at their nominal or originally presumed value, as they appear not to have a significant effect on the model output. Sensitivity analysis methods are commonly grouped in three main categories, namely screening, local, and global methods. A comparative analysis of these methods is presented

in Table V.2. It can be concluded from the comparative analysis that global methods perform better in comparison to local or other methods, especially in cases of non-linear ODE models³²⁰.

Table V.2: Comparison of screening, local, and global methods

Sensitivity Analysis³²¹		
Screening	Local	Global
mutual interaction between parameters not considered	-	mutual interaction between parameters considered
indicate the most important factors	only account for small variations from the parameter nominal values	applicable to the whole range of the model's existence
calculation of only first order effects	-	calculation of higher order effects
lack precision, especially when used on nonlinear models	can be used for non-linear models	able to cope with nonlinearities
		Model approximation
		<i>e.g.</i> , regression analysis, correlation ratios, and rank transformation
		cannot account for higher order effects
		Variance-based methods
		<i>e.g.</i> , sensitivity indices
		can account for higher order effects

5.2.3. Global Sensitivity Analysis (GSA)

GSA is a global tool used to quantify the importance of model parameters and their interactions with regards to the model output³²⁰. The two main properties are (i) varying all parameters simultaneously and (ii) sensitivity measurement is done over the complete range of each input parameter. A number of global sensitivity methods such as FAST, extended FAST, the Sobol' indices and the Morris method are available. The Sobol'

indices method has been found to perform better with respect to – application to nonlinear and non-additive models, calculation of the total sensitivity indices, distinguish between individual and total sensitivity index and more. Hence, in this work, Sobol sensitivity indices have been used that are based on an ANOVA type of a high dimensional model representation³²².

5.2.4. Flexibility analysis

In order to determine the capability of a process to operate within the maximum parameter range under constraints such as product quality, safety, and demand, flexibility or feasibility analysis is conducted. The pioneering work of Grossman and his coworkers developed some sophisticated mathematical formulations to determine the feasible region for steady state operations^{323, 324, 325, 326, 140}. Dimitriadis et al. presented an advanced approach for the flexibility analysis under dynamic conditions³²⁷. A dynamic optimization formulation was demonstrated for two cases:

- when uncertain parameters variation with time was known or
- when the feasible region could be presented by a rectangular region where

the critical points that limited feasibility were vertices

A MINLP formulation was suggested for cases other than above by following an explicit discretization scheme for the differential equations and combining it with an active constraint strategy.

5.3. Case study: Batch reactor case study

5.3.1. Process description

The batch reactor process system used in this work to demonstrate the methodology has been considered by³²⁸. This process system consists of a batch reactor and a jacket cooling system as illustrated in Figure V.3.

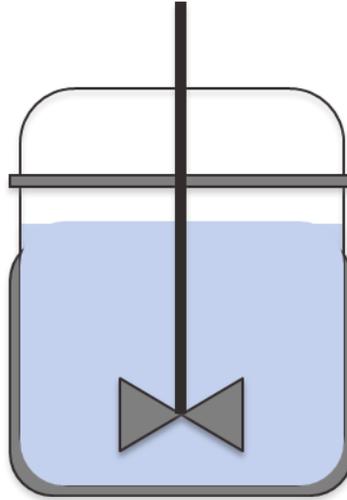
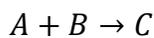


Figure V.3: Batch reactor process system

The typical process has two exothermic reactions being carried out in parallel in the reactor as shown below:



Here, A and B are the raw materials, C is the desired product, and D is the undesired by-product. The batch reactor dynamics is modeled based on first principles as captured by equations (5.1) – (5.14).

Material balance

$$\frac{dM_A}{dt} = -k_1 M_A M_B - k_2 M_A M_C \quad (5.1)$$

$$\frac{dM_B}{dt} = -k_1 M_A M_B \quad (5.2)$$

$$\frac{dM_C}{dt} = +k_1 M_A M_B - k_2 M_A M_C \quad (5.3)$$

$$\frac{dM_D}{dt} = +k_2 M_A M_C \quad (5.4)$$

Energy Balance

$$\frac{dT_r}{dt} = \frac{Q_r + Q_j}{M_r C_{pr}} \quad (5.5)$$

$$\frac{dT_j}{dt} = \frac{F_j \rho_j c_{pj} (T_{jsp} - T_j) - Q_j}{V_j \rho_j c_{pj}} \quad (5.6)$$

with

$$k_1 = \exp\left(k_1^1 - \frac{k_1^2}{T_r + 273.15}\right) \quad (5.7)$$

$$k_2 = \exp\left(k_2^1 - \frac{k_2^2}{T_r + 273.15}\right) \quad (5.8)$$

$$W = MW_A M_A + MW_B M_B + MW_C M_C + MW_D M_D \quad (5.9)$$

$$M_r = M_A + M_B + M_C + M_D \quad (5.10)$$

$$C_{pr} = \frac{C_{pA} M_A + C_{pB} M_B + C_{pC} M_C + C_{pD} M_D}{M_r} \quad (5.11)$$

$$Q_r = -\Delta H_1 (k_1 M_A M_B) - \Delta H_2 (k_2 M_A M_C) \quad (5.12)$$

$$Q_j = UA(T_j - T_r) \quad (5.13)$$

$$A = \frac{2W}{\rho r} \quad (5.14)$$

The reactor temperature is a critical process parameter to watch and has the following constraints:

- First set point: 90°C (within 70 minutes)
- Second set point: 105°C

- System failure: 150°C

5.4. Methodology application

Step1: Scenario analysis

A report published by the U.S. Chemical Safety Board illustrated that around 35 % of incidents were caused due to runaway reactions³²⁹. In the batch reactor process system, there are three main system states: normal operation, process-upset event, and catastrophic state as shown in Figure V.4. As noted in literature, rate of heat removal vs heat generation is critical for a thermal runaway reaction³³⁰. The literature on exothermic reaction leading to a thermal runaway has highlighted several causes^{330, 331}. Some of them are thermochemistry, reactants mischarging, temperature control, inadequate agitation, maintenance, and human errors. In this example, the purpose is to predict the high temperature situation in the reactor. Hence, the initiating events IE1, IE2, IE3, IE4 – these are medium temperature, agitator failure, mischarging of reactants, and unknown disruptions respectively - selected for this study are the ones that relate closely to the selection of optimal operating conditions.

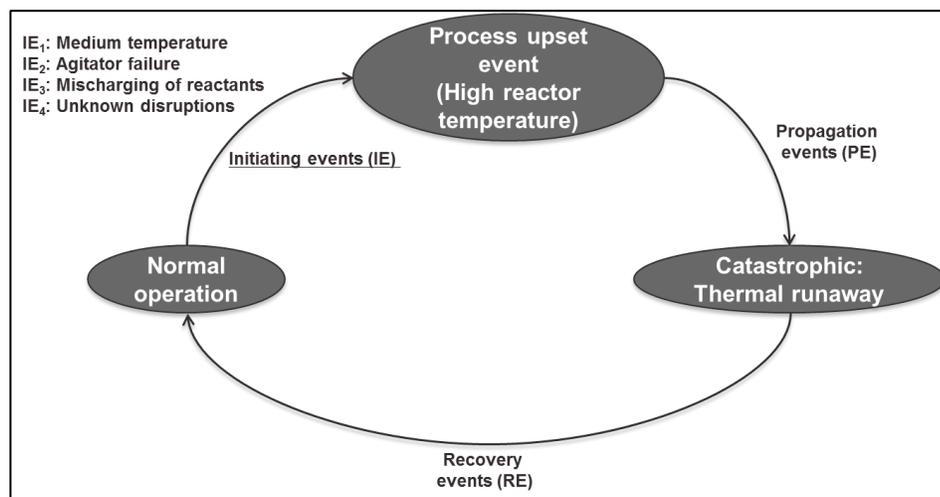


Figure V.4: Batch reactor process system transition diagram

Step2: Process simulation

The impact or variability in the reactor temperature can occur due to various uncertainties. This research focuses on evaluating the following uncertainties: jacket medium temperature, no/partial mixing caused due to issues with equipment such as agitator, and mischarging of reactor. The process simulation for a wide range of input process parameters is carried out in the gPROMS platform to study the impact of variability of these parameters on the output indicators of interest. The following modifications are made in the reactor system by Podofillini³²⁸, in order to study the problem as described:

- The heat transfer coefficient is not considered as constant and the following equation is introduced to study the influence of the agitator working on the reactor temperature,

$$\frac{UD_t}{k} = a\left(\frac{D_a^2 N \rho}{\mu}\right)^b \left(\frac{c_p \mu}{k}\right)^{\frac{1}{3}} \left(\frac{\mu}{\mu_w}\right)^m$$

- Equations (5.15) and (5.16) are added to incorporate the uncertainties involved in the reactor feed,

$$M_A = M_{A_i} + M_A \quad (5.15)$$

$$M_B = M_{A_i} + M_B \quad (5.16)$$

- A Proportional-Integral (PI) controller is added to the reactor dynamics to simulate both the controlled and uncontrolled cases using the following equation,

$$u(t) = K_p e(t) + K_i \int_0^t e(t) dt \quad (5.17)$$

where $u(t)$ is the control variable, $e(t)$ is the deviation of the output compared to the set point. K_p and K_i are the PI controller design parameters.

Robust simulation results

The four plots presented in Figures V.5, V.6, V.7, and V.8 illustrate how the three uncertainties affect the profile of performance indicators of interest, which are reactor temperature and product concentration with time. The red and the orange lines represent the uncontrolled case and black and green indicate the controlled case. On the X-axis is time, primary Y-axis represents the reactor temperature, and secondary Y axis shows the product concentration.

The blue and maroon dotted lines indicate the first two set points of 90°C in first 70 minutes and 105°C respectively.

From Figure V.5, it can be observed that for the medium temperature, reactor temperature reaches the first set point and gets close to the second set point. As evident from Figure V.6, for the agitator revolutions, and inert compositions cases it remains within the set points desired range. Figures V.7 and V.8 depict that the product concentration is affected by the inert compositions presence in the raw materials A and B.

Some conclusions that can be drawn are:

- Reactor temperature has highest sensitivity to medium temperature, followed by agitator revolutions.
- Product concentration is impacted by inert compositions in the feed.
- In the controlled case, the process operations is stable with respect to both reactor temperature and product concentration.

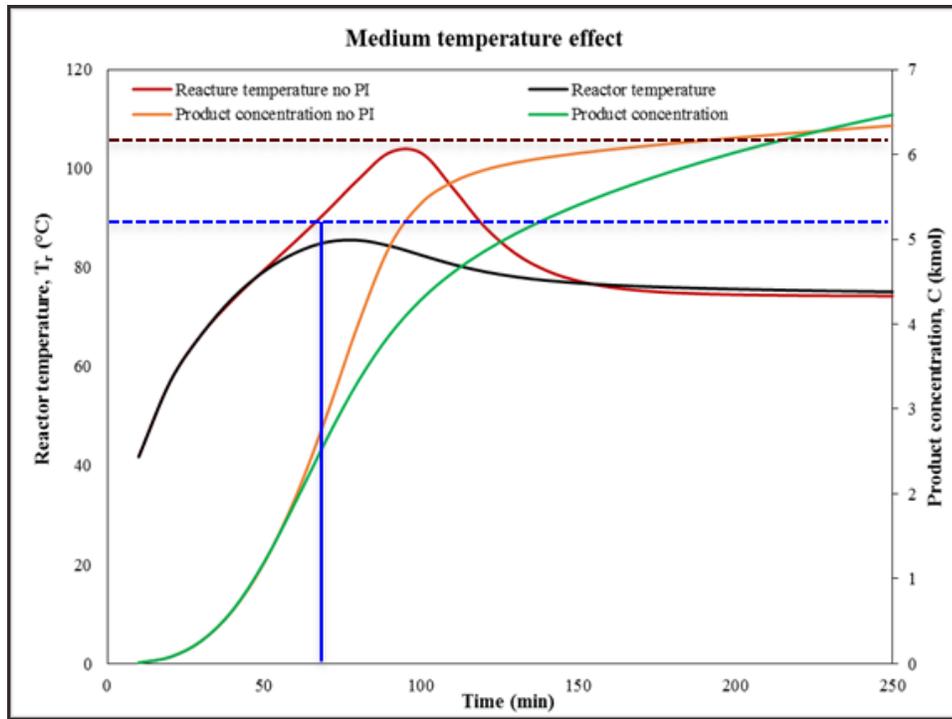


Figure V.5: Effect of medium temperature on the KPIs

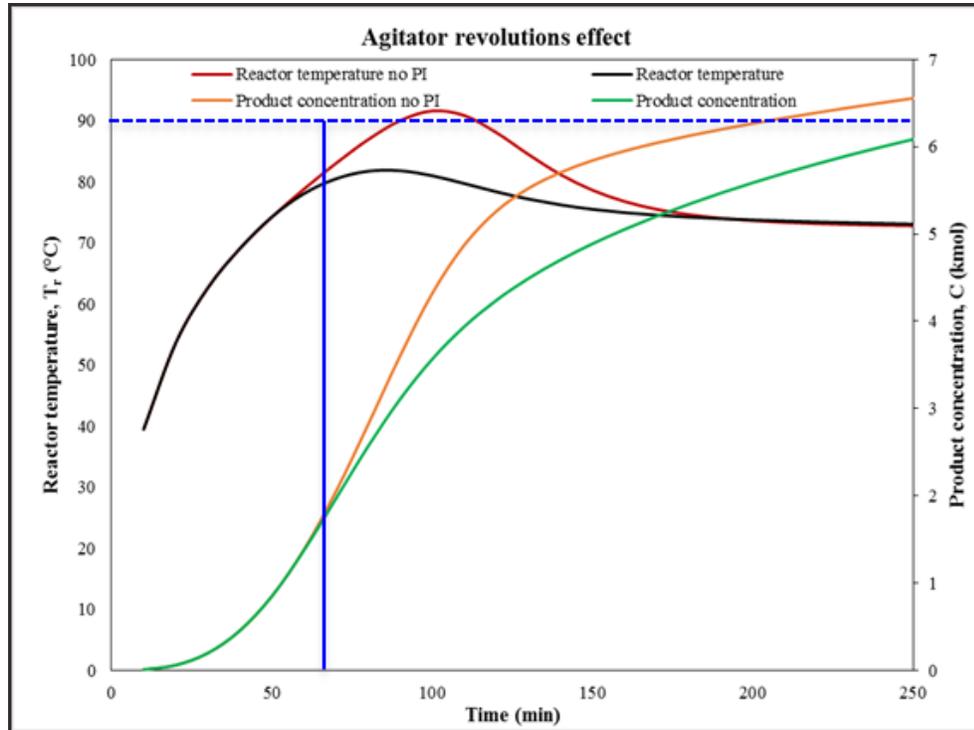


Figure V.6: Effect of agitator revolutions on the KPIs

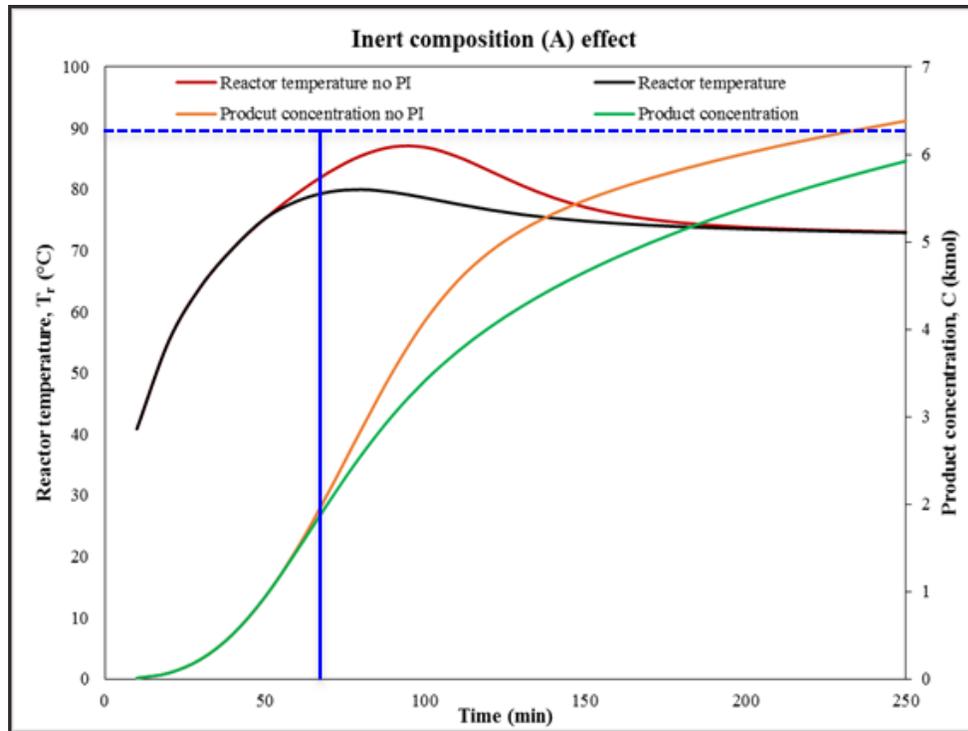


Figure V.7: Effect of inert composition (A) on the KPIs

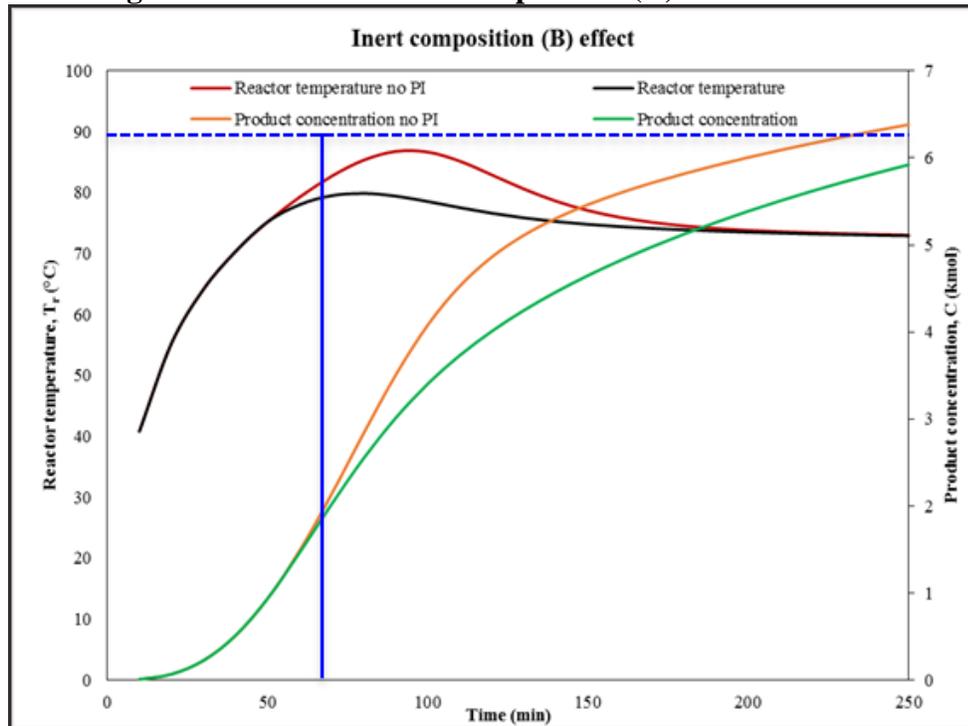


Figure V.8: Effect of inert composition (B) on the KPIs

The plot in Figure V.9 depicts the combined or emergent effect of uncertain parameters on the reactor temperature and the product concentration. It is evident that the mutual effect of uncertain parameters is very different from their individual contribution. It can be seen that the reactor temperature for uncontrolled case is almost touching the third setpoint by reaching a temperature of 150°C. Also, the product concentration is decreased to slightly above 3 kmol.

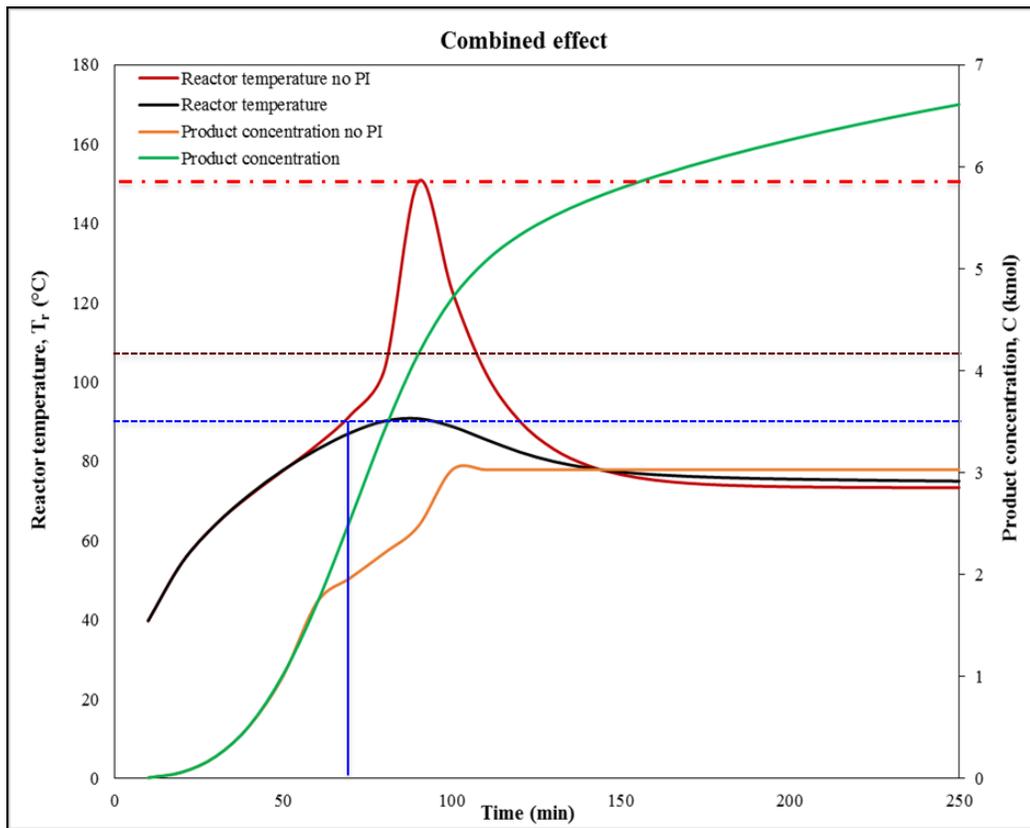


Figure V.9: Combined effect of uncertain process parameters on the KPIs

Step3: Global Sensitivity Analysis

GSA is the mathematical method according to which the model parameters are simultaneously excited, within the range of interest, and their effect on the model outputs is monitored. Such methods facilitate the exploration of the global parameter space,

handling adequately the nonlinearities, yielding a complete set of results that demonstrates both the sensitivity of the model to the uncertainty of the parameter values and the effect of one model parameter to the other^{332, 333}. In this work, RS-HDMR is applied to analyze 4 parameters on the 3 differential model variables. Data are collected for the entire batch period (240 minutes) using a sampling time of 10 minutes. The GSA results indicate two significant parameters.

The model consists of 30 differential and algebraic equations, 27 variables and 30 parameters. The model simulation is performed in gPROMS[®] ModelBuilder v5.0.2. Following the framework presented by Kiparissides et al., the model is subjected to sensitivity analysis for the identification of the significant parameter set³³². The sensitivity analysis is executed through the gO:MATLAB interface that allows in tandem utilization of gPROMS[®] ModelBuilder and MATLAB[®].

Sensitivity analysis results

The bar graphs in Figures V.10 and V.11 are showing the calculated sensitivity indices for the selected time points and four different input parameters for PI and no PI cases. A threshold value of 0.1 is generally considered to study strong significance.

Some conclusions are as follows:

- Reactor temperature is affected primarily by the jacket medium temperature.
- Other parameters have very small and really not noticeable (<0.1) SI.
- For the PI case, no parameters have noticeable SI.

The bar graphs in Figures V.12 and V.13 are showing the second order or the combination effects for the selected time points and four different input parameters for PI

and no PI cases. A threshold value of 0.04 is generally considered to study strong significance. The following are some conclusions:

- There is a noticeable second order effect for the combination of P1 and P2 that is jacket medium temp and agitator revolutions.
- Other parameters combinations have very small and really not noticeable (<0.04) TSI.

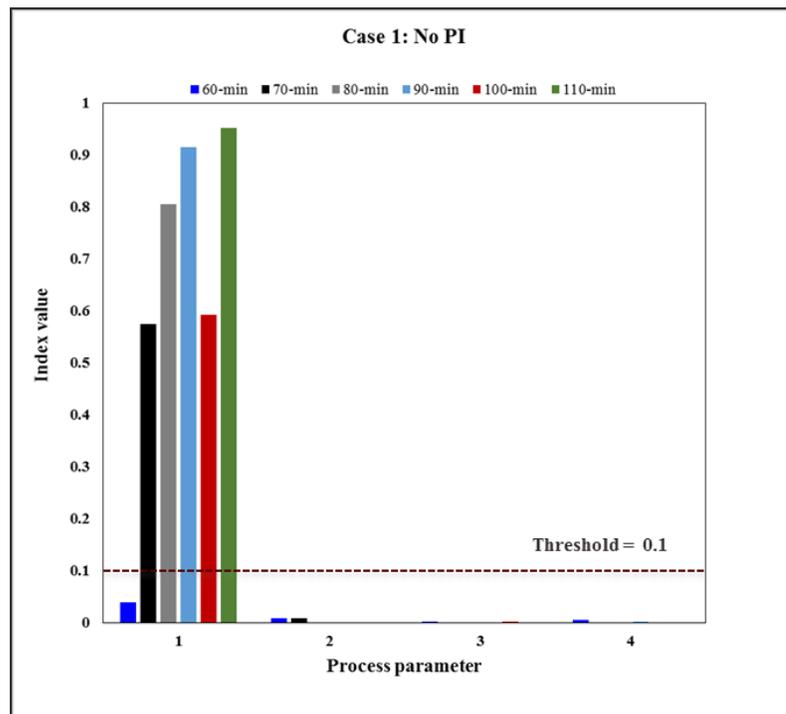


Figure V.10: First order sensitivity indices for the uncontrolled case

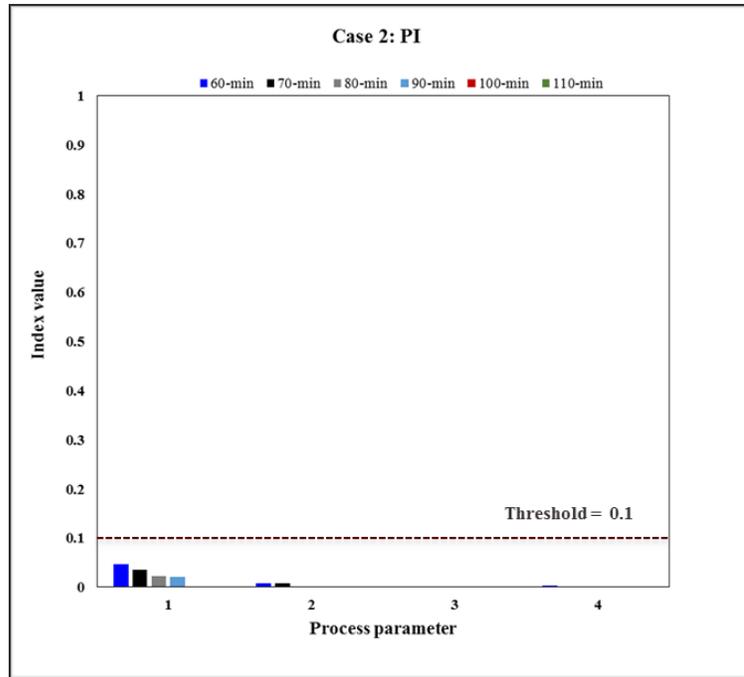


Figure V.11: First order sensitivity indices for the controlled case

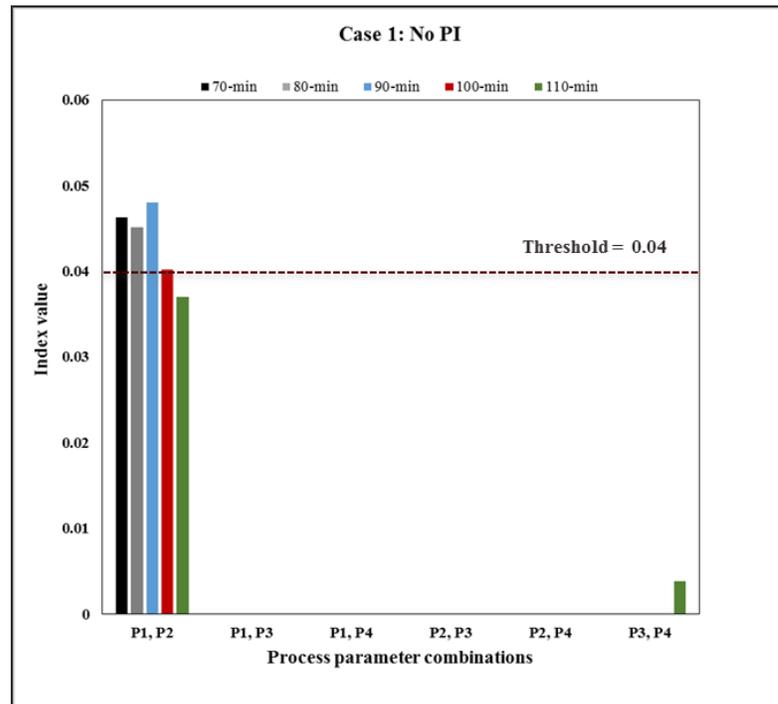


Figure V.12: Second order sensitivity indices for the uncontrolled case

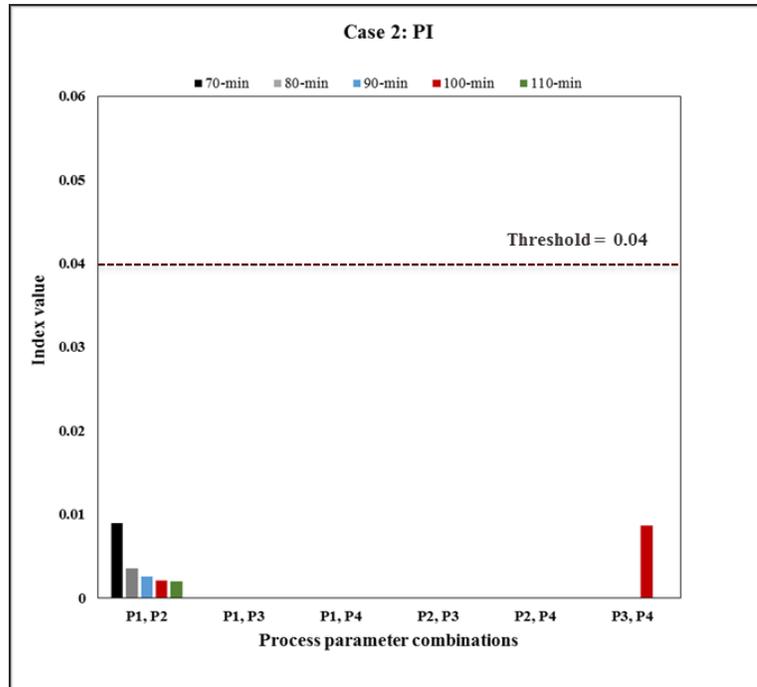


Figure V.13: Second order sensitivity indices for the controlled case

Step4: Statistical analysis

Finite sample performance of statistical procedures can be largely enhanced when domain expertise is incorporated in such analysis³³⁴. In the current case study, domain knowledge and information from plant performance is utilized in the form of prior information and likelihood respectively. Also, there is a two-pronged objective to estimate the parameters in the model, and to quantify the uncertainty associated in the form of posterior distribution. Models for three variables are demonstrated using hypothetical data to quantify uncertainty incorporating the plant process and resilience metrics data. These metrics should be selected to utilize in the analysis based on the following two factors:

- Relevance to the case study or scenario under study. For example, metric such as unplanned maintenance can give an indication of the health of the agitator or pump.

- Availability of information on the metrics. Many organizations already capture information on most of the metrics, although it is important to see what information is available to conduct the analysis.

Medium temperature analysis

Model and Prior

Figure V.14 shows the detailed algorithm for medium temperature analysis.

Suppose there is a set of medium temperatures (these can be observed from Historian) $\{T\}_{i=1}^n$ measured in Celsius scale. An additive model is proposed with three components for T_i ; a grand mean μ , a deterministic known effect v and a random effect α . μ can be interpreted as the unknown population mean of the temperatures. The number $v = v(X) = \sum w_j X_j$ is a linear weighted summary of resilience metrics (X_j) where the weights have been determined based on the results of PRAF survey on the resilience metrics³³⁵. To accommodate further randomness due to unknown resources, a random effect that follows normal distribution, $\alpha \sim N(0, \varphi^2)$ is added. With these components, the i^{th} cooling medium temperature T_i is assumed to be,

$$T_i = \mu + v(X) + \alpha + \varepsilon_i, \quad (5.18)$$

where $\varepsilon \sim N(0, \sigma^2)$, the usual randomness in any measurement independent of the random effect alpha. Equation (5.18) can alternatively be written as,

$$T_i^* = \mu + \varepsilon_i^* \quad (5.19)$$

where $T_i^* = T_i - v(X)$ and $\varepsilon_i^* = \alpha + \varepsilon_i$. Clearly, $\varepsilon_i^* \sim N(0, \tau^2)$ where $\tau^2 = \sigma^2 + \varphi^2$.

The model is complemented with a conjugate prior specification on the parameters μ and τ^2 :

$$\begin{aligned} T_i^* | \mu, \tau^2 &= \mu + \varepsilon_i^* \\ \mu &\sim N(\mu_0, \sigma_0^2), \tau^2 \sim \text{Inverse Gamma}(\beta_1, \beta_2) \end{aligned} \quad (5.20)$$

The hyperparameters μ_0 , σ_0^2 are chosen to reflect prior belief on μ . The β_1 and β_2 are chosen such that the prior distribution of τ^2 remains sufficiently non-informative.

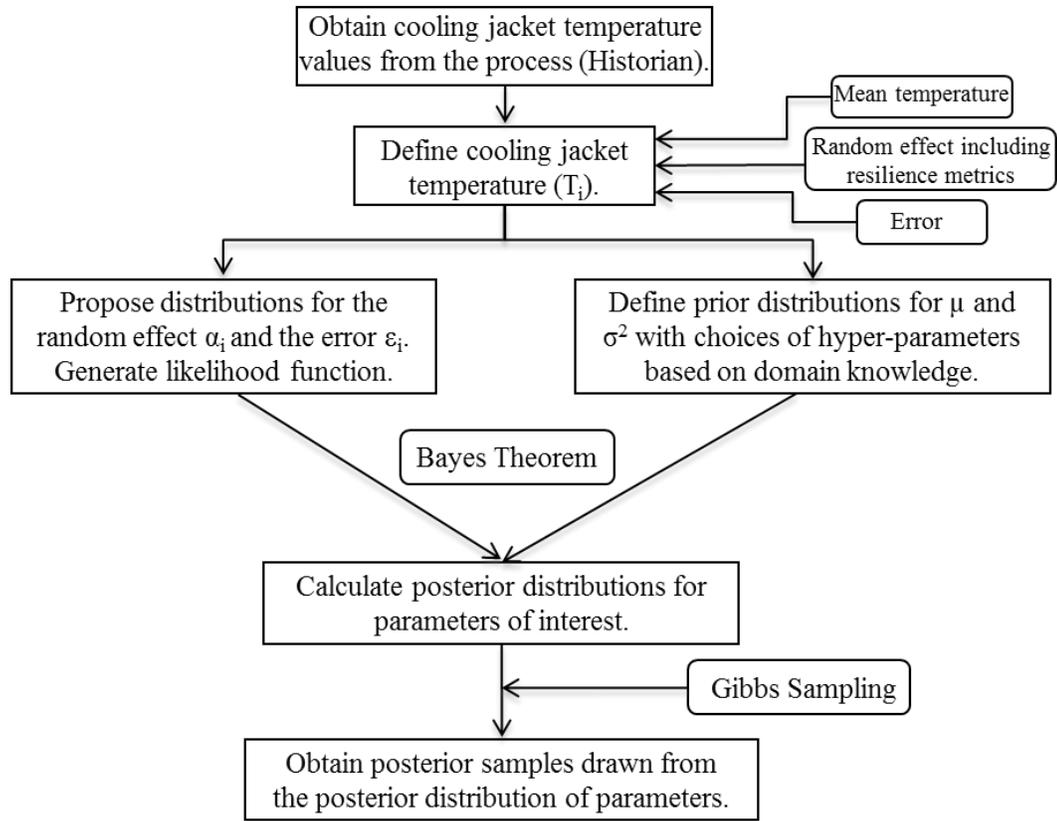


Figure V.14: Algorithm: jacket medium temperature analysis

Analysis

The objective is to obtain the full posterior distribution of the parameters that can be written as $\pi(\mu, \tau^2 | T, X)$. Often, such posterior distributions are not analytically tractable and hence Markov Chain Monte Carlo (MCMC) techniques are employed to sample from the posterior³³⁴. The conjugate prior specification allows for conditional Gibbs update of the parameters and the MCMC sampler cycles through the following steps:

$$1. \quad \pi(\mu | T, X, \tau^2) \sim N\left(\frac{\sum_{i=1}^n \frac{T_i^* + \mu_0}{\tau^2 + \sigma_0^2}}{\frac{n}{\tau^2 + \sigma_0^2} + \frac{1}{\sigma_0^2}}, \frac{1}{\frac{n}{\tau^2 + \sigma_0^2} + \frac{1}{\sigma_0^2}}\right) \quad (5.21)$$

$$2. \quad \pi(\tau^2 | T, X, \mu) \sim \text{Inverse-Gamma}(n/2 + \beta_1, 1/2 \sum_{i=1}^n (T_i^* - \mu)^2 + \beta^2)$$

In these simulation experiments, a sample size of $n = 8736$ (one year of hourly observations of temperature) is considered. The prior mean is fixed as $\mu_0 = 71^\circ\text{C}$ based on domain knowledge for the process with a high prior variance, $\sigma_0^2 = 30^\circ\text{C}$. Essentially, this choice quantifies a moderately strong belief of a process running in normal conditions. β_1 and β_2 were both fixed at 0.001 which gives a sufficiently flat prior for τ^2 .

Agitator failure analysis

Model and Prior

Figure V.15 illustrates the detailed algorithm for agitator failure analysis. Typical statistical techniques to model binary events such as agitator failure include logistic regression, probit regression *etc.*. The authors rely on analyzing underlying variables that are believed to drive agitator performance³³⁶. In this analysis, two variables $I_1 =$ current load in Ampere and $I_2 =$ number of unplanned maintenance are used. A joint distribution of (I_1, I_2) is a mixture with two components - when the agitator is more likely to fail joint distribution of (I_1, I_2) , it takes the form $f_1(\cdot, \cdot)$ and when agitator is working normal it takes the form $f_2(\cdot, \cdot)$. Formally, this can be written as $g(I_1, I_2)$, and the distribution of (I_1, I_2) as,

$$g(I_1, I_2) = p_A f_1(I_1, I_2) + (1 - p_A) f_2(I_1, I_2) \quad (5.22)$$

where p_A denotes the agitator failure probability.

Although $f_1(\cdot, \cdot)$ and $f_2(\cdot, \cdot)$ can be assumed to belong to different parametric families, here it is restricted to the case where both f_1 and f_2 belong to the same parametric

family possibly with different parameters. Since, I_1 is a positive real number and I_2 is a positive integer, the following data generating mechanism is assumed:

$$I_1 \sim \text{Gamma}(\alpha_1, \beta_1), \quad I_2 | I_1 \sim \text{Poisson}(c_1, I_1) \quad (5.23)$$

when the agitator is working normal and

$$I_1 \sim \text{Gamma}(\alpha_2 + v(X), \beta_2), \quad I_2 | I_1 \sim \text{Poisson}(c_2, I_1) \quad (5.24)$$

when the agitator is not working normally. The resilience summary $v(X)$

determines the additional shift in shape of the distribution of I_1 . Since I_2 is generated conditional on I_1 , this shift in scale will also influence I_2 . Here, it is assumed $c_1, c_2 \in \mathbb{R}^+$. The objective, given the data is to estimate p_A and quantify the associated uncertainty. As for the priors, a conjugate Beta (a, b) on the agitator failure probability is placed to complete the model specification.

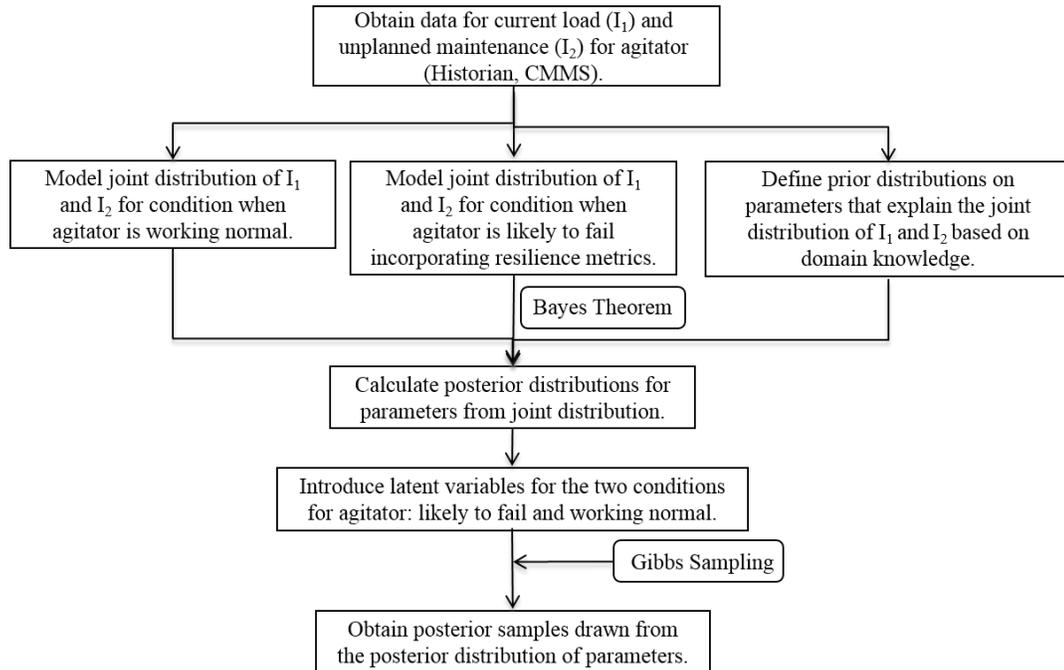


Figure V.15: Algorithm: agitator failure analysis

Analysis

In order to facilitate the posterior computation, a binary latent variable Z for each pair of (I_1, I_2) which indicates the underlying distribution (I_1, I_2) is coming from is introduced. Hence, $I_1, I_2 | Z = 0 \sim f_1$ and $I_1, I_2 | Z = 1 \sim f_2$. Clearly, a priori $P(Z_i = 1) = p_A$ for all pairs (I_{1i}, I_{2i}) . The following conditional Gibbs steps are used to update the joint posterior distribution of $(p_A, Z | I_1, I_2)$.

$$1. \quad \pi(p_A | Z, I_1, I_2) \sim \text{Beta} \sim (a + \sum_{i=1}^n Z_i, b + \sum_{i=1}^n (1 - Z_i)) \quad (5.25)$$

$$2. \quad P(Z_i=1 | p, I_1, I_2) =$$

$$\frac{p_A f_\gamma(I_{1i} | \alpha_1, \beta_1) f_P(I_{2i} | c_1 I_{1i})}{p_A f_\gamma(I_{1i} | \alpha_1, \beta_1) f_P(I_{2i} | c_1 I_{1i}) + (1 - p_A) f_\gamma(I_{1i} | \alpha_2 + v(X), \beta_1) f_P(I_{2i} | c_2 I_{1i})}$$

where $f_\gamma(\cdot | \alpha, \beta)$ denotes the Gamma probability density function with parameters α and β and $f_P(\cdot | \lambda)$ denotes the Poisson probability mass function with parameter λ .

In these simulation experiments, a sample size of $n = 8736$ (one year of hourly observations of agitator), $\alpha_1 = 1$, $\beta_1 = 3$, $\alpha_2 = 10$ and $\beta_2 = 3$ was used. The constants c_1 and c_2 were chosen as 2 and 4 respectively. The prior parameters a and b were fixed at 0.00001 and 0.009702. In Figure V.16 displays the values of (I_1, I_2) generated from the mixture density in eqn. (4).

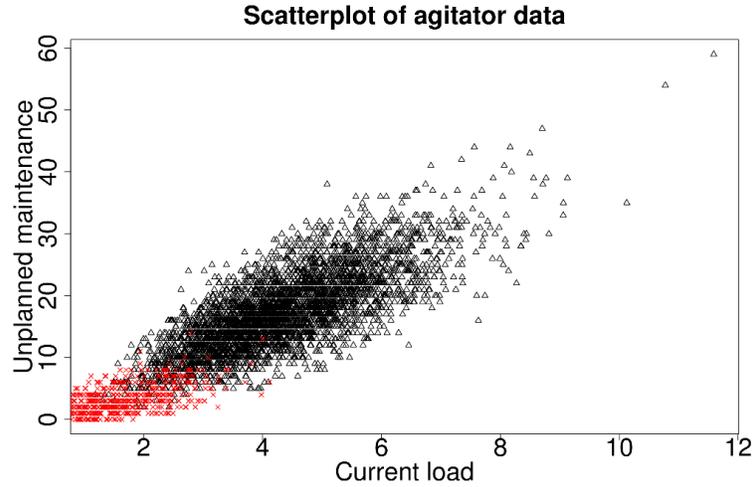


Figure V.16: Scatterplot showing the clustering of (I₁, I₂)

Mischarging of reactants

Model and Prior

Figure V.17 illustrates the detailed algorithm for reactor mischarging analysis. Two metrics, Y_1 = percentage of process safety required procedures reviewed or revised as scheduled and Y_2 = percentage of process safety required training sessions completed are considered. Additionally, there is C_{st} = socio-technical congruence metric lying in the interval $[0, 1]$ which depend on Y_1 and Y_2 . In these simulation experiments, a sample size of $n = 720$ (one year of observations for every batch) is considered. The following decomposition is used for the joint distribution of (Y_1, Y_2, C_{st}) ,

$$f(Y_1, Y_2, C_{st}) = p_R f(Y_1) f(Y_2) f(C_{st} | Y_1, Y_2) + (1 - p_R) f(Y_1) f(Y_2) f(C_{st} | Y_1, Y_2) \quad (5.26)$$

where p_R is probability of reactants mischarging. The mixture formulation can be interpreted in the same manner as in the agitator failure case. The individual components of the mixture density are products of the densities of Y_1 and Y_2 , which are assumed to be independent and then the product is multiplied by the conditional distribution $f(C_{st} | Y_1, Y_2)$.

In these simulations $f(Y_1)$ and $f(Y_2)$ are assumed to be Uniform (0, 1). A weighted sum of Y_1 and Y_2 is considered to generate the C_{st} values. C_{st} is formulated as,

$$\begin{cases} C_{st} = \frac{e^{Z_1}}{1+e^{Z_1}} \\ C_{st} = \frac{e^{Z_2}}{1+e^{Z_2}} \end{cases} \quad (5.27)$$

where $Z_1 \sim N(w_1 Y_1 + w_2 Y_2, 1)$ and $Z_2 \sim N(w_1 Y_1 + w_2 Y_2 + v(X), 1)$.

Here Z_1 represents a Gaussian random summary of (Y_1, Y_2) when there is no reactant mischarging.

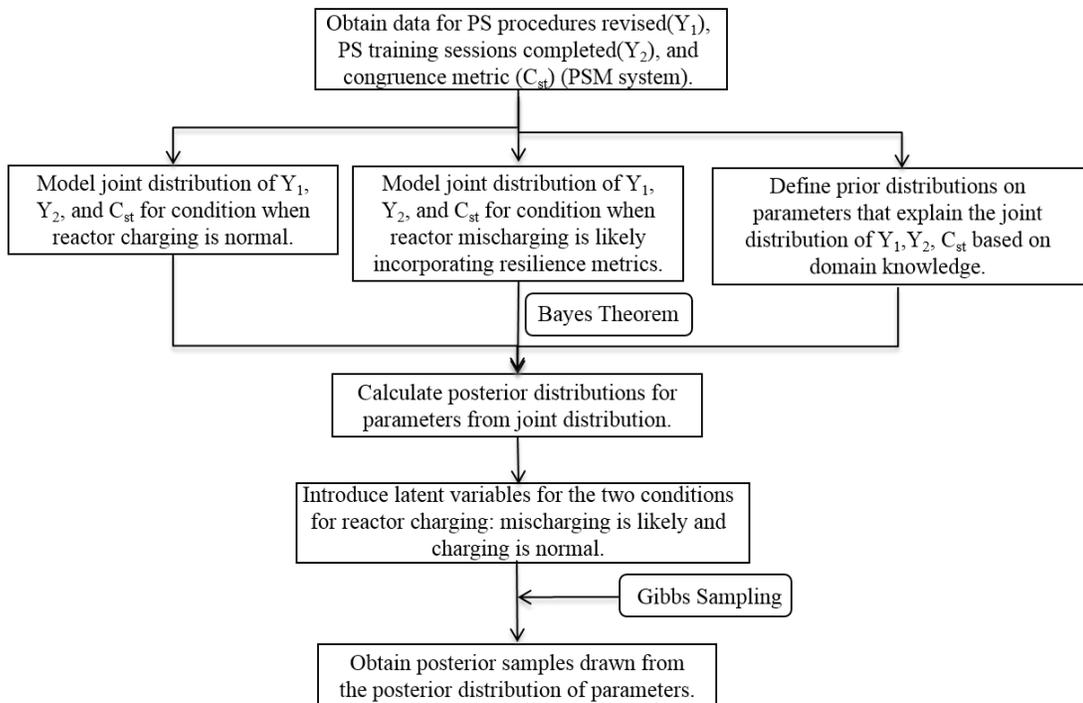


Figure V.17: Algorithm: reactor mischarging analysis

If reactant mischarging occurs, the mean of the index is shifted by an amount determined by $v(X)$. Finally, since $C_{st} \in [0, 1]$, a logistic transformation is used to generate C_{st} . The choice of logistic transformation is not necessary. For example, it can be set to $C_{st} = P(Z \leq z)$ for any probability distribution function P . However, the logistic

transformation is the most widely used transformation in the analysis of variables, which lie in the interval [0, 1]. Similar to the previous section a Beta (a, b) prior on the mischarging probability is assumed and the prior parameters a and b were fixed at 0.00001 and 0.9999.

Analysis

A binary latent variable V is introduced. These latent variables play the same role as Z in the agitator failure analysis. As such, $P(V = 1) = p_R$ a priori. The following Gibbs sampling scheme is adopted to sample from the joint posterior distribution of (p_R, V_1, \dots, V_n) .

$$1. \quad \pi(p_R | V, C_{st}, Y_1, Y_2) \sim \text{Beta} \sim (a + \sum_{i=1}^n V_i, b + \sum_{i=1}^n (1 - V_i)) \quad (5.28)$$

$$2. \quad P(V_i=1 | p_R, I_1, I_2) =$$

$$\frac{p_R f_U(Y_{1i}) f_U(Y_{2i}) f_N(\log C_{st,i} | Y_1, Y_2)}{p_R f_U(Y_{1i}) f_U(Y_{2i}) f_N(\log C_{st,i} | Y_1, Y_2) + (1 - p_R) f_U(Y_{1i}) f_U(Y_{2i}) f_N(\log C_{st,i} | Y_1, Y_2 + v(X))}$$

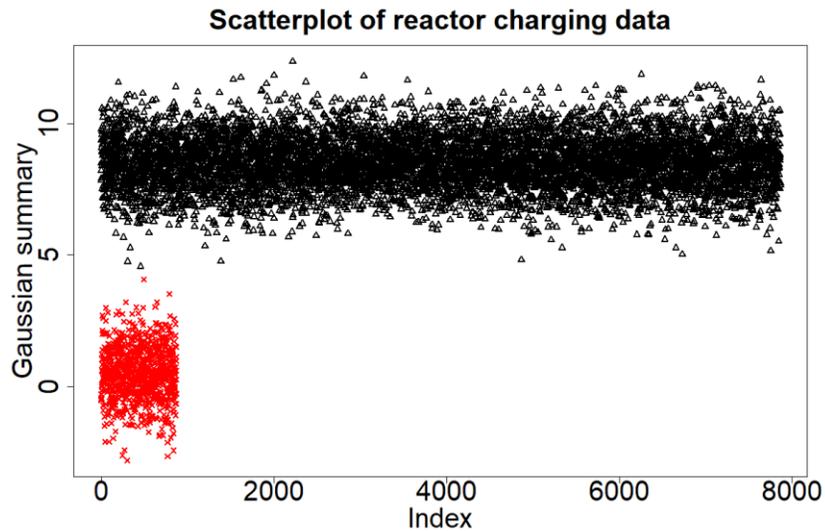


Figure V.18: Scatterplot of Z_1 and Z_2

Since the distribution of Y_1 and Y_2 is same for the two different mixture components, values of Z_1 and Z_2 are plotted in Figure V.18 to gain a better insight into how a typical data generated from the above model would look like.

Uncertainty management results

The results for three different variables – medium temperature, agitator failure, and reactor mischarging – for six different choices of true mean or true probabilities are presented in Table V.3. Also, the true data generating parameters (μ_0 , p_{0A} , p_{0R}) are reported. These are complemented with the posterior mean estimate obtained from the model and analysis. Additionally, the 95% symmetric credible intervals of all the parameters, which are computed as the 0.025, and 0.975 quantile of the posterior samples of the parameters and the posterior standard deviation are provided. All simulations and analysis were carried out in the programming language R¹⁸⁴.

Table V.3: Uncertainty analysis: simulation results

Cases	Jacket medium temperature				Agitator failure				Mischarging of reactants			
	Prior mean cooling medium temperature: 71 °C				Prior mean probability of agitator failure: 0.00103				Prior mean probability of mischarging of reactants: 0.001			
	Prior variance cooling medium temperature: 30 °C				Prior variance probability of agitator failure: 0.001				Prior variance probability of mischarging of reactants:0.00091			
	True mean temperature (μ_0)	Posterior mean (μ)	Posterior sd	Length of credible interval	True probability of agitator failure (p_{0A})	Posterior mean (p_{0A}^{\wedge})	Posterior sd	Length of credible interval	True mean of mischarging of reactants (p_{0R})	Posterior mean (p_{0R}^{\wedge})	Posterior sd	Length of credible interval
Case 1	68	68.3	1.8	7.11	0.004	0.00400	0.000840	0.0035	0.006	0.00620	0.002081	0.0037
Case 2	70	70.1	1.71	7.05	0.005	0.00490	0.000917	0.0040	0.005	0.00560	0.001951	0.0046
Case 3	72	71.9	1.74	7.36	0.006	0.00600	0.001000	0.0044	0.004	0.00420	0.001696	0.0060
Case 4	74	73.7	1.81	7.94	0.007	0.00730	0.001096	0.0046	0.003	0.00350	0.001549	0.0065
Case 5	76	75.4	1.94	9.24	0.008	0.00790	0.001132	0.0050	0.002	0.00210	0.001199	0.0076
Case 6	78	77.1	2.24	11.68	0.009	0.00900	0.001207	0.0053	0.001	0.00140	0.000988	0.0081

Jacket medium temperature

Simulation results for different choices of the true mean μ are summarized in Figure V.19. It is evident that the posterior distribution centers around the true data generating μ with a very small spread around it. Posterior credible intervals were also formed to further gain insight into the associated uncertainty in the estimation procedure. The coverage probability was 0.96.

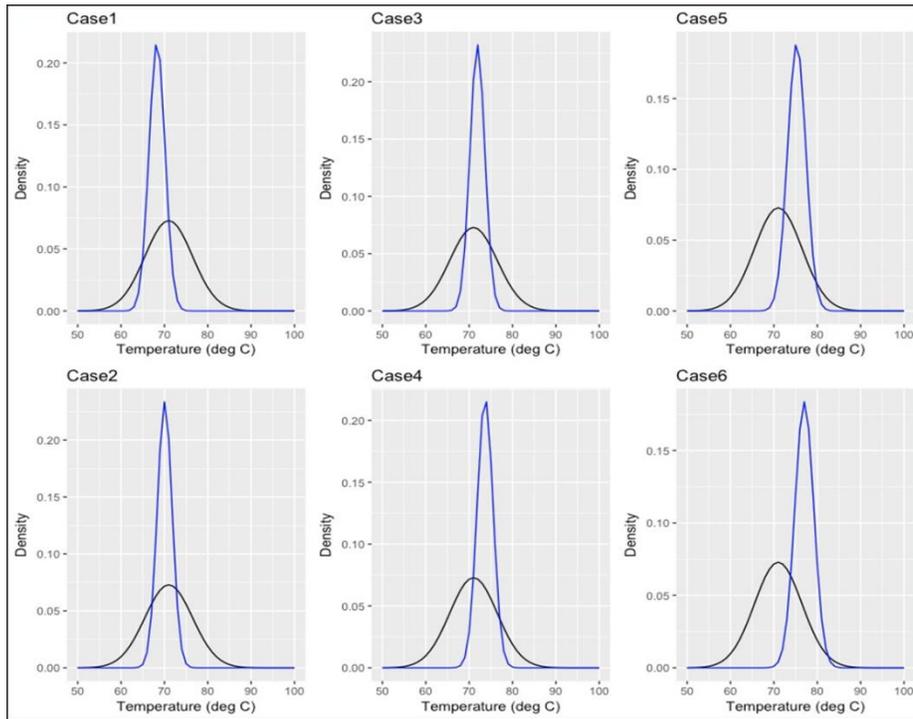


Figure V.19: Jacket medium temperature: Prior (black) and posterior (blue)

Agitator failure

This section summarizes the results with boxplots of prior and posterior samples of agitator failure probability as shown in Figure V.20. It is also observed here that the concentration of the posterior distribution centers around the truth with a very small

spread. Similar to the temperature case, posterior credible intervals were also formed and the coverage probability was 0.97.

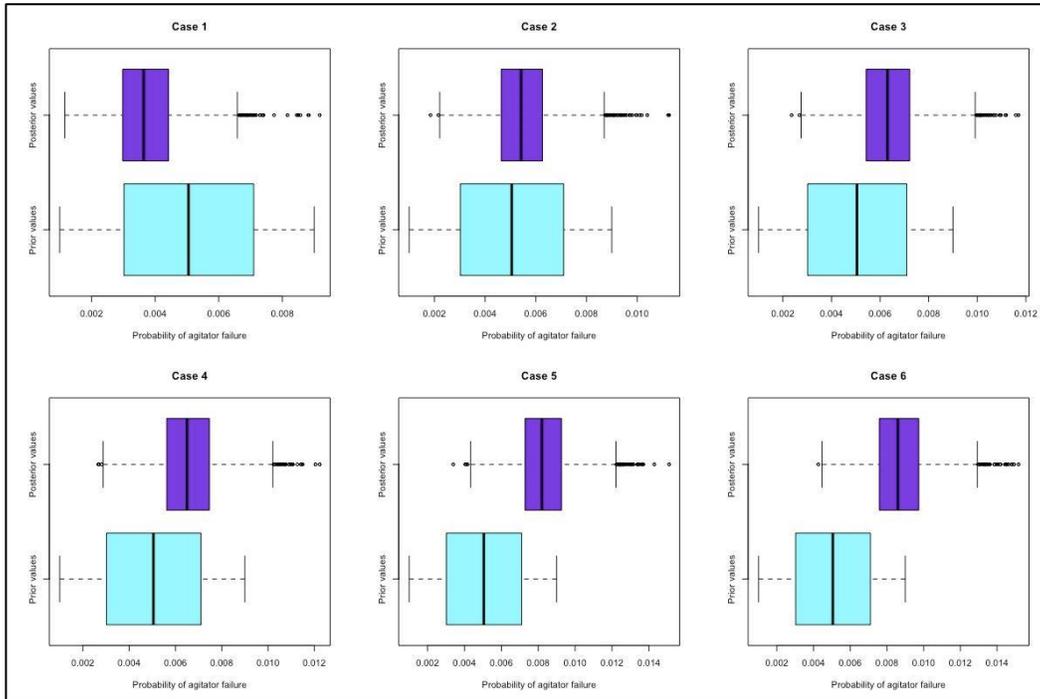


Figure V.20: Boxplot of prior and posterior samples: agitator failure probability

Reactor mischarging

This section summarizes the results with boxplots of prior and posterior samples of reactor mischarging probability as represented in Figure V.21. It is also observed here that the concentration of the posterior distribution centers around the truth with very small spread. Similar to previous cases, posterior credible intervals were also formed and the coverage probability was 0.95.

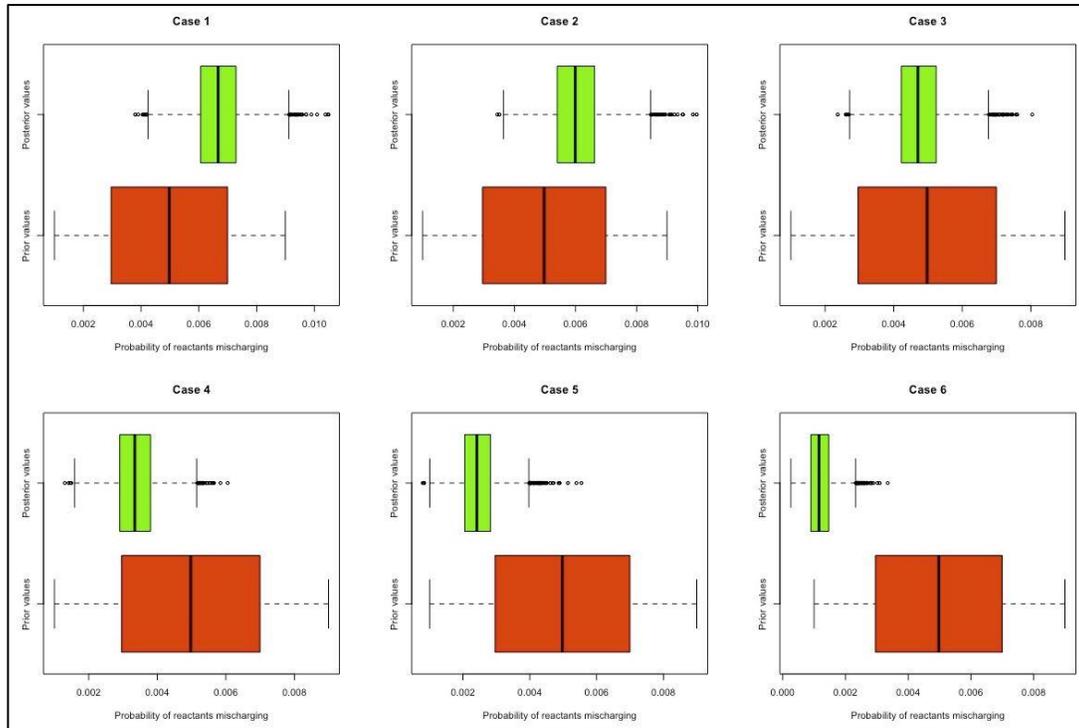


Figure V.21: Boxplot of prior and posterior samples: reactor mischarging probability

Step5: Dynamic flexibility and economic optimization

Given this process model and significant uncertain parameters, dynamic feasibility problem is formulated to obtain the maximum feasible bounds and economic optimization is conducted for maximum profitability. Through robust simulation, feasible region shown as shaded here is obtained for two significant uncertain parameters P1 and P2. The aim is to find the flexibility index or how farther can operations go on the uncertain bounds. The optimization problem is solved in GAMS platform after discretization using the Euler's method (See Appendix C).

For the economic optimization, the objective is to compute the optimal reactor temperature and jacket flowrate policy maximizing the profit for a given fixed batch time

subject to bounds on the reactor temperature. Here is the mathematical version of the problem,

$$\max_{F_j} P = M_C P_{sale} - F_j C_f - M_A C_A - M_B C_B - E_C \quad (5.29)$$

subject to
 process model
 initial conditions
 temperature constraint

Dynamic flexibility optimization results

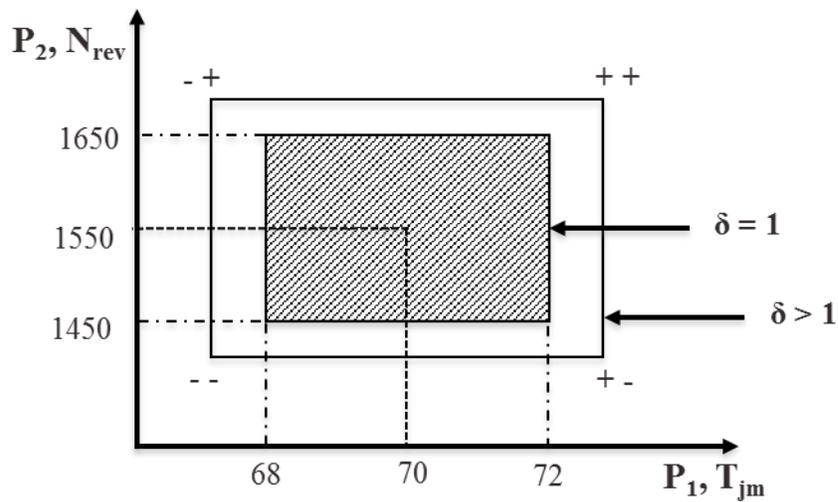


Figure V.22: Feasible region

The dynamic flexibility index for the uncontrolled case is obtained as 1.15 after optimization and 1.875 for the controlled case. The plot in Figure V.23 depicts the reactor temperature and product concentration profiles at the critical points for the controlled and uncontrolled cases. It is evident that the temperature constraints are satisfied. This type of information is useful to assess how farther one can stretch the operational region and still satisfy any product quality or safety constraints. The plot in Figure V.24 shows the required profile of the jacket flowrate for the system to operate feasibly at the critical point.

This type of analysis is useful to determine if there is a combination of events for uncertainty space considered, that can lead the system to any dangerous operating zones.

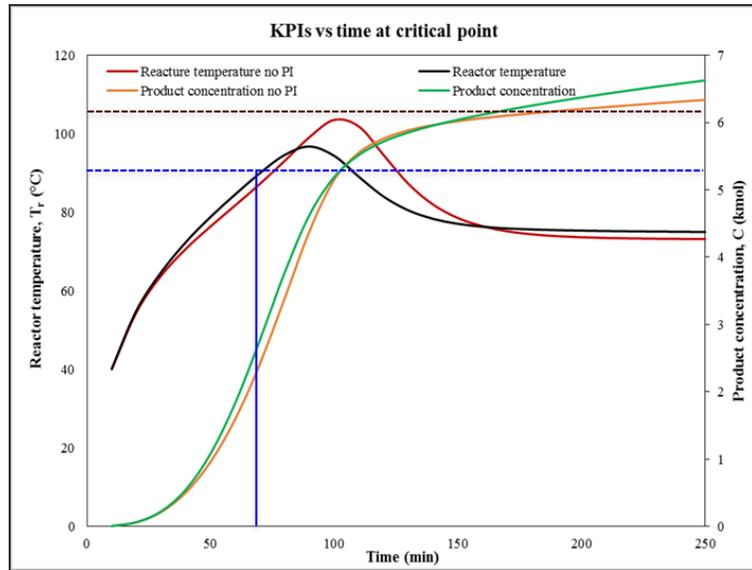


Figure V.23: KPIs vs time at critical point

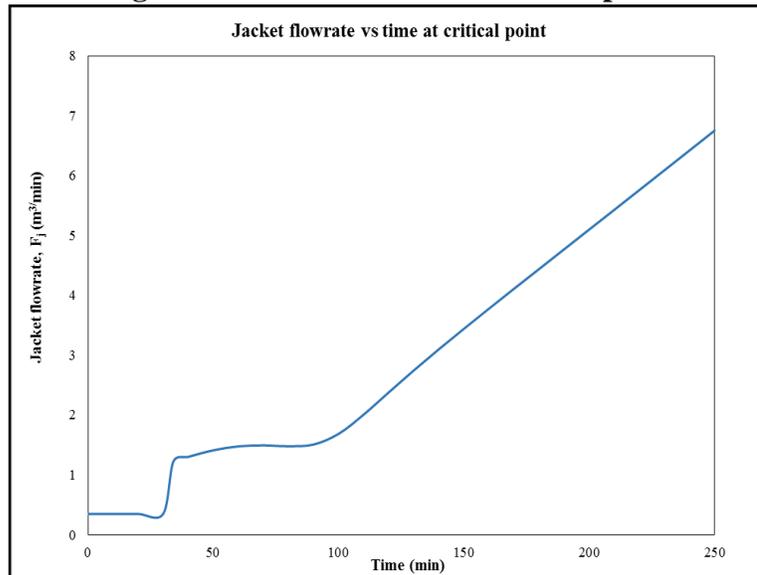


Figure V.24: Jacket flowrate vs time at critical point

The product concentration increases from 6.63 to 7.06 kmol for the optimized case and the profit increases from around 535 USD to 718 USD. Different objectives and

constraints can be set based on intended application such as product quality or specification.

5.5. Summary

With changing technology and increasing regulatory standards in process industries, process safety management and risk analysis have become challenging. There are uncertainties involved in the risk assessment of process systems operations due to exposure to expected or unexpected disturbances. In this chapter, an integrated resilience-based approach to manage uncertainties for predictability assessment of process-upset conditions and determination of feasible operational region has been conducted using plant performance data, sensitivity analysis, robust process simulation and optimization, and advanced statistical methods. The use of resilience metrics data in quantifying uncertainties, determining the maximum feasible operating region with maximum profit, and prediction of process upset event of high reactor temperature in the batch reactor process system has been demonstrated. The statistical models developed for three uncertainties - medium jacket temperature, agitator failure and reactants mischarging - are robust.

The major contribution of the proposed approach is the establishment of accurate and integrated method to predict process upset situations by virtue of a MCMC formulation, GSA, and flexibility optimization backed by process resilience concepts. Most of the existing risk assessment methods for failure rates use failure numbers from the historical databases that do not represent the true picture of the process system for which the risk assessment is being conducted. The proposed approach would enable the risk assessors to make risk decisions based on information of their process plant and hence

better allocate the resources towards improvement areas. The implementation of the developed models can (i) integrate the social factors analysis in a single approach, (ii) move from traditional point values for occurrence of loss of containment events (used in QRAs) to a range similar to the Probabilistic Risk Assessment (PRA) methods, and (iii) manage the uncertainties in the limited historical database on frequency or failure rates by using resilience metrics and thus incorporating the process plant performance data of the plant under study. This subsequently may increase safety, reliability, efficiency, and profitability of the process system.

The proposed method is easy to understand and implement in the real application to a process system. Some of the initial challenges that the team could face are – identification of the process operations data and choice of resilience metrics, data collection format, and data pre-processing.

Overall, this study strengthens the idea that with the PRAF approach incorporation of both technical and social aspects was achieved, which would help the risk assessor to make informed process design and operations decisions. This would lead to safer, reliable, efficient, and profitable process systems.

CHAPTER VI

QUANTITATIVE ASSESSMENT: SURVIVABILITY ANALYSIS*

In a process plant system, safe and reliable operations are highly sensitive to utilities such as power, steam, cooling water, nitrogen, and instrument air. These utilities play an important role or act as safety barriers. A disturbance in their supply is likely to affect process operations downstream, may reduce the production efficiency, and may lead to a sudden shutdown or contribute to an unsafe condition. The focus of this chapter is to introduce and evaluate a model for survival of a process system under upset conditions using the Process Resilience Analysis Framework (PRAF). Resilience metrics within a data-driven and model-based optimization approach using Bayesian regression are employed integrating both technical (process parameter variations) and social (human and organizational) factors. Based on an optimization objective function accounting for the overall system performance in terms of energy consumption, maintenance costs, safety impact, environmental impact, asset damage, and production loss, the proposed methodology aims to determine the optimal maintenance policy for optimal and safer plant operations. The implementation of the survival model within the PRAF is demonstrated on a cooling tower operation example problem, where optimal operation and maintenance (preventive, corrective, and predictive) strategies are determined based on trade-off analysis of process revenue, safety impact, and maintenance costs.

*Reprinted with permission from Jain, P., Pistikopoulos, E.N., & Mannan, M. S., "Process resilience analysis based data-driven maintenance optimization: application to cooling tower operations," *Computers & Chemical Engineering*, Vol 121, Pages 27-45. Copyright 2018 Elsevier Ltd.

6.1. Background

The complex socio-technical nature of process systems makes them vulnerable to process upset conditions or in the worst-case to catastrophic incidents^{337, 338}. There are several reasons that can be attributed to such upsets or catastrophic events⁸⁵. For example, mechanical failure³³⁹, instrument malfunction³⁴⁰, process hazards³⁴¹, organizational deficiency³⁴², poor alarm management¹⁶⁵, poor management systems, ineffective policies or regulations²⁹⁰, and human error³⁴³. When the system transitions to a process upset condition, various safety barriers in the plant can save the system from leading to the catastrophic incident state. A considerable amount of literature has been published on the inclusion of safety barriers in risk analysis^{344, 345}.

Many studies have noted that it is important to include human and organizational safety barriers to study their effect on the overall risk assessment of the complex socio-technical process system^{346, 347, 348, 282}. For example, ³⁴⁹ reports the symbolic barriers that pertain to the action by someone and are indirect in their nature. Some examples include instructions, procedures, and work permits. ³⁴⁷ formed an audit process for barrier management that consists of both hardware and behavioral elements. In addition, capability or functionality of safety barriers is critical to risk assessment, and this approach was utilized in the nuclear industry to carry out the operational decisions³⁵⁰. Furthermore, maintenance has been deemed vital for high performance and effectiveness of safety barriers³⁵¹.

In the process industry, with rapid advancements in technology and at the same time gradual system degradation, there prevails a continuous challenge to adapt to new

system configurations and maintain productivity. Furthermore, a balance between productivity, safety, and environmental performance for overall sustainability of the system is essential. Therefore, maintenance plays a critical role as a safety barrier in process system operations. In particular, the cooling tower provides cool process water for a wide range of applications for critical process operations. These processes are highly sensitive to the loss of cooling water. The poor performance of cooling towers may affect business and operations in various ways:

- (i) Process Safety: domino effects on downstream units that may contribute to fire/explosion leading to loss of human life and property damage
- (ii) Productivity: impaired performance, unplanned downtime, operations interruption, unplanned shutdown
- (iii) Business: high maintenance costs, production losses, increased capital equipment replacement
- (iv) Sustainability: financial losses, environmental degradation, long-term impact on reputation

Hence, an effective maintenance program is paramount for consistently obtaining the needed temperature and flowrate of cooling water. This supports safer downstream units and is important in maximizing the operating life of the cooling tower³⁵².

The Process Resilience Analysis Framework (PRAF) is an integrated, systems-based, quantitative, and data-driven methodology. It encompasses the whole anatomy of a process incident through the three-phase analysis of predictability, survivability, and recoverability. The PRAF application in the current study concentrates on surviving through upsets, incorporating process, maintenance, safety, and cost models. It features (i)

a process model that captures the details such as availability/operability of system equipment; (ii) a maintenance model that decides the maintenance action type based on data-driven analysis of frequency, downtime, and variability in equipment life; (iii) a safety model that takes into account the impact scenarios and respective losses through a system safety threshold; (iv) a cost and an expected revenue objective function, which examines the trade-off between safety, maintenance, and energy costs. The application of this method is demonstrated with an example of cooling tower operations. The major contributions of this work include:

- Definition of novel metric System Survivability Index, SSI that is incorporated as the system safety threshold to analyze the safety impact costs.
- Consideration of safety impact costs in the expected revenue objective function to assess the system effectiveness.
- Introduction of Resilience Survivability Index (RSI) metric to assess the system capacity to respond to process upset situations.
- Use of varying reliability or efficiency of the equipment in the process model.
- Incorporation of quantitative social metrics (human and organization related such as percentage of maintenance backlogs, percentage of required maintenance procedures reviewed or revised as scheduled, percentage of process safety required training sessions completed) in the analysis in addition to the technical factors.

The rest of the chapter is organized as follows. The maintenance policies are outlined in Section 6.2. Section 6.3 provides the details of the problem formulation and the general methodology for survivability assessment. Section 6.4 gives the complete analysis and detailed algorithms using an application example of cooling tower operations. Section 6.5 discusses the results of this work and conclusions are made in Section 6.6.

6.2. Maintenance policies

The maintenance policies in a plant are usually divided into the following three main types^{353, 354}:

(i) Preventive maintenance (PM): covers all maintenance tasks that are pre-planned with the purpose to maintain equipment in a satisfactory working condition. These tasks are periodic inspection, detection of any minor faults, and reconditioning whenever demanded.

(ii) Corrective maintenance CM: refers to maintenance action(s) to restore equipment to an operating state when a failure is noted.

(iii) Predictive maintenance (PdM): includes scheduling and performing maintenance tasks based on the condition of the equipment to predict any failure scenarios.

Maintenance scheduling and analysis have been investigated by many researchers using various methods such as statistical methods – Bayesian analysis, Markov models, Monte Carlo simulation; data-driven methods – Artificial Neural Network, Predictive models; and optimization methods – Genetic Algorithms, Optimization under uncertainty. An indicative list of works on maintenance optimization is summarized in Table VI.1.

Table VI.1: An indicative list of works on maintenance optimization

Authors (year)	Contribution
355	Overview and analysis of maintenance optimization models
356	General framework for preventive maintenance optimization combining Monte Carlo simulation with a genetic algorithm.
357, 358, 359	Integrated maintenance optimization model for optimal life cycle process design and maintenance scheduling under uncertainty.
360	Condition-based maintenance decisions optimization model for asset management.
328	Multi-objective optimization to determine the optimal on-condition maintenance strategy.
361	Simultaneous optimization framework for optimal allocation of reliability for multipurpose process plants at the design stage.
362	PM costing framework: an effective tool for cost assignment and tracking cost efficiency.
363	Optimal inspection frequency model.
364	Monte Carlo simulation-based maintenance model that includes imperfect maintenance and detailed spare parts policy.

Some of the gaps from these methods when looking at the safety and resilience of the process system are identified below:

- What is the influence of social (human/organizational) factors such as spare parts management policy, operators' training on maintenance procedures, and maintenance backlogs on the maintenance policies?
- How do the safety impact costs influence the overall profitability and sustainability of the process system?

- How does the system reliability and maintenance policy change when system effectiveness is the top requirement based on system safety thresholds (explained in Section 6.3)?

6.3. Survivability assessment: model development

The primary objective of the survivability assessment is to prevent the escalation of the process-upset situation to the catastrophic incident state. A plant may transition from process upset to a catastrophic state owing to propagation events such as poor performance of safeguards, unavailability of barriers, low reliability of safeguard equipment, and poor maintenance. In the scenario analysis, various propagation events are identified for the process system under analysis to aid further in the model development. The safeguard analysis step relates to the process system safeguards performance assessment considering both technical and social aspects. For the current application example, it is the data-driven analysis of reliability, availability, and maintenance of the cooling tower system by carrying out frequency, downtime and variability in equipment life assessment. The results of this data-driven approach provide useful quantitative information that is subsequently used to select the maintenance action type of preventive (PM), corrective CM, and predictive maintenance (PdM). This further improves the system effectiveness in terms of reliability, maintenance, safety, and profitability. Figure VI.1 represents the overview of survivability assessment.

6.3.1. Process model

The integrated optimization problem addressed in this chapter can be defined as follows:

Problem definition: The aim is to achieve optimal and safer plant operations, without catastrophic incidents and maximum profit, where role of safeguards can be incorporated in the analysis of process upset situations. Currently, safety impact cost is not considered in the analysis of process upset situations. Currently, safety impact cost is not considered in the process system upset analysis and the safeguard analysis is limited to historical data (only on technical aspects) rather than actual plant performance data. If these aspects are ignored, process systems may escalate to catastrophic situations, and more resources will be required to handle the cascading problems. These catastrophic situations could result in loss of production, bad reputation, financial losses, and business interruption. PRAF methodology is used in evaluating the survival of process systems by incorporating safeguard performance analysis, and safety impact cost in terms of system safety threshold. For this research, amongst the various safeguards, the focus is on the maintenance as an effective safeguard to prevent the acceleration of a total failure of the process system.

Given: process model, system equipment configuration, cost data, maintenance data, safety scenarios, a cost/revenue function describing the relation between equipment reliability, equipment maintenance cost, and safety impact costs,

To determine: optimal system reliability that maximizes the expected revenue and system effectiveness accounting for capital, operations, maintenance, and safety impact costs. This problem can be mathematically written as problem P as follows,

$\min_{z_s, x_s, \eta_s} TAC_s(z_s, x_s, \eta_s) \quad \text{and} \quad \max_{z_s, x_s, \eta_s} EPR_s(z_s, x_s, \eta_s) \quad (6.1)$
<p>s.t.</p>
$h_s(z_s, x_s, \eta_s) = 0 \quad (6.2) \quad (P)$
$g_s(z_s, x_s, \eta_s) \leq 0 \quad (6.3)$

where each operable system state s is described by a different set of equality (h_s) and inequality constraints (g_s), η_s is a vector describing the efficiency of the equipment that depends on the reliability, z_s is a vector of degrees of freedom specified in Z that are manipulated to achieve minimum total annualized cost and maximum expected revenue, x_s is the vector of process variables specified in X , TAC is the total annualized cost, and EPR is the expected process revenue. The solution to the above optimization problem P can be obtained using solvers available with the GAMS modeling language³⁶⁵.

The complete problem is solved as below in two stages,

- Stage 1: is focused on the solution of process model to obtain process data (such as flowrate, temperature) to calculate the System Survivability Index, SSI and also optimize for the minimal total annualized cost, TAC.
- Stage 2: after obtaining the data, SSI is calculated and is used as the system safety threshold in the safety model jointly with the process model and input from the data-driven maintenance model to obtain the maximum expected revenue, system reliability, and maintenance policy.

The process model is formulated from the first principles expressions for mass and energy balance. The process data is obtained from process simulation to calculate the system safety threshold at the minimum annualized cost. In the conventional method of problem formulation, the equipment efficiencies and reliability are considered constant. However, in practice, equipment failure, unplanned shutdown, unplanned downtime, and reduced equipment efficiency have a significant impact on safety and productivity. Therefore, these should be recognized while assessing the system effectiveness or process

system survivability index. Hence, in this work, equations relating to the reliability and efficiency of equipment are added to the process model by using η_s .

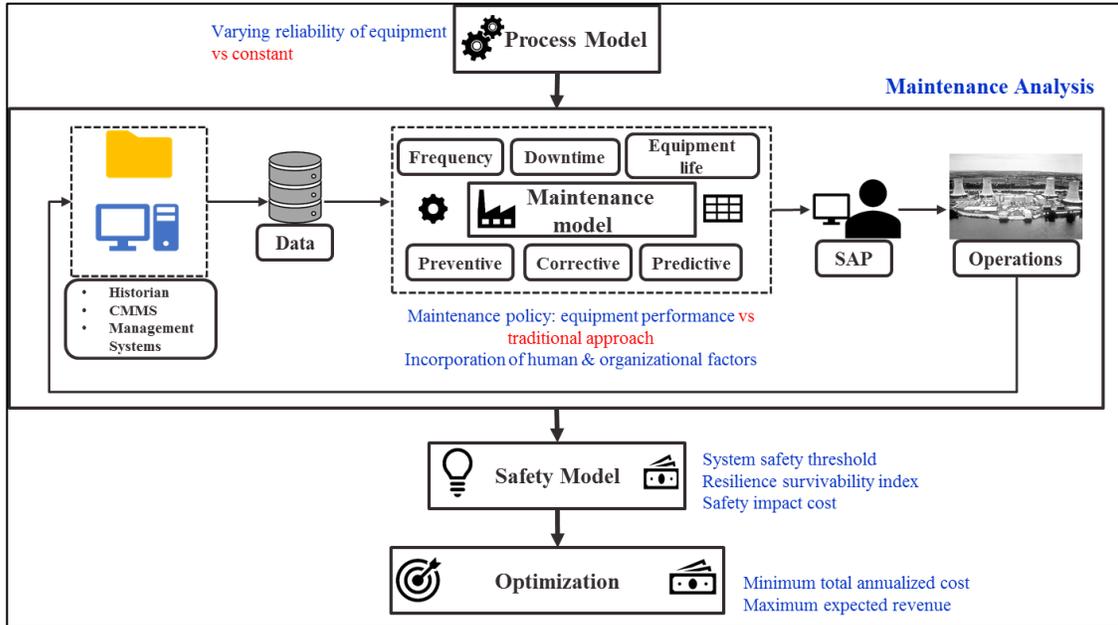


Figure VI.1: Survivability assessment methodology

6.3.2. Maintenance model

Maintenance action selection

Three types of maintenance alternatives preventive (PM), corrective CM, and predictive (PdM) as defined in Section 6.2 are studied. Three important variables of frequency, downtime, and equipment life are considered as an input to select the maintenance action alternative. Figure VI.2 demonstrates the model for maintenance action selection from preventive, corrective, and predictive maintenance.

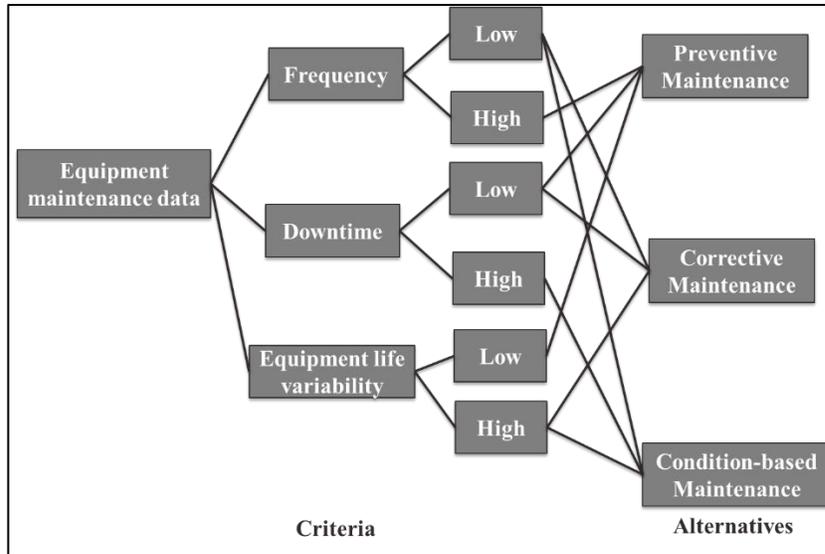


Figure VI.2: Model for maintenance action selection

Table VI.2 presents the ground truth based on the values of three factors frequency, downtime, and variability of equipment life to decide the maintenance action alternative. For the cases other than those included in the ground truth, cost values of the action type are considered to determine the alternative. The generic algorithm to select the maintenance action alternative is outlined in Appendix D. The overall system reliability for different states is calculated based on system reliability concepts of series or parallel configurations (See Appendix D) and system availability/operability (See Appendix D).

Table VI.2: Maintenance action analysis (ground truth)

Maintenance Action	Frequency (# of failures per unit time)	Downtime (hours)	Variability of equipment life (years)
Preventive maintenance (PM)	High	Low	Low
Corrective maintenance ⁷	Low	Low	High
Predictive maintenance (PdM)	Low	High	High

Data-driven maintenance model

For the method developed in this research, the models for three variables – frequency, downtime, and equipment life variability are expressed covering the plant maintenance and resilience metrics data. Using the PRAF methodology, information from plant data in way of resilience metrics is utilized in the selection of the maintenance alternative. The resilience metrics including both technical and social aspects incorporate plant data from the historian, Central Maintenance Management System (CMMS), the PSM system, and others¹⁶⁴. Table VI.3 lists the resilience metrics used in this work with their weights³³⁵.

Table VI.3: Resilience metrics for maintenance model

Resilience Metrics	Weights
Number of unplanned maintenance jobs	0.79
Rotatory equipment pieces vibration/voltage rating/impeller speed	0.87
Management response to the inspection findings of safety critical equipment (SCE) deficiency (spare parts)	1
% of maintenance backlogs	0.81
% of required maintenance procedures reviewed or revised as scheduled	0.81
% of process safety required training sessions completed	0.81

A regression method ³⁶⁶ as illustrated in Figure VI.3 is utilized applying the Bayes concept. Models for three factors – frequency, downtime, and equipment life variability are expressed covering the plant maintenance and resilience metrics data.

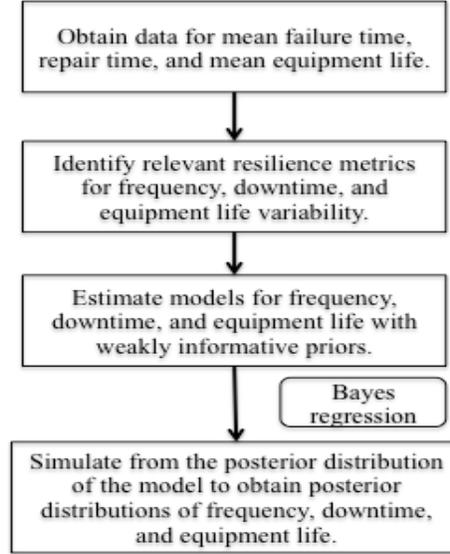


Figure VI.3: Methodology for data-driven maintenance model

The models for frequency, downtime, and equipment life (y_i) are formulated in the following form,

$$y_i = x_i' \beta \quad (6.4)$$

where x_{is} are the various weighted resilience metrics.

We assume standard, semi-conjugate priors:

$$\beta \sim N(b_0, B_0^{-1}) \quad (6.5)$$

where β is assumed *a priori* independent. Note that only starting values for β are allowed because the simulation is done using Gibbs sampling with the conditional error variance as the first block in the sampler.

The estimate at a new time point is given by the following equation,

$$\hat{y}_{i,t+1} = x_{i,t+1}' \hat{\beta}_{post.mean} \quad (6.6)$$

6.3.3. Safety model

The safety impact cost depends on the loss function based on the system safety threshold in terms of the type of incident (Tier 1 or Tier 2). Tier 1 and Tier 2 incidents are differentiated based on the level of consequence. Tier 1 is of greater consequence and Tier 2 is of lesser consequence. For more details refer to API RP 754¹⁶⁹. The four types of loss categories considered owing to these incidents are safety injuries/fatalities (S), environmental damage (E), asset damage (A), and production loss (L). The impact costs due to Tier 1 type incident scenario are denoted by S1, A1, E1, L1 and S2, A2, E2, L2 for Tier 2 type incident scenario.

System Survivability Index

In order to analyze the influence of safety on the system effectiveness in terms of overall profitability, a novel metric System Survivability Index, SSI is defined. The SSI is a dimensionless index and is interpreted as the ratio of the actual system effectiveness, SE_a to the required system effectiveness, SE_r

$$SSI = \frac{SE_a}{SE_r} \quad (6.7)$$

System effectiveness is a function of process parameters and equipment characteristics and can be defined for various process systems. The actual system effectiveness is determined from the process model simulation and optimization for the minimum total annualized cost. The required system effectiveness is calculated based on the threshold specifications based on the safety scenarios for the process system under study.

Additionally, another metric called the Resilience Survivability Index (RSI) for the process system is measured as part of the result from this work and is as follows,

$$RSI = \frac{SSI * ER}{\max ER} \quad (6.8)$$

where ER is the expected revenue of the system defined by eqn. (6.11).

This metric measures the system capacity to respond to process upset situations. A higher value of RSI implies better system capacity to respond to process upset situations and a lower value of RSI means poor system capacity to respond or survive through process upset situations.

6.3.4. Cost/revenue model

The objective is to minimize the total annualized cost TAC and maximize the expected revenue for the process system. This cost/revenue function comprises different elements – capital cost, operating cost, product revenue, the energy cost of mechanical equipment (*e.g.* pumps and fan), maintenance cost, and safety impact cost.

Total Annualized Cost

The total annualized cost TAC is calculated as follows,

$$TAC = K_f C_{cap} + C_{op} \quad (6.9)$$

where C_{cap} is the annualized capital cost, C_{op} is the annual operating costs, and K_f is the annualized factor for investment.

Revenue

The expected process revenue (EPR) is calculated as follows,

$$EPR = PR - E_c - M_{cost,system} - SI_{cost} \quad (6.10)$$

where PR is the product revenue, E_c is the energy cost; $M_{cost,system}$ is the annual maintenance cost for the whole system; and SI_{cost} is the safety impact cost.

The expected revenue is calculated as follows,

$$ER = \sum p_s (EPR) \quad (6.11)$$

the expected revenue (ER) of the system is given as the weighted sum of the expected process revenue of each system state using as weights the probability of the system is in each particular state. The state probabilities p_s are a function of the reliability and maintenance characteristics of the process equipment.

Product revenue

$$PR = C_p - C_{rm} \quad (6.12)$$

where C_p is the cost of products and C_{rm} is the cost to make the products.

Energy costs

The energy cost for equipment (n) in the process system is calculated using the following equation,

$$E_c = c_e * \sum_{m=1}^n P_n \quad (6.13)$$

where c_e is the cost coefficient of electricity (US\$/kWh); P_n is the power for the equipment (kWh).

Maintenance costs

The maintenance cost is included in the objective function as follows,

$$M_{cost,system} = H * [\sum_{i=1}^j (C_{insp,j} + MA_{cost,j})] \quad (6.14)$$

where H is the number of hours of operations in a year; $M_{cost,system}$ is the annual maintenance cost for the whole system; and $C_{insp,j}$ is the inspection cost of unit j ; $MA_{cost,j}$ is the maintenance cost of unit j that depends on the maintenance action type (preventive, corrective, or predictive analyzed from the data-driven maintenance model).

Safety costs

The safety impact costs for different scenarios and loss categories are incorporated in the objective function depending on the system survivability index (described in Section 6.3) as below,

$$SI_{\text{cost}} = H * (1 - SSI) * \sum_{k=1}^n DC_k \quad (6.15)$$

where SI_{cost} is the safety impact cost; and SSI is the system survivability index (described in Section 6.3); DC_k is the damage cost that depends on the various loss categories based on the safety impact scenarios mentioned in Section 6.3.

6.4. Application to the cooling tower operations

6.4.1. System and process description

This section provides an example of the process system to demonstrate the survivability assessment methodology. The process system is a cooling tower operation with a fan and a network of three pumps supplying cooling water to two downstream units – batch reactor and distillation column. Figure VI.4 is a schematic depicting the equipment configuration for this process system. This is a counter flow induced draft cooling tower. In this type of design, the air flows vertically upwards, directly opposite to the flow of water or counter to the current as the hot water flows downwards. For the induced-draft design, there is a fan mounted on the top of the cooling tower that pulls the air through the fill media. The cold water is pumped from the cooling tower basin to the downstream units. This cold water absorbs heat from the hot process streams and the warm water circulates back to the top of the cooling tower.

The complete step-wise methodology applied to cooling tower and downstream process system is shown in Figure VI.5. Maintenance has been considered as one of the essential factors affecting life and energy efficient operation of the cooling tower³⁶⁷. In the

cooling tower process system, there are three primary system states: normal operation, process-upset event, and catastrophic state. The literature on maintenance issues of cooling tower components resulting in poor performance has highlighted several causes^{352, 368, 369}. In the cooling tower example, the purpose is to prevent the catastrophic incident at downstream units by avoiding complete loss of cooling water supply. Poor or degraded performance of cooling towers is typically attributed to factors such as failure of the gearbox, bearings, motor, driveshaft; blockage and fouling of piping; corrosion; or uneven water distribution. Hence, the propagation events PE1, PE2, PE3, PE4 - poor pump performance, damaged fan blades, scale deposition, and clogged spray nozzles are selected for this study. These relate closely to the reliability and maintenance of cooling tower system components and hence maintenance has been used as the critical safeguard for this study and the model analysis.

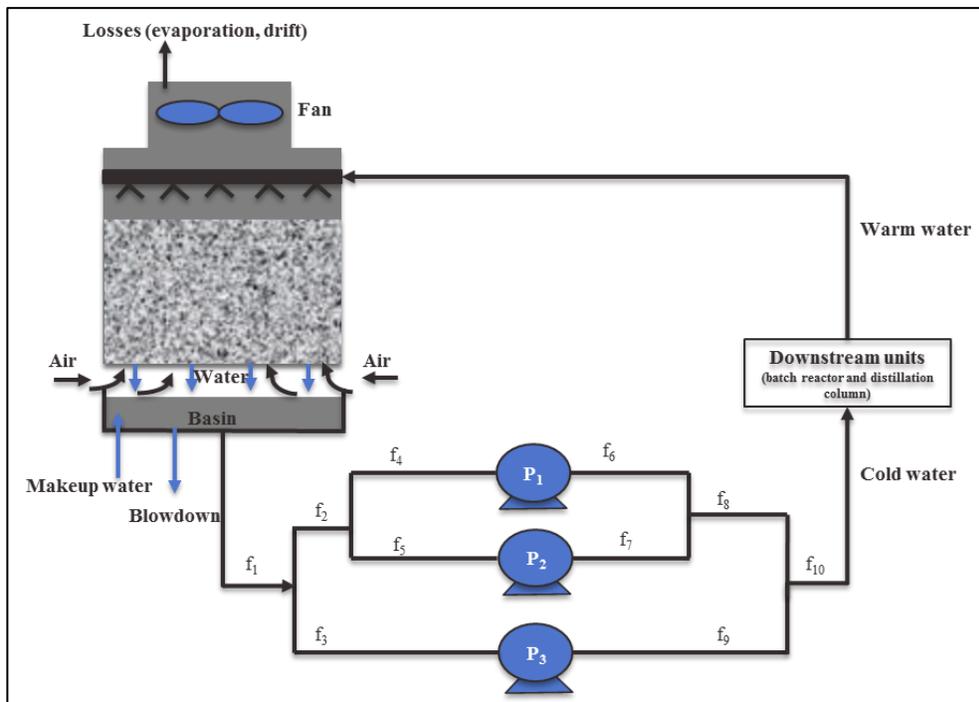


Figure VI.4: Cooling tower operations process system

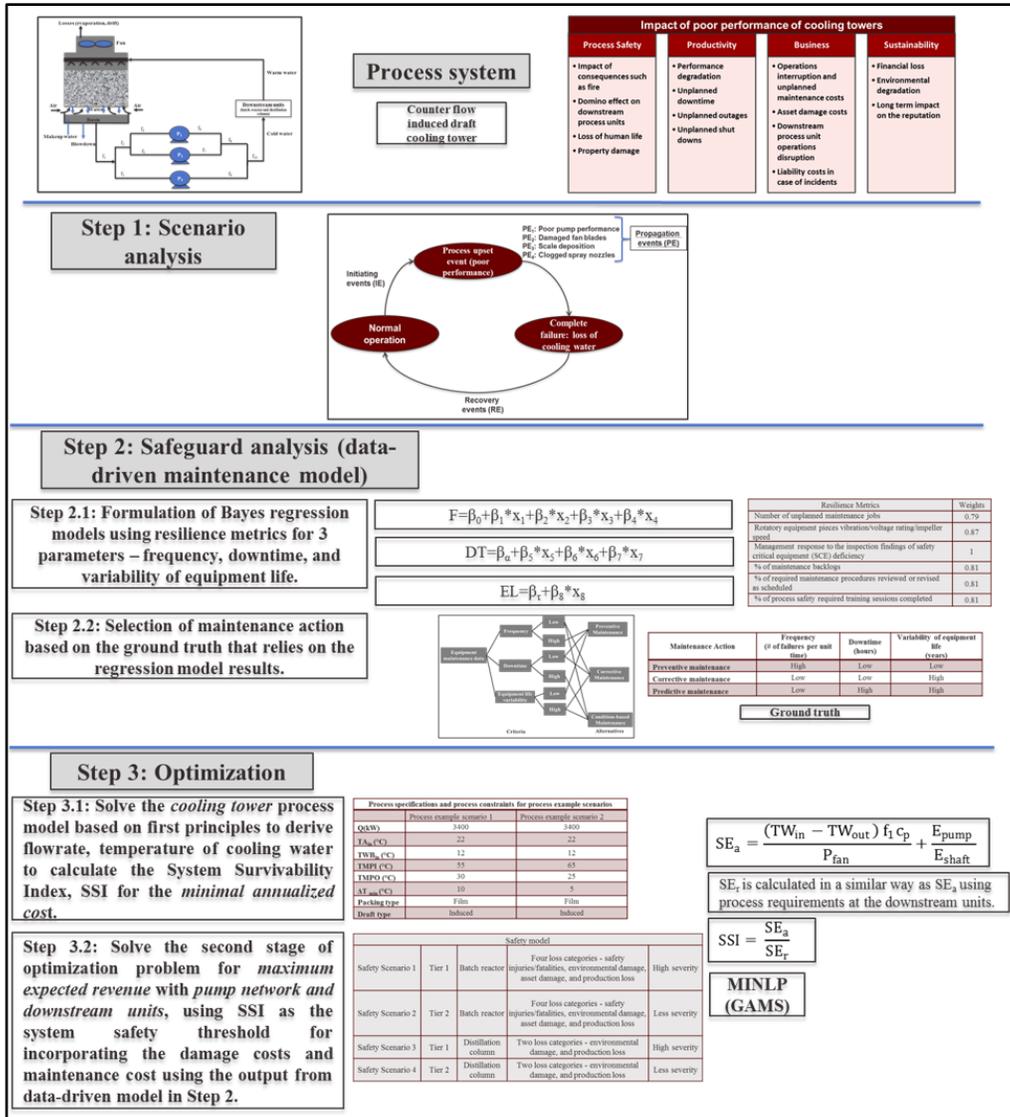


Figure VI.5: Survivability assessment methodology: cooling tower operations

6.4.2. Process model

A schematic representation of the general arrangement of the counter-flow cooling tower is exhibited in Figure VI.4 and the underlying equations presented in Appendix E.

In order to combine reliability and maintenance aspects, fan efficiency equation has been added to this model. This is determined by the overall equipment effectiveness³⁷⁰, which is a product of availability, performance, and quality. The availability of the fan is

assumed as one, performance is defined as the ratio of actual air flowrate to ideal air flowrate (0.75) and quality is considered as the reliability. It can be mathematically written as,

$$\eta_{fan} = 0.75 * R_{fan} \quad (6.16)$$

From Figure VI.4, for the pump network system, a pump can be either available or unavailable in the time horizon of operation. Therefore, the status of a pump is specified by a binary parameter ω_j^s .

$$\omega_j^s = \begin{cases} 1 & \text{if pump } j \text{ is available} \\ 0 & \text{if pump } j \text{ is unavailable} \end{cases} \quad (6.17)$$

where, $\omega_j^s = (\omega_1^s, \omega_2^s, \omega_3^s)$ is the state vector of this pump network system.

The pump network with three pumps involves a total of $2^3 = 8$ states in which the system may reside with possible degradation, failure, or availability of the pump. The states of the pump network system are classified as structurally available/operable or unavailable/inoperable as shown in Appendix D. Equations (6.18) to (6.27) based on concepts from ³⁷¹ describe all the eight states in which the system may reside by adjusting the values of the binary parameters ω_j^s according to whether pump j is available or not in the system state s . f represents the flowrates through the pumps and η_j , pc_j , are the efficiencies and capacities of each pump, respectively.

$$f_1 = f_2 + f_3 \quad (6.18)$$

$$f_2 = f_4 + f_5 \quad (6.19)$$

$$f_8 = f_6 + f_7 \quad (6.20)$$

$$f_{10} = f_8 + f_9 \quad (6.21)$$

$$f_9 = \eta_{p3} * f_3 \quad (6.22)$$

$$f_6 = \eta_{p1} * f_4 \quad (6.23)$$

$$f_7 = \eta_{p2} * f_5 \quad (6.24)$$

$$f_4 \leq pc_1 * \omega_1^s \quad (6.25)$$

$$f_5 \leq pc_2 * \omega_2^s \quad (6.26)$$

$$f_3 \leq pc_3 * \omega_3^s \quad (6.27)$$

Table VI.4 presents the process specifications and process constraints for the two example process scenarios considered in the case study. For both the examples, cooling tower was required to remove 3400 kW of heat load at an ambient air pressure. For both the example process scenarios, film packing is used as the selected type of filling material as it provides the best combination of heat transfer and pressure losses so that the lowest total annual cost is obtained. Additionally, the draft type was chosen as the induced draft.

In the first stage of the optimization problem, only cooling tower i.e. excluding the pump network and the downstream units is considered in the system boundary. The objective function involves the minimization of the total annual cost, TAC,

$$\text{minimize TAC} = K_f C_{\text{cap}} + C_{\text{op}} \quad (6.28)$$

where C_{cap} , C_{op} , K_f are described in Section 6.4.

Table VI.4: Process specifications of process example scenarios

Process specifications and process constraints for process example scenarios		
	Process example scenario 1	Process example scenario 2
Heat load, Q^{257}	3400	3400
Dry-bulb temperature of the air at tower inlet, TA_{in} (°C)	22	22
Wet-bulb temperature of the air at tower inlet, TWB_{in} (°C)	12	12
Minimum process inlet temperature, $TMPI$ (°C)	55	65
Minimum process outlet temperature, $TMPO$ (°C)	30	25
Minimum allowable temperature difference, ΔT_{min} (°C)	10	5

This cooling tower MINLP model is presented in Appendix E and can be solved using the BARON³⁷² or ANTIGONE³⁷³ solvers available with the GAMS modeling language³⁶⁵. For this work, ANTIGONE solver was used to obtain the solution. The solution from stage 1 of the optimization problem stated above gives the process data such as flowrate and temperature at the minimum TAC. This data is used to calculate the SSI, which is used as a system safety threshold in the second optimization problem. Here, the system includes the pump network and the two downstream units. The objective function is below,

$$\text{maximize } \text{EPR} = \text{PR} - E_c - M_{\text{cost,system}} - \text{SI}_{\text{cost}} \quad (6.30)$$

where PR, E_c , $M_{\text{cost,system}}$, and SI_{cost} are described in Section 6.4.

6.4.3. Maintenance model (Safeguard analysis)

Frequency analysis

For the frequency analysis, the failure rate captured from the data is augmented using the following metrics that authors identified and included them as covariates: weighted 24-h rolling vibration mean (x_1), weighted 24-h rolling voltage mean (x_2), weighted number of unplanned maintenance jobs (x_3), and weighted percentage of maintenance backlogs (x_4). The model estimated is:

$$F = \beta_0 + \beta_1 * x_1 + \beta_2 * x_2 + \beta_3 * x_3 + \beta_4 * x_4 \quad (6.31)$$

Downtime analysis

For the downtime analysis, the repair time captured from the data is augmented using the following metrics that authors identified and included them as covariates: weighted percentage of SCE inspections findings managed consistent with company expectations based on the management response (x_5), weighted percentage of required

maintenance procedures reviewed or revised as scheduled (x_6), weighted percentage of process safety required training sessions completed (x_7). The model estimated is:

$$DT = \beta_0 + \beta_5 * x_5 + \beta_6 * x_6 + \beta_7 * x_7 \quad (6.32)$$

Equipment life analysis

For the equipment life analysis, the variability in equipment life captured from the data is augmented using the following metric that authors identified and included it as a covariate: weighted 24-h rolling impeller speed means (x_8). The model estimated is:

$$EL = \beta_r + \beta_8 * x_8 \quad (6.33)$$

For this purpose, synthetic dataset containing 8760 data points over one year was generated. Figure VI.6 shows a snapshot of the final extracted features file for the frequency model. The model identification was done using the Monte Carlo Markov Chain regression method to find the coefficients or the β_i values. All analysis was conducted in the programming language R¹⁸⁴.

	DateandTime	Voltmean24	Vibmean24	No_unplannedmaint	Percentage_maintbacklogs
1	1/2/16 0:00	217.958	2.465	0	0.24
2	1/2/16 3:00	218.000	2.475	0	0.00
3	1/2/16 6:00	218.708	2.471	0	0.00
4	1/2/16 9:00	219.250	2.461	0	0.00
5	1/2/16 12:00	220.167	2.470	0	0.00
6	1/2/16 15:00	219.500	2.469	0	0.00

Figure VI.6: Extracted features snapshot

The methods and diagnostics tests used in this study to assess convergence are:

- Trace plots: plot (), these are plots of the sampled parameter values versus the iteration number. It is good convergence if the lines are ‘wiggly’.
- Autocorrelation plots: acf (), these are used to determine the correlation between the values. It is a good sign if the correlation plots decay rapidly.

- Heidelberg-Welch diagnostic: heidel.diag (), the null hypothesis that the sampled values come from a stationary distribution is tested using the Cramer-von-Mises statistic.

6.4.4. Safety Model

Safety Scenario 1

The temperature control of a batch reactor is critical to the safe operation and product quality. In this scenario, the downstream unit is a batch reactor, where the supply of cooling water is safety critical as it maintains the jacket temperature of the reactor. When the cooling water supply is disrupted or not adequate or not temperature controlled, it can lead to runaway reaction situation leading to disastrous consequences such as fire, explosion *etc.* This would result in consequences in all four loss categories - safety injuries/fatalities, environmental damage, asset damage, and production loss.

Safety Scenario 2

This scenario is same as the Safety Scenario 1 where the downstream unit is a batch reactor. The only difference is in the severity of consequences as this is a Tier 2 type incident scenario.

Safety Scenario 3

The downstream unit, distillation column, in this case, requires the cooling water at a specific temperature and flowrate for overhead vapor condensation. In case of absence of cooling water at the required specifications, there will be a buildup of overhead vapors in the column. This would lead to relief through pressure safety valve to the flare system. There would be consequences in two loss categories – environmental damage, and the

production loss. The Safety Scenario 3 has been considered as more severe and hence Tier type 1 incident in the analysis.

Safety Scenario 4

This scenario is same as the Safety Scenario 3 where the downstream unit is a distillation column. The only difference is in the severity of consequences as this is a Tier 2 type incident scenario.

The required water mass flowrate and outlet water temperature for these four safety scenarios are taken as 30kg/s and 25°C.

System Survivability Index

The System Survivability Index is a dimensionless index and is defined in Section 6.3. For the cooling tower operations, the system effectiveness is described as the cooling capability in terms of energy consumption. For current work, the cooling capability index³⁷⁴ is modified to include pump network. Therefore, it is a function of outlet water temperature of the cooling tower, water mass flowrate to the pump network, and the product flowrate of the cooling tower to the downstream units. It is expressed mathematically as follows,

$$SE_a = \frac{(TW_{in} - TW_{out}) f_1 c_p}{P_{fan}} + \frac{E_{pump}}{E_{shaft}} \quad (6.34)$$

The overall pump network efficiency is the ratio of the energy delivered by the pump to the energy supplied to the pump shaft(s), which is a function of f_{10} (output flowrate from pump network to downstream units). TW_{in} is the water temperature at the tower inlet, TW_{out} is the water temperature at the tower outlet, f_1 is the input flowrate to the pump network, P_{fan} is the electric power of the fan, and c_p is the specific heat. The

required system effectiveness, SE_r is evaluated based on the four different safety scenarios and the requirements as provided in this section.

6.4.5. Cost/revenue model

The cost values of various safety loss categories, maintenance activities, and process operations used in the example case study are listed in Appendix F. Different safety impact scenarios have been considered as described in Section 6.3. In addition, different cost structures of corrective and predictive maintenance, CCM/CPdM are employed in the study.

6.5. Results and Discussion

The results for the two example process scenarios for the first optimization problem are presented in Table VI.5. It is noticeable from the results that tower approach increases with the decrease in ΔT_{min} . In addition, for both the process example scenarios, with the decline in reliability of the fan, more power is consumed in order to maintain the flowrate and the outlet temperature of the tower. This results in an increase in the operation cost and hence an increase in the total annualized cost of the tower.

Table VI.5: Optimization results

Optimization results								
	Process example scenario 1				Process example scenario 2			
Reliability of fan, η_{fan}	0.68	0.63	0.53	0.50	0.68	0.63	0.53	0.50
Mass flow rate of water, m_w (kg/s)	32.74	32.88	33.14	33.28	33.84	34.56	35.31	36.91
Water temperature at tower outlet, TW_{out} (°C)	20.2	20.3	20.5	20.6	26	26.5	27	28

Table VI.5: Continued
Optimization results

Optimization results								
	Process example scenario 1				Process example scenario 2			
Water temperature at tower inlet, TW_{in} (°C)	45	45	45	45	50	50	50	50
Electric power of fan, P_{fan}^{257}	74.5	79.8	95.8	100.2	23.3	24.9	29.9	31.3
Range (°C)	24.8	24.7	24.5	24.4	24	23.5	23	22
Approach (°C)	8.2	8.3	8.5	8.6	14	14.5	15	16
Total Annualized Cost (USD)	95570	99424	110834	113988	58807	60399	64327	66316

6.5.1. System reliability

The overall system reliability for different states as shown in Table VI.6 is calculated based on system availability/operability. The system availability/operability as reported before in this example case study depends on the pump network with three pumps.

Table VI.6: System reliability for different scenarios

		Reliability	System reliability (s1)	System reliability (s2)	System reliability (s3)	System reliability (s4)	System reliability (s5)	System reliability (s6)	System reliability (s7)
Reliability Scenario 1	P1	0.65	0.666	0.657	0.646	0.626	0.599	0.543	0.437
	P2	0.81							
	P3	0.89							
	F	0.67							
Reliability Scenario 2	P1	0.78	0.898	0.887	0.871	0.845	0.809	0.733	0.590
	P2	0.66							
	P3	0.39							
	F	0.90							
Reliability Scenario 3	P1	0.54	0.829	0.818	0.804	0.780	0.746	0.677	0.544
	P2	0.86							
	P3	0.81							
	F	0.84							
Reliability Scenario 4	P1	0.84	0.693	0.684	0.672	0.652	0.624	0.566	0.455
	P2	0.43							
	P3	0.61							
	F	0.70							

The reliability of the system is plotted against time over the maintenance horizon of one year for each system state as exhibited in Figure VI.7. The reliability of the system decreases with time. Furthermore, it is evident from the plot that the system reliability has a steeper decrease for system state 7 as compared to system state 1.

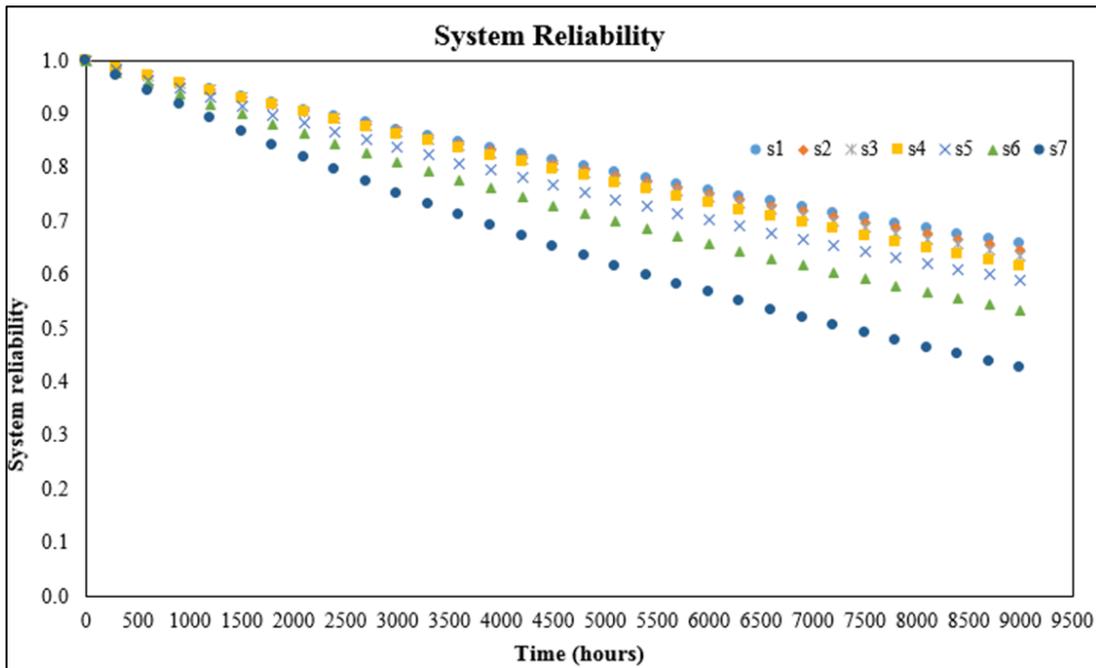


Figure VI.7: System reliability for different states

6.5.2. Maintenance action analysis

Data-driven maintenance model

It is necessary to examine some diagnostics to assess whether the Markov chain has converged to its stationary distribution. The trace and density and autocorrelation plots are illustrated in Figures VI.8 and VI.9 respectively. It is evident that there is convergence as the trace plots are wiggly and the autocorrelation plots decay rapidly. Heidelberg-Welch convergence diagnostic test was implemented in the coda package³⁷⁵ and the results were checked before using the posterior density sample for inference. All variables passed the

Heidelberg-Welch convergence test and the margin of error was found to be less than 0.1 for all cases. This result reinforces the conclusions made from the trace and autocorrelation plots.

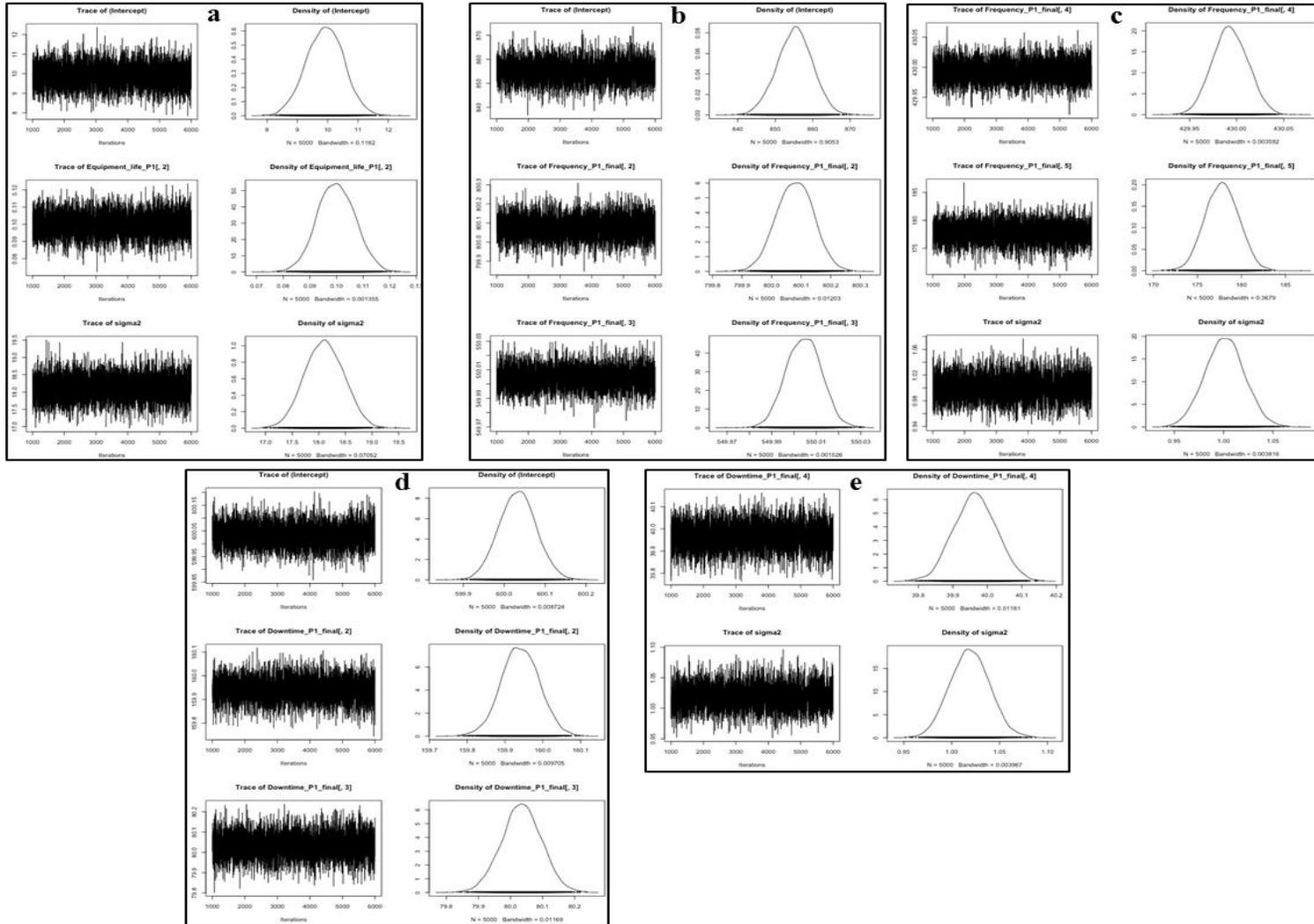


Figure VI.8: Trace and density plots for coefficients for pump 1: a – Equipment life; b,c – Frequency; d,e – Downtime

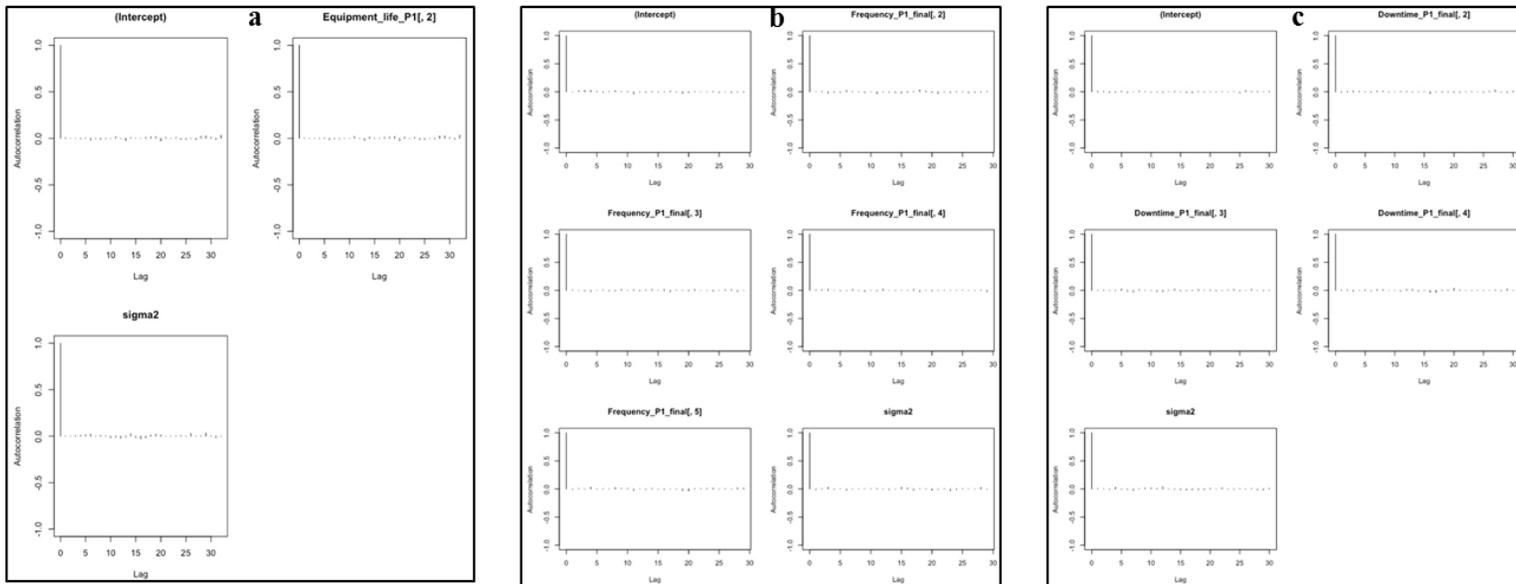


Figure VI.9: Autocorrelation plots for pump 1: a – Equipment life; b – Frequency; c – Downtime

The posterior probability density functions for equipment life, frequency, and downtime for all three pumps are represented in Figure VI.10.

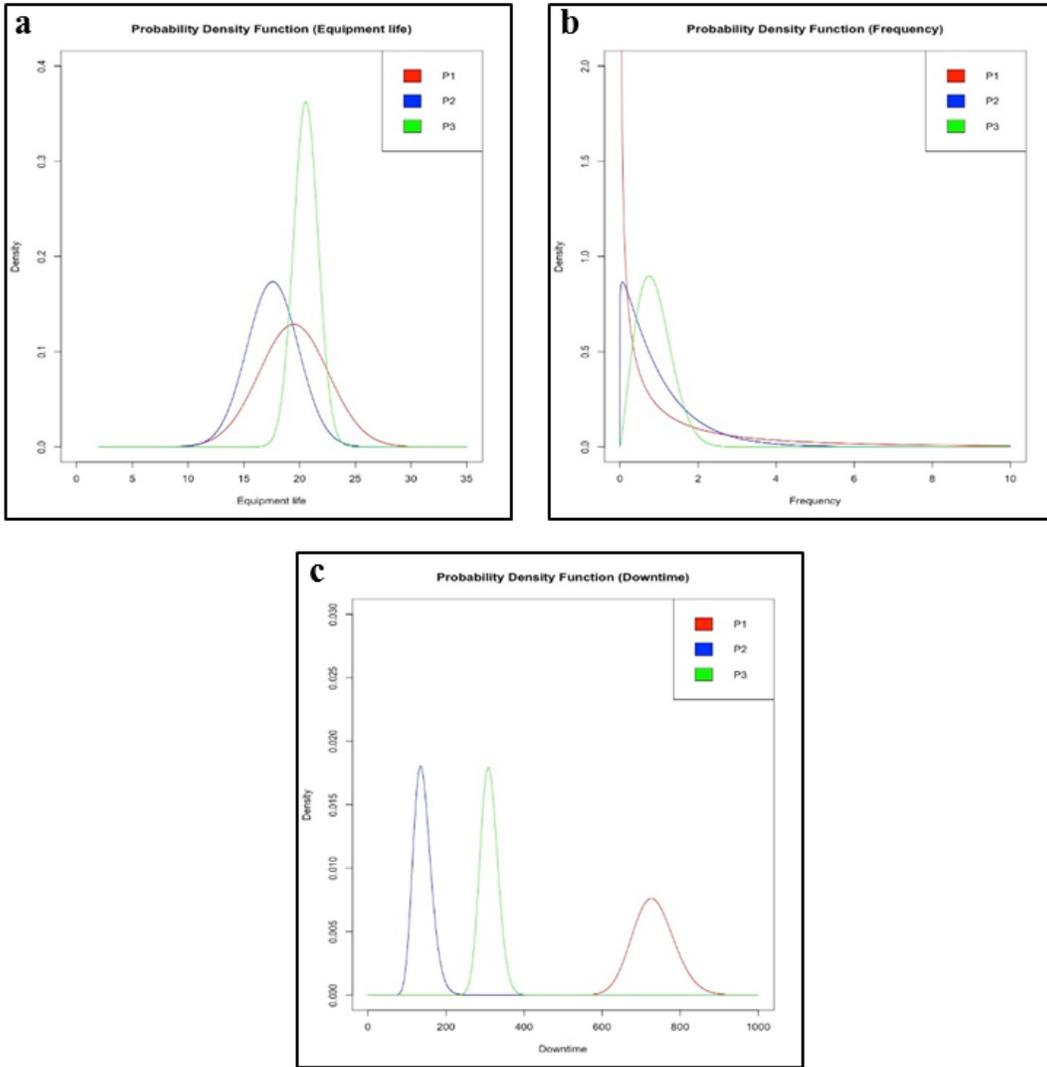


Figure VI.10: Posterior probability density functions for P1, P2, and P3

6.5.3. Maintenance action selection

In order to select the maintenance action alternative, the results of the three factors from the data-driven maintenance model as summarized in Table VI.7 are utilized. These

quantified results are used with the algorithm described in Appendix D to select the maintenance action alternative.

Table VI.7: Results of maintenance action analysis

Maintenance Action	Frequency (# of failures per unit time)	Downtime (hours)	Variability of equipment life (years)	Pump
Preventive maintenance (PM)	2.14	310	1.341	P ₃
Corrective maintenance	1.05	140	3.896	P ₂
Predictive maintenance (PdM)	0.562	730	4.293	P ₁

6.5.4. Reliability and expected process revenue

Figure VI.11, is a plot of overall expected revenue of the system against system reliability. It is presented for four different safety scenarios and four maintenance cost classification types M1, M2, M3, and M4 as per Appendix F. From the graph, it is observed that with an increase in reliability, expected revenue increases. Furthermore, the expected revenue at a given system reliability is least for safety scenario 1 that is most severe in consequences and hence has higher losses and maximum for safety scenario 4, which is comparatively less severe in consequences and therefore has lower losses.

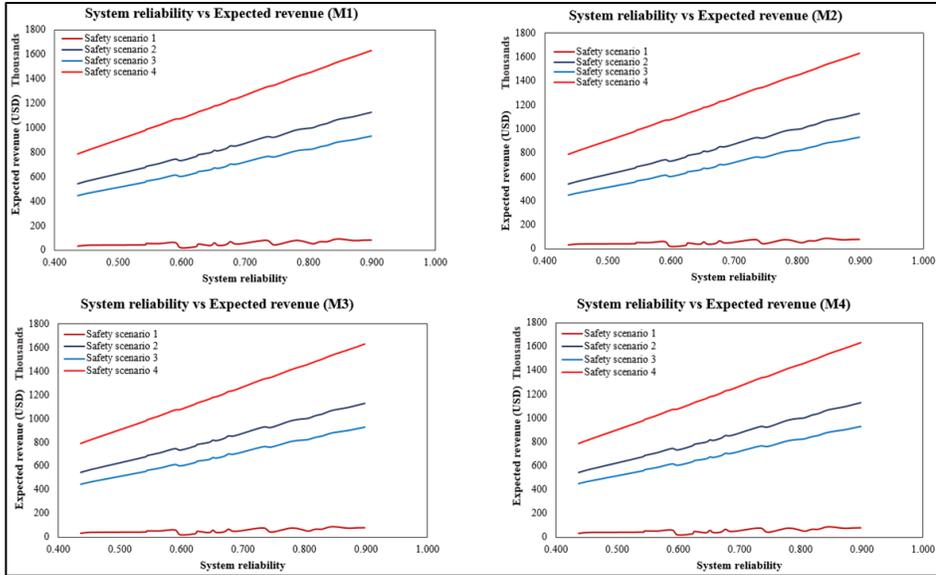


Figure VI.11: System reliability vs expected revenue

The graph in Figure VI.12 portrays the change in expected revenue of the system with changing system reliability for four different safety scenarios and maintenance cost classification type M2. As visible in the graph, expected revenue has a rising trend with an increase in system reliability for all four safety scenarios. Additionally, the expected revenue (with SIC) for all safety scenarios follow a similar rising trend, which is linear except that for safety scenario 1. For safety scenario 1, expected revenue increases logarithmically with increasing system reliability. It is further vital to note that with the incorporation of the safety impact costs the expected revenue does not follow the classic exponential trend with increase in system reliability, which is generally the case. However, expected revenue without safety impact cost displays an exponential trend.

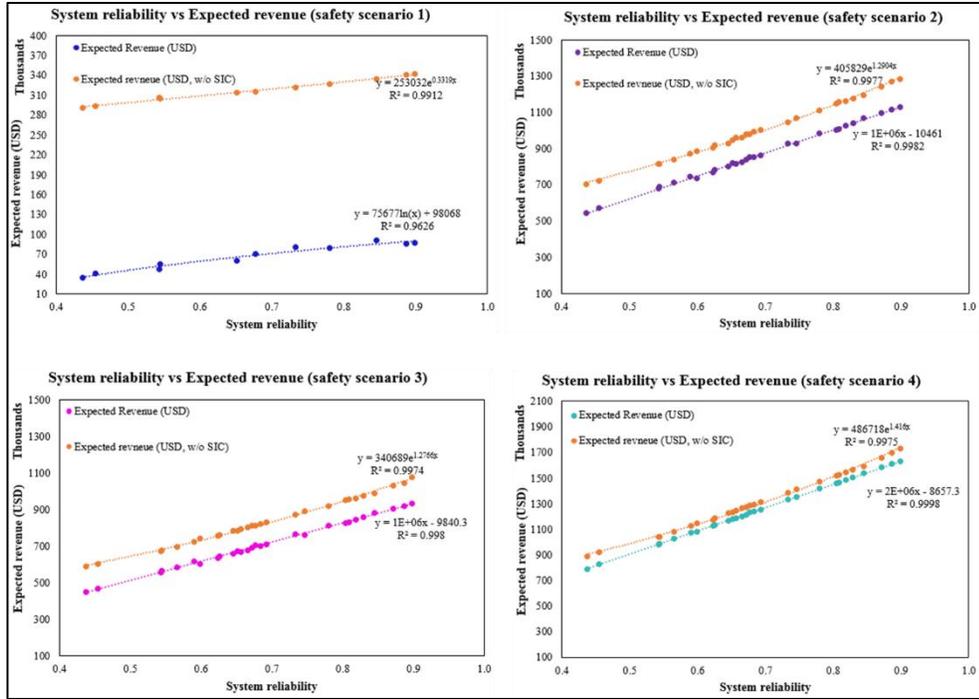


Figure VI.12: Trend of expected revenue with and without safety impact cost

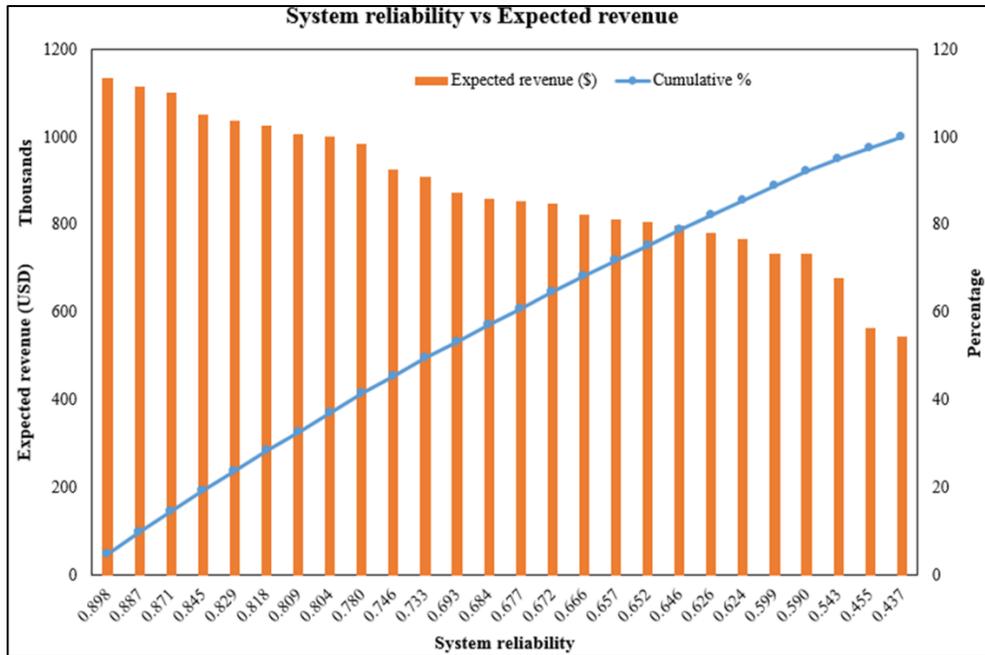


Figure VI.13: A pareto chart showing system reliability and expected revenue

Figure VI.13 illustrates a Pareto chart for system reliability vs expected revenue. On the X-axis, is the system reliability, primary Y-axis has expected revenue and secondary Y-axis shows the cumulative percentage. It can be concluded that 80% of the revenue is generated when system reliability is greater than 0.65. This type of information can be useful to develop effective maintenance policies.

Reliability and safety impact cost

Figure VI.14 depicts a bar graph that represents the change in the safety impact cost of the system with varying system reliability for seven different system states, four different safety scenarios, and maintenance cost classification type M2. One notable conclusion that is drawn from here is that, safety impact cost has a declining trend with an increase in system reliability for all states. Additionally, all system states follow a similar decreasing trend except that for system state 3. Furthermore, the minimum safety impact cost obtained is 2,40,450 USD with system reliability of 0.733 for system state 6. Likewise, it is noteworthy that 0.733 is not the highest system reliability but corresponds to minimum safety impact cost.

Reliability and resilience survivability index

Figure VI.15 highlights system reliability vs the resilience survivability index (RSI) of the system for seven different system states, four different safety scenarios, and maintenance cost classification type M2. Some observations that can be made from the graph are - resilience survivability index displays an increasing trend with respect to the system reliability for all states, the RSI is maximum for safety scenario 4 for all system states and minimum for safety scenario 1. This is aligned with the results of safety impact

cost with system reliability; the RSI is maximum for system state 4 with a value of 9.3 and is least for system state 5 with a value of 0.04.

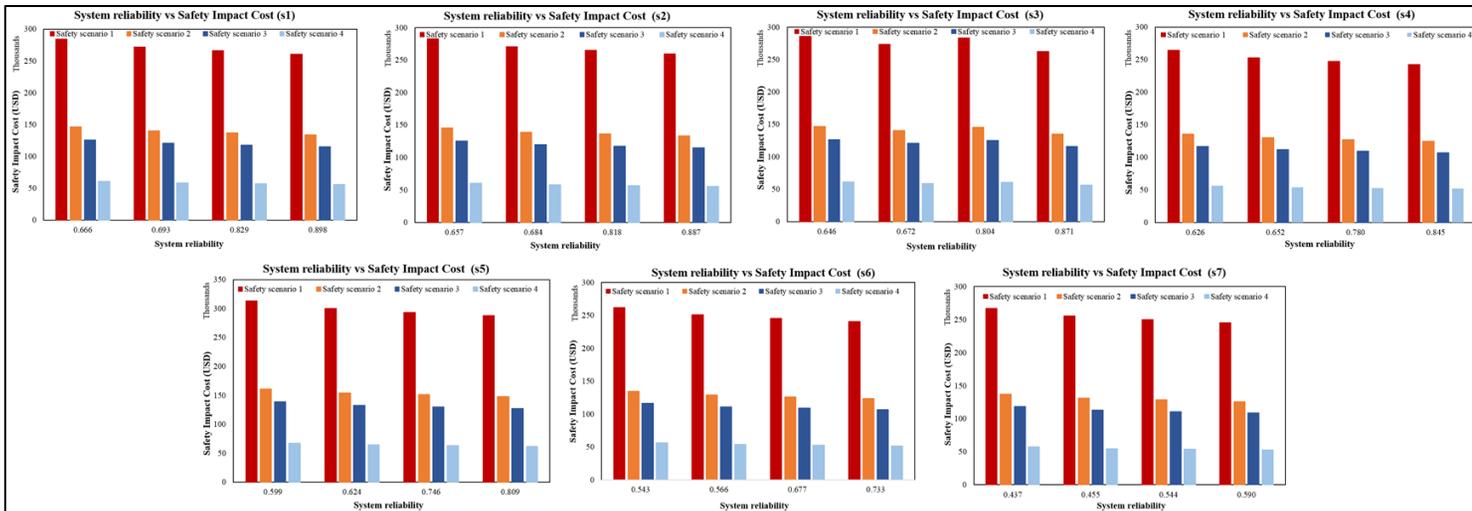


Figure VI.14: System reliability vs safety impact cost

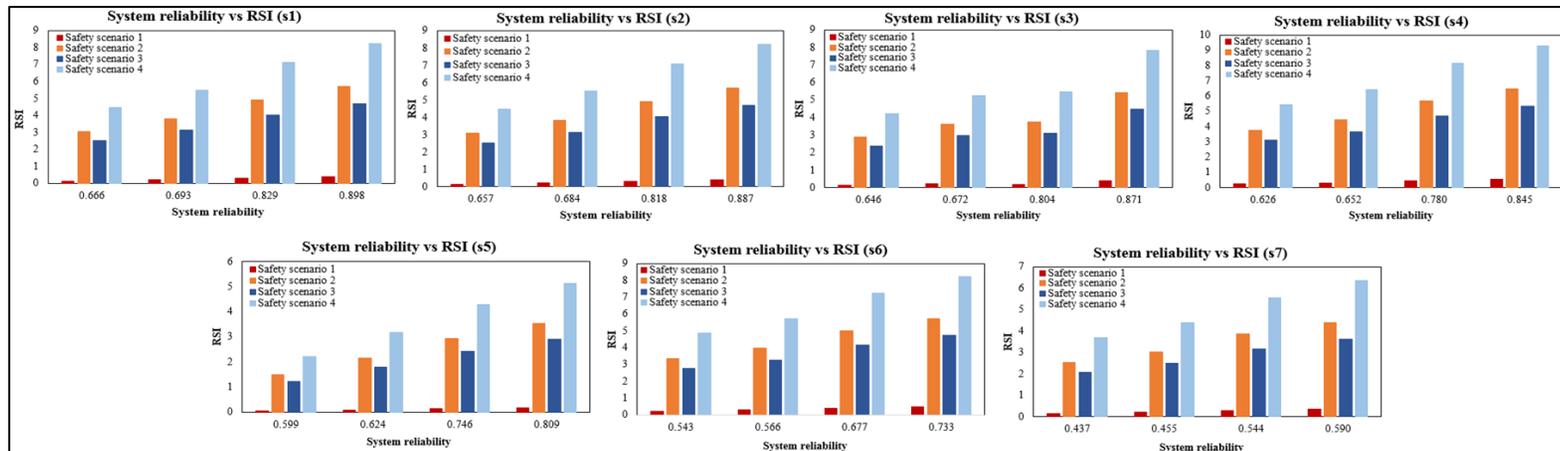


Figure VI.15: System reliability vs RSI

6.6. Summary

In this work, a novel method of survivability assessment using Process Resilience Analysis Framework (PRAF) was presented. The work demonstrates the development of an integrated model incorporating safety impact costs to identify optimal maintenance policy and process operating characteristics for safer and reliable operations. The key elements of this approach are (i) a process model that captures the details such as availability/operability of system equipment; (ii) a maintenance model that decides the maintenance action type based on data-driven analysis including frequency, downtime, and variability in equipment life; (iii) a safety model that takes into account the impact scenarios and respective losses through a system safety threshold; (iv) a cost and an expected revenue objective function, which examines the trade-off between safety, maintenance, and energy costs. The major contribution of this work is the definition of novel metric System Survivability Index, SSI that is incorporated as the system safety threshold to analyze the safety impact costs. Most of the conventional modeling considers reliability and efficiency of equipment as constant in process modeling. This in reality is not true as equipment failure, unplanned shutdown, unplanned downtime, less equipment efficiency can result in safety impacts and production losses. In current work, varying reliability or efficiency of the equipment is used. This approach also demonstrates the consideration of both technical and social factors (human and organization related such as percentage of maintenance backlogs, percentage of required maintenance procedures reviewed or revised as scheduled, percentage of process safety required training sessions completed) during the analysis. Finally, this work introduces Resilience Survivability Index (RSI) metric to assess the system capacity to respond to process upset situations.

Furthermore, the approach demonstrates the utilization of the existing data recorded in plants and gain valuable insights about the overall system performance.

An example of cooling tower operations, which is a MINLP formulation to obtain system effectiveness using minimum total annualized cost and maximum expected revenue as the objective function, explains the application of this method. The process system consists of counter flow induced draft cooling tower, and two downstream units – batch reactor and distillation column. The equipment considered in this system are - fan on top of the cooling tower and pump network of three pumps. The results from the example case study explicitly show the trade-off between the process revenue, safety impact, and maintenance costs. Different scenarios were investigated and it was found that the highest reliability of the process system does not ensure maximum expected revenue or minimum safety impact cost or maximum resilience survivability index. This symbolizes the complexities and connectivity within the process system. Furthermore, this type of integrated analysis based on the data on process operations and equipment health provides valuable insights about the process system performance. Additionally, the expected revenue does not follow the exponential trend with increasing system reliability, which is usually the case in the conventional methods. The results indicate that the developed application of PRAF can effectively identify the maintenance action to implement to the process system and can incorporate safety impact costs successfully in an integrated manner. Hence, the methodology and analysis presented in this work can be adopted to make effective resource allocation and risk mitigation decisions and can be customized to different process or energy systems and industrial sectors.

CHAPTER VII
PROCESS SYSTEM RESILIENCE, BUSINESS CONTINUITY AND
SUSTAINABILITY

In general, process safety and risk management challenges have increased because of competition, scale increase, pressure on energy use, reduced staff, *etc.*, in the process industry, along with a heavier focus of public perception on hazards and risks globally. This shift has necessitated exploring tools for an efficient transition from the narrower risk management aims to a risk management with the broader goals of business continuity and sustainability. In this context, the application of the resilience engineering perspective, not only in humans and organizations but also in a real technical sense, is being explored as an approach for considering the dynamics of socio-technical aspects based on systems theory. As established in the previous chapters, the resilience methodology emphasizes the defense against non-linear dynamics, new types of threats, uncertainty, and recovery from upset or catastrophic situations. The chapter establishes and presents the relationship between risk management and resilience capabilities. As an example, the 2012 Chevron Richmond Refinery Pipe Rupture and Fire incident is reviewed, and the established relationship between resilience and sustainability is applied. Based on the review of this case, the conclusion is drawn that using the PRAF, which is a quantitative and integrated approach, ensures a more effective risk management in the process industry. Hence, it strengthens the resilience capabilities of a process system to foster business continuity and sustainability.

Resilience is known as the elastic property of a solid material to regain its original state when stress ceases. Process system resilience refers to the capability of process plant

facilities and the enterprise as a whole to sustain their functions with a minimum of long-term damage when subjected to shocks due to unexpected or unknown threats of a different kind. Threats can be both of internal and external nature. The difference between a risk and a resilience analysis has been well described³⁹, stressing that risk is analyzed in view of a known hazard threat defined by a scenario, while resilience is analyzed in view of any threat. Some examples of these external threats are typically the 2017 Houston flooding due to hurricane Harvey causing the organic peroxide explosion and fires at the Arkema plant, and the earthquake and the following very high tsunami leading to the 2011 Fukushima Daiichi nuclear reactor core melts. The two cases have in common the same failed thinking: the power supply will not cease because there are diesel generators as a back-up. As the diesel generators are not placed at a sufficient elevation or as in the Fukushima plant even in an underground room, floodwater will put these generators out-of-action. Even, if flooding was imagined as a possibility, the chance had been estimated too remote for taking measures. In the case of the Arkema plant, the damage did not threaten yet the continuity of the company, but in quite some cases an unforeseen or ignored scenario may put the continuity at stake, or at least the damage done is much larger than it would have been if resilience measures would have been taken.

This chapter will sketch the various aspects that come into play when an organization given its resources wants to be as resilient as possible to safeguard continuity of its business.

7.1. Business Continuity

7.1.1. Definition of Business Continuity

ISO 22301 and ISO 22313 define Business Continuity as ‘the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident’.

7.1.2. Business Continuity Metrics

Following are some Business Continuity metrics relevant to manufacturing systems that are reported in the literature^{301, 376, 377, 378, 379}:

- Business resumption response time: the time taken before your organization can continue with business after an incident or failure scenario;
- Recovery time: the time taken for an organization to fully recover its original state after an incident or failure scenario;
- Recovery Point Objective (RPO): the maximum amount of data loss an organization can sustain during an event;
- Return Time Objective (RTO): the “target time for the resumption of product, service or activity delivery after an incident;”
- Maximum tolerable period of disruption (MTPoD) Duration after which an organization’s viability will be irrevocably threatened because of the adverse impacts that would arise as a result of not providing a product/service or performing an activity.

7.2. Sustainability

7.2.1. Definition of Sustainable Process System

Inspired by the definition of Sustainability by the United Nations Commission on Environment and Development (otherwise known as the Brundtland Commission) in 1987, a sustainable process system can be defined as follows: A process system that generated value to meet the needs of the present without compromising the ability of future generations to meet their own needs. This objective is achieved by maintaining and continuously improving the environmental, safety, and social performance of the system.

7.2.2. Sustainability Metrics

Sustainability metrics can be categorized based on the three dimensions of Environment, Economy, and Social acceptability that are relevant to process systems³⁸⁰, as follows:

- Eco-efficiency: a combination of impact of economic and environmental aspects, *e.g.*, set flaring.
- Socio-economic: a combination of societal/off-site impact (safety injuries or fatalities) and financial impact (statutory fines).
- Socio-environmental: a combination of effects of natural resources degradation, environmental releases, the safety of people, greenhouse gas emissions, air emissions, *etc.*

7.3. Case study: Chevron Refinery Fire

The Chevron Refinery Fire incident happened on August 6, 2012 in Richmond, California due to a catastrophic pipe rupture in the crude unit. The sulfidation corrosion led to the pipe rupture releasing flammable, high temperature light gas oil that ignited

subsequently. This incident led to minor injuries to six employees, community impact with 15,000 local residents seeking medical attention, the shutdown of the Bay Area Rapid Transit (BART) metro, and around 13 million USD (including citations, statutory fines, medical reimbursements)³⁸¹.

7.3.1. Analysis

To establish a relationship between resilience, business continuity, and sustainability, relevant metrics for all three with respect to Chevron incident are analyzed.

Business continuity

Based on the information available, two metrics for business continuity – business resumption response time, and recovery time are considered for this case study. Table VII.1 369, 370 provides the two important business continuity metrics for this case study.

Table VII.1: Business continuity metrics

Business Continuity Metrics	Days
Business resumption response time	257
Recovery time	1916

From Table VII.1, following can be concluded:

- The business resumption response time for the process unit is close to nine months or three quarters of a year.
- The recovery time for the whole organization is around five years.

Sustainability

In order to assess the sustainability of the process system under study, metrics or indicators relevant to the scope of the study are used to evaluate the performance. As mentioned earlier, three types of interrelated metrics are important and these can be

broadly assessed by social, environmental, and economic performance. Table VII.2 summarizes the key sustainability performance indicators for Chevron as a whole for years 2012, 2013, 2014, 2015, and 2016.

Figures VII.1 and VII.2 illustrate the total revenue and profit of Chevron for few years. It is important to note that these numbers represent the cumulative performance of whole Chevron and not just the Richmond Refinery site. Following are some interesting conclusions from Table VII.2:

- The social performance within sustainability is assessed based on the health and safety performance. It is observed that the year 2012 (incident year) had the worst performance followed by 2013 while comparing the performance for five years. The only exception is for days away from work rate where the worst performance is in the year 2013.
- For the environmental performance, the years 2012 and 2013 have the worst performances in the last five years. Metrics or indicators such as costs of environmental, health and safety fines paid and settlement is worst for the year 2013 (the year following the incident).
- The financial performance depends on a variety of factors other than the incident itself such as oil price. It follows a declining trend for financial performance since 2011.

Table VII.2: Sustainability metrics

Year	2016	2015	2014	2013	2012
Health and Safety Performance					
Total Recordable Incident Rate (incidents per 200,000 work-hours)					
Workforce	0.14	0.18	0.18	0.21	0.24
Employees	0.1	0.1	0.1	0.15	0.2
Contractors	0.16	0.2	0.21	0.23	0.25
Lost-Time Incident Frequency (Days Away From Work incidents and fatalities per million work-hours)					
Workforce	0.1	0.1	0.11	0.13	0.15
Employees	0.08	0.1	0.06	0.14	0.13
Contractors	0.11	0.1	0.12	0.12	0.15
Days Away From Work Rate (incidents per 200,000 work-hours)					
Workforce	0.016	0.019	0.021	0.02	0.027
Employees	0.015	0.02	0.011	0.026	0.024
Contractors	0.016	0.018	0.023	0.018	0.027
Work-related fatal incident rate					
Work-related incidents per 100 million work-hours	0.81	0.51	0.49	1.02	1.11
Number of process safety Tier 1 events	22	29	19	38	76
Environmental Performance					
GHG emission (operated basis)					
Average flare gas volume rate, direct, operated basis (million standard cubic feet per day)	644	615	563	692	821
Air Emissions					
Total volatile organic compounds (VOCs) emitted (thousand metric tons)	154	144	134	147	159
Total sulfur oxides (SOx) emitted (thousand metric tons)	66	84	112	141	123
Total nitrogen oxides (NOx) emitted (thousand metric tons)	151	148	138	147	146
Fines and settlements					
Number of EHS fines paid and settlements entered into, equity basis	102	135	292	284	339
Cost of EHS fines paid and settlements entered into, equity basis (millions of dollars)	6.7	3.9	57.1	119.2	91.1
Key Financials \$ Millions					
Revenue	107567	131,118	203,784	220356	233899
Profit	-497	4,587	19,241	21423	26179
Assets	260078	266103	267236	253753	232982
Total Shareholder Equity	145556	152,716	155,028	149113	136524

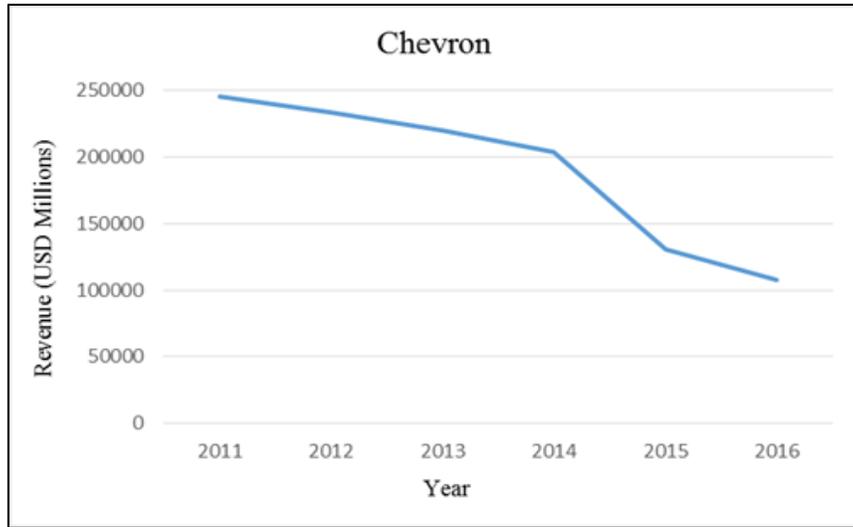


Figure VII.1: Total annual revenue of Chevron

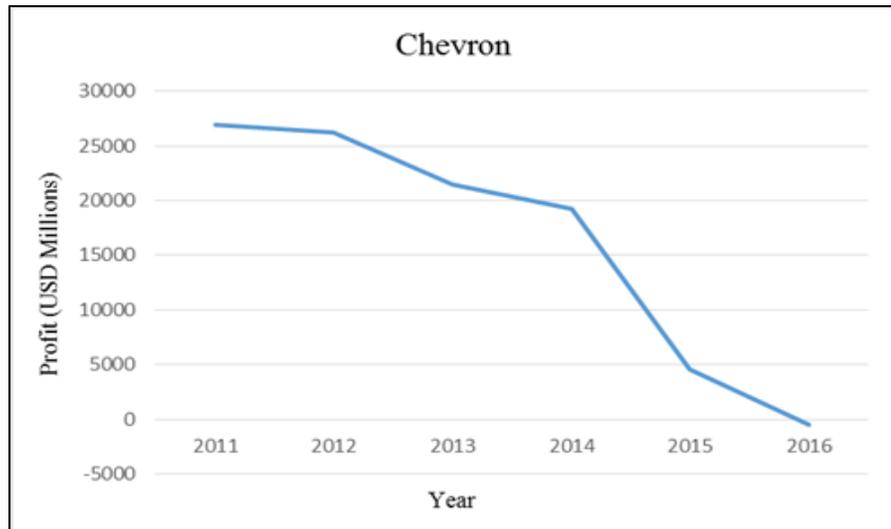


Figure VII.2: Total annual profit of Chevron

Process resilience

Process resilience of the system under study is evaluated for three different phases of resilience – avoidance, survival, and recovery. The overall Resilience Performance Index (RPI) is assessed and summarized in Table VII.3. In the current case study of the Chevron refinery fire incident, resilience score is assigned based on the findings from the

investigation report. This score is used to calculate the actual resilience metrics ($R_{m_{actual}}$) and best performance or full score is used to calculate the expected resilience metrics ($R_{m_{expected}}$). An RPI value of greater than one (>1) is considered being good, $0.5 < RPI < 1$ is average, and <0.5 is poor performance. The RPI is calculated based on the plant data from resilience metrics using the following set of equations.

$$RPI = \frac{R_{m_{actual}}}{R_{m_{expected}}} \quad (7.1)$$

$$R_{m_{actual}} = \frac{\text{Resilience score (actual performance)} * \text{Weight}}{\max(\text{Resilience score (actual performance)} * \text{Weight})} \quad (7.2)$$

$$R_{m_{expected}} = \frac{\text{Resilience score (full)} * \text{Weight}}{\max(\text{Resilience score (full)} * \text{Weight})} \quad (7.3)$$

Some conclusions that can be drawn from Table VII.3 are as follows:

- The RPI for all the relevant metrics is below 0.5, which is an indicator of poor performance.
- The lowest value of RPI is 0.11, and it is interesting to note that this is for social metrics such as process hazard evaluations completion, past-due process safety actions, on-time safety critical equipment (SCE) inspections completion, and maintenance backlogs. This provides an indication of strong significance of social metrics in the risk and resilience assessment during the operational part of a plant's life cycle. And that is also when the Safety-II attitude is most relevant.
- The highest value of RPI is 0.37 for the metric mock drills for emergency situations.

- For the three phases, the process system had best possible ways to control the upset situation in the survival phase, followed by avoidance, and lastly recovery.

Table VII.3: Resilience metrics

Resilience Metrics	Weights₃₃₅	Investigation Report Recommendations³⁸¹	Resilience Performance Index (RPI)*
Avoidance			
Communications on learning from incidents	0.68	Previous catastrophic failures due to sulfidation corrosion in the refinery industry Chevron's Richmond, California 2007	0.22
Process hazard evaluations completion	0.81	Detailed inherently safer analysis, safeguard evaluation, and damage mechanism hazard review not performed.	0.11
Past-due process safety actions	0.93	No formal method to communicate and implement Energy Technology Company (ETC) findings and recommendations.	0.11
Survival			
Changes executed through the MoC procedure	0.75	No MoC performed to evaluate the risk of new T-Min.	0.34
On-time safety critical equipment (SCE) inspections completion	0.94	Recommendation to inspect 4-Sidecut line not implemented.	0.11
Management response to the inspection findings of (SCE) deficiency	1		0.34
Maintenance backlogs	0.81	100% component inspection not completed.	0.11
Recovery			
Successful tests for emergency systems and procedures	1	No guiding emergency leak response protocol.	0.25
Mock drills for emergency situations	0.94		0.37

* RPI stands for Resilience Performance Index (ratio of actual to expected value of resilience metrics)

Furthermore, from the combined analysis of Tables VII.1, VII.2, and VII.3 it is evident that resilience and sustainability are closely related. Also, all three metrics clearly depict the fact that resilience, sustainability, and business continuity aspects are related in some way or the other.

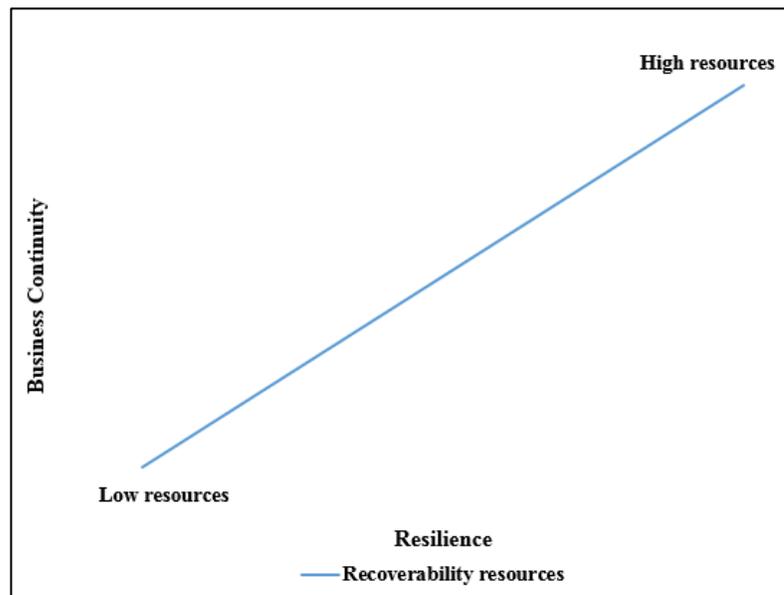


Figure VII.3: Trendline result for Business Continuity and Resilience relationship

The analysis results based on the incident case study are summarized in Figures VII.3 and VII.4. As illustrated in the qualitative analysis in Figure VII.3, with the increase in resources in the recoverability phase, both resilience and business continuity of the process system increase. This increase is because time is the critical parameter for both resilience and business continuity in the recovery phase. With more resources, the response time and hence overall recovery time can be reduced. This would lead to increase in both process system resilience and business continuity. Therefore, with regard to the recoverability resources, it is clear that there exists a positive proportional relationship between business continuity and resilience. Figure VII.4 illustrates the relationship

between process system resilience and sustainability for three resilience phases based on results from Tables VII.2 and VII.3 and also considering the number of resources available. In the avoidance phase, a moderately sustainable process system would require fewer resources. However, the system would have been more robust and as well as resilient with more resources. For the survival phase, the system gains both robustness and sustainable characteristics to a medium level only, even at the deployment of more resources. This is due to limited time and resources available, the process system will unlikely reach its full potential. Clearly, for the recovery phase, with low resources, both the sustainability and resilience of the system is low and would be high with more resources.

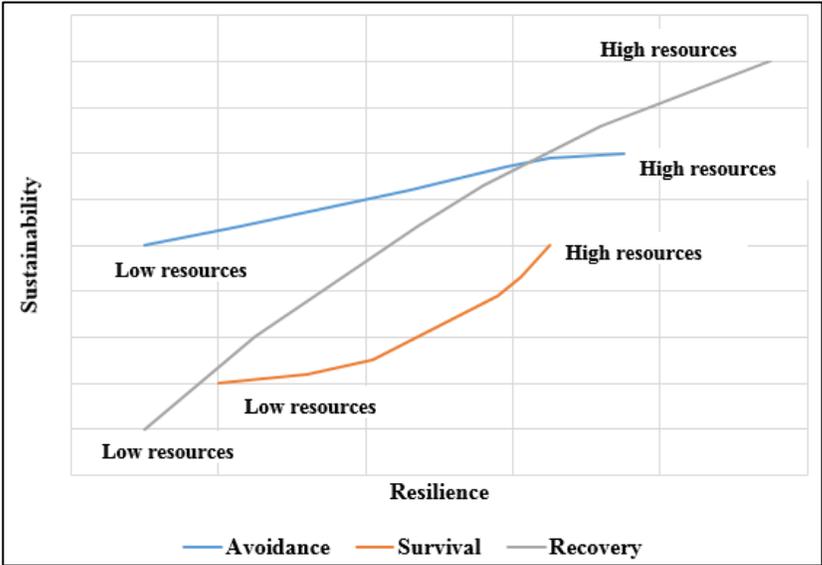


Figure VII.4: Trendline results for Sustainability and Resilience Relationship

It is difficult to establish a correlation between sustainability and business continuity and it needs further research with more data. Similarly, at this stage of research, at least a semi-quantitative correlation between resilience, sustainability and business continuity is difficult to state and it requires more data and a further detailed analysis of

various trade-offs based on risk acceptance and desired resilience levels of process system or management. This may be considered as future work, which will incorporate explicit cost values and detailed simulation and multi-objective optimization methods to incorporate conflicting goals and their mutual impacts.

7.4. Summary

Building resilience capability of a process plant is initiated by being concerned about continuity of the business in the longer term, and it consists of a way of thinking. The framework for this was laid down. As a result of a system approach pushing for resiliency, a comprehensive analysis of the capabilities of an organization is needed that will be quite effort intensive. Because threats may be unknown and unexpected, a full risk assessment in the plant design stage will certainly not be sufficient. Although thorough hazard identification will be of great help then and in later stages, the four aspects of process system resilience – early detection, error-tolerant design, plasticity, and recoverability - require other aspects to also be considered. This will certainly be the case in the operational stage where the effectiveness of the organization, teamwork, hence the human interaction both within the organization and with the plant equipment are key, and when the idea of resilience engineering in the human sense with the Safety-II approach should be deployed. Effective management needs indicators to steer an organization in the right direction. Practical, effective and efficient realization of the ideas of resilience will need therefore further development of software tools, and data analytics.

In the case study presented, the effect of neglecting to keep sufficient resources for unexpected disturbances, and the correlations of resilience capacity of a process system with regard to business continuity and sustainability were shown.

CHAPTER VIII

CONCLUSIONS AND FUTURE WORK

The objective of this research has been to establish a systematic framework for early detection of unsafe domains of operation, assessment of aggregate risks and prioritization of safety barriers during process upset situations and reduction in response time resulting in a reduced frequency of loss of containment events³⁷, reduced consequences and enhanced recovery. The implementation of models within PRAF would also result in better flexibility and control, operability, and maintainability of process operations.

8.1. Conclusions

Chapter I provided the motivation and challenges behind the research in the area of advanced risk and resilience assessment. The limitations of existing methods, reasons for complex systems failure, comparative regulatory regime analysis, and potential improvement opportunities have been reviewed and presented.

A significant amount of work has been previously conducted in area of resilience by research community. Chapter II presents a literature review of the previous developments on which the Process Resilience Analysis Framework (PRAF) concepts and model formulations presented are based. The review covers the previous work carried out in system resilience and resilience engineering, risk and resilience assessment of process systems, and modeling aspects of process system resilience.

The foundations of the proposed framework PRAF have been formally introduced in Chapter III. In particular, concepts of process system resilience, unified taxonomy, and four aspects of process system resilience: early detection, error-tolerant design,

recoverability, and plasticity, have been presented. The details on resilience metrics and PRAF survey and response analysis is also provided in this chapter. In addition, matrix-based quantification method for social aspects is represented and demonstrated using an example of reactor charging procedure.

In Chapter IV, a novel resilience-based qualitative method for hazard analysis called Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA) has been proposed. The key aspects of the RIPSHA approach such as bi-layered method, covering four modes of operations, along with templates for RIPSHA worksheets has been provided.

A thorough predictability assessment analysis procedure has been formally proposed in Chapter V, for the identification of the process upset situations or events affecting the flexibility and control of the process system under study. A new method using MCMC algorithms, sensitivity analysis and optimization has been introduced that utilizes plant data.

In Chapter VI, a novel method of survivability assessment using PRAF has been presented. The proposed methodology aimed to determine the optimal maintenance policy for optimal and safer plant operations. The implementation of the survival model is demonstrated on a cooling tower operation example problem (MINLP formulation), where optimal operation and maintenance (preventive, corrective, and predictive) strategies are determined based on trade-off analysis of process revenue, safety impact, and maintenance costs.

Finally, the concepts of business continuity, sustainability, process system resilience and their relationships have been explored and presented in Chapter VII. A case

study on Chevron Richmond refinery incident is applied to find out the relationships based on the metrics for the three aspects.

In summary, the main contributions of this work have been:

- A standard process system resilience framework called *PRAF* - '*Process Resilience Analysis Framework*' with a unified taxonomy has been established. This framework is an integrated, dynamic, systems-based, quantifiable framework for enhanced risk and resilience management through improved flexibility, operability, maintainability, and controllability.
- 24 process system resilience metrics including both technical and social aspects have been developed. These resilience metrics in principle allow for system optimization to develop effective risk management strategies in design and operations of such systems.
- A PRAF survey has been conducted and survey response has been analyzed to answer the three research questions related to incorporation of the resilience metrics in the risk and/or resilience assessment – what are the most important metrics for each of the three phases of PRAF – avoidance, survival, and recovery?, are there any differences in viewpoints of various groups of survey respondents?, what are the weights or level of importance for each of the metrics?
- A new resilience-based and integrated systems approach for hazard analysis called *RIPSHA* – '*Resilience-based Integrated Process Systems Hazard Analysis*' has been developed and methodology demonstrated using a LNG

and tank explosion case study examples. A significant feature of RIPSHA methodology is that it covers two layers – management system (process safety culture and resilient leadership; operational discipline, and process safety systems) and plant system (process/plant equipment, operator/human and procedures) and four different modes of analysis – design, normal operations, simultaneous operations, and transient operations to be applied throughout the life cycle of a facility. The study results illustrate that the resilience-based approach is useful for identification of unknown scenarios from human and organizational perspectives.

- A predictability assessment methodology to predict process upset situations and hence have better flexibility and control of process system by virtue of a Monte Carlo Markov Chain formulation, Global Sensitivity Analysis, robust simulation, and optimization backed by process resilience concepts has been developed and demonstrated using a batch reactor example.
- The established predictability assessment approach would enable the risk assessors to make risk decisions based on information of their process plant and hence manage and quantify uncertainties and better allocate the resources towards improvement areas.
- A novel method of survivability assessment using PRAF was presented. The work demonstrates the development of an integrated model incorporating safety impact costs to identify optimal maintenance policy and process operating characteristics for safer and reliable operations. A

novel metric called SSI – ‘*System Survivability Index*,’ was incorporated as the system safety threshold to analyze the safety impact costs.

- The implementation of the developed models can (i) integrate the social factors analysis and quantify them using a single approach, (ii) move from traditional point values for occurrence of loss of containment events (used in QRAs) to a range similar to the Probabilistic Risk Assessment (PRA) methods, and (iii) manage the uncertainties in the limited historical database on frequency or failure rates by using resilience metrics and thus incorporating the process plant performance data of the plant under study. This subsequently may increase safety, reliability, efficiency, and profitability of the process system.
- Concepts of business continuity, sustainability, process system resilience and their relationship was summarized. A case study using the metrics in each of these areas and study results on the effect of resources for unexpected disturbances, and the correlations of resilience capacity of a process system with regard to business continuity and sustainability were shown.

8.2. Recommendations for future directions

Within the PRAF research, the following aspects could be looked into for further development:

- Recoverability Assessment: the concepts for uncertainty quantification and social aspects analysis can be furthered for the recoverability analysis. Some major elements of this assessment are 1) a process model that

captures the details such as process variations, 2) a barriers assessment model that enhances the assessment of mitigation barriers by quantifying the uncertainty in the probability of failure on demand values, 3) a decision-making model to evaluate the behavior of personnel during emergency situation, for example, in selection of the evacuation route, and 4) an optimization model based on the objective of maximum flow and minimum cost.

- Process resilience index (PRI): the current work proposes the methods for estimation of the resilience sub-indices for the prediction, survival, and the recovery phases. These are resilience prediction index (RPI), resilience survival index (RSI), and resilience recovery index (RRI). This work and concepts could be extended to evaluate the PRI for a single process system.
- Process system resilience metrics: the results of the metrics study indicate potential improvement for further research such as extending the survey to determine the most appropriate phase of the metric, find the relative level of significance of three phases, and establish correlations between metrics and performance by using actual data.
- Maintenance model: the maintenance model, presented in Chapter VI, is based on steady-state considerations; here extensions to include time-dependent maintenance activities could be an essential step for a more realistic representation of dynamic process operations. Additionally, objective such as of maintenance scheduling and planning would be another interesting aspect to incorporate in the current model.

- PRAF application in design phase: the models developed within PRAF can be extended to formulate multi-objective optimization problems for different applications such as process intensification during the design stage analysis. Various objectives and constraints can be set and a trade-off analysis can be carried out for such studies.
- Environmental considerations: the same models can be developed further in order to explicitly include environmental losses or constraints in addition to process, product quality and safety constraints in the optimization formulation.
- Computing platform: the analysis in the current research has been carried out in different platforms – gPROMS, MATLAB, programming language R, and GAMS. In future, opportunities may be explored to carry out complete analysis in a single platform and deliver it as a PRAF-based software tool.
- Benchmarking studies: predictive and survival assessment models in the current research have been limited to single process unit case studies, however, this work could be extended to multiple process system units and can also be used to benchmark and compare the resilience capacities and performance of any two process systems.
- Extension to supply chain network analysis: the various concepts and methods developed within PRAF have been currently applied to manufacturing design and operations. In future, the systems thinking, top requirements of the system for effectiveness, business continuity and

statistical techniques, sensitivity analysis, prediction tools, and optimization methods can be furthered in areas of supply chain network analysis.

- Application: the methodology and analysis presented in this research can be adopted to make effective resource allocation and risk mitigation decisions and can be customized to different process or energy systems and industrial sectors such as pharmaceutical plants, LNG industry, and oil and gas units. Additionally, the PRAF methodology can be applied to compare process technologies during the conceptual stages of design.

REFERENCES

1. Tixier, J.; Dusserre, G.; Salvi, O.; Gaston, D., Review of 62 risk analysis methodologies of industrial plants. *Journal of Loss Prevention in the process industries* **2002**, *15* (4), 291-303.
2. White, D., Application of systems thinking to risk management: a review of the literature. *Management Decision* **1995**, *33* (10), 35-45.
3. Kidam, K.; Sahak, H. A.; Hassim, M. H.; Hashim, H.; Hurme, M., Method for identifying errors in chemical process development and design base on accidents knowledge. *Process Safety and Environmental Protection* **2015**, *97*, 49-60.
4. Taylor, J. R., Statistics of design error in the process industries. *Safety science* **2007**, *45* (1-2), 61-73.
5. Baybutt, P., A critique of the Hazard and Operability (HAZOP) study. *Journal of Loss Prevention in the Process Industries* **2015**, *33*, 52-58.
6. Marsh *The 100 Largest Losses 1974-2015*; 2016.
7. Dalziell, E. P.; McManus, S. T., Resilience, vulnerability, and adaptive capacity: implications for system performance. **2004**.
8. Atherton, J.; Gil, F., *Incidents that define process safety*. Wiley: 2008.
9. DOME From Tragedy to Transformation. **2016**, *67* (1).
10. Allen, M., How Many Die From Medical Mistakes in U.S. Hospitals? **2013**.
11. Thakor, A. V., The financial crisis of 2007–2009: Why did it happen and what did we learn? *Review of Corporate Finance Studies* **2015**, *4* (2), 155-205.
12. Board, C. A. I., CAIB Report. *Washington, DC, August* **2003**.

13. Hopkins, A. In *Why 'safety cultures' don't work*, 3rd Annual Offshore Safety Conference, Decomworld Business Intelligence for the Offshore Industry, 2014.
14. Engen, O. A.; Lindøe, P. H., The Nordic Model revisited: Focusing Events and Regulator as Proactive Agent in the Norwegian Petroleum industry. *Durham, NC: Kenan Institute for Ethics* **2014**.
15. Norway, P. S. A. From Prescription to Performance in Petroleum Supervision, Petroleum Safety Authority Norway. (accessed 05 May, 2014).
16. Commission, O. (accessed 05 May 2014).
17. Re, S., Teleconference with Ernst Zirngast. 2014.
18. Leveson, N., *Engineering a safer world: Systems thinking applied to safety*. MIT press: 2011.
19. Baybutt, P., Competency requirements for process hazard analysis (PHA) teams. *Journal of Loss Prevention in the Process Industries* **2015**, *33*, 151-158.
20. Seligmann, B. J.; Németh, E.; Hangos, K. M.; Cameron, I. T., A blended hazard identification methodology to support process diagnosis. *Journal of Loss Prevention in the Process Industries* **2012**, *25* (4), 746-759.
21. Pasman, H.; Reniers, G., Past, present and future of Quantitative Risk Assessment (QRA) and the incentive it obtained from Land-Use Planning (LUP). *Journal of loss prevention in the process industries* **2014**, *28*, 2-9.
22. Dowell, A. M. In *Layer of protection analysis: A new PHA tool after HAZOP, before fault tree analysis*, International Conference and Workshop on Risk Analysis in Process Safety, 1997.

23. Salvi, O.; Debray, B., A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive. *Journal of hazardous materials* **2006**, *130* (3), 187-199.
24. Cozzani, V.; Reniers, G., Special issue: domino effects in the process industry-advancing the state of the art. *Reliability Engineering & System Safety* **2015**, *143*, 1-2.
25. Rasmussen, J., Risk management in a dynamic society: a modelling problem. *Safety science* **1997**, *27* (2-3), 183-213.
26. Rasmussen J, S. I. *Proactive risk management in a dynamic society. 1st ed. ISBN 91-7253-084-7.* , 2000.
27. Kahneman, D.; Egan, P., *Thinking, fast and slow.* Farrar, Straus and Giroux New York: 2011; Vol. 1.
28. Lauridsen, K.; Kozine, I.; Markert, F.; Amendola, A.; Christou, M.; Fiori, M., Assessment of uncertainties in risk analysis of chemical establishments. The ASSURANCE project. Final summary report. **2002**.
29. HSE, U. *Failure Rate and Event Data for Use within Risk Assessments (28/06/2012)*; 2012.
30. OREDA, *Offshore Reliability Data Handbook 6th Edition Volume 1 – Topside Equipment, Volume 2 – Subsea Equipment, SINTEF, Norway* 2015.
31. Paskan, H. J., *Risk Analysis and Control for Industrial Processes-Gas, Oil and Chemicals: A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events.* Butterworth-Heinemann: 2015.
32. Mannan, M. S.; Sachdeva, S.; Chen, H.; Reyes-Valdes, O.; Liu, Y.; Laboureur, D. M., Trends and challenges in process safety. *AIChE Journal* **2015**, *61* (11), 3558-3569.

33. Weick, K. E.; Sutcliffe, K. M., *Managing the unexpected: Resilient performance in an age of uncertainty*. John Wiley & Sons: 2011; Vol. 8.
34. Visser, J. In *Managing safety in the oil industry—the way ahead*, 14th World Petroleum Congress, World Petroleum Congress: 1994.
35. Knegtering, B.; Pasman, H., Safety of the process industries in the 21st century: A changing need of process safety management for a changing industry. *Journal of Loss Prevention in the Process Industries* **2009**, 22 (2), 162-168.
36. Madni, A. M.; Jackson, S., Towards a conceptual framework for resilience engineering. *IEEE Systems Journal* **2009**, 3 (2), 181-191.
37. Bruce K. Vaughen, K. B. Use the Bow Tie Diagram to help reduce process safety risks 2016. <http://www.aiche.org/resources/publications/cep/2016/december/use-bow-tie-diagram-help-reduce-process-safety-risks>.
38. Youn, B. D.; Hu, C.; Wang, P., Resilience-driven system design of complex engineered systems. *Journal of Mechanical Design* **2011**, 133 (10), 101011.
39. Steen, R.; Aven, T., A risk perspective suitable for resilience engineering. *Safety science* **2011**, 49 (2), 292-297.
40. Francis, R.; Bekera, B., A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety* **2014**, 121, 90-103.
41. Hollnagel, E.; Woods, D. D.; Leveson, N., *Resilience engineering: concepts and precepts*. Ashgate Publishing, Ltd.: 2007.

42. Morari, M., Design of resilient processing plants—III: A general framework for the assessment of dynamic resilience. *Chemical Engineering Science* **1983**, 38 (11), 1881-1891.
43. Grossmann, I. E.; Morari, M., Operability, resiliency, and flexibility: Process design objectives for a changing world. **1983**.
44. Woods, D. D., Creating foresight: How resilience engineering can transform NASA's approach to risky decision making. *Work* **2003**, 4 (2), 137-144.
45. Hollnagel, E., RAG-The resilience analysis grid. *Resilience engineering in practice: a guidebook*. Ashgate Publishing Limited, Farnham, Surrey **2011**, 275-296.
46. Dinh, L. T.; Pasman, H.; Gao, X.; Mannan, M. S., Resilience engineering of industrial processes: principles and contributing factors. *Journal of Loss Prevention in the Process Industries* **2012**, 25 (2), 233-241.
47. Shirali, G.; Motamedzade, M.; Mohammadfam, I.; Ebrahimipour, V.; Moghimbeigi, A., Challenges in building resilience engineering (RE) and adaptive capacity: A field study in a chemical plant. *Process safety and environmental protection* **2012**, 90 (2), 83-90.
48. Azadeh, A.; Salehi, V.; Mirzayi, M.; Roudi, E., Combinatorial optimization of resilience engineering and organizational factors in a gas refinery by a unique mathematical programming approach. *Human Factors and Ergonomics in Manufacturing & Service Industries* **2017**, 27 (1), 53-65.
49. Holling, C. S., Resilience and stability of ecological systems. *Annual review of ecology and systematics* **1973**, 4 (1), 1-23.

50. Mileti, D., *Disasters by design: A reassessment of natural hazards in the United States*. Joseph Henry Press: 1999.
51. Walker, B.; Holling, C. S.; Carpenter, S.; Kinzig, A., Resilience, adaptability and transformability in social–ecological systems. *Ecology and society* **2004**, 9 (2).
52. Grote, G. In *Rules management as source for loose coupling in high-risk systems*, Proc. of the second resilience engineering symposium, 2006; pp 116-124.
53. Fiksel, J., Sustainability and resilience: toward a systems approach. *Sustainability: Science, Practice, & Policy* **2006**, 2 (2).
54. Cimellaro, G. P.; Reinhorn, A. M.; Bruneau, M. In *Quantification of seismic resilience*, Proceedings of the 8th US National conference on Earthquake Engineering, 2006; pp 18-22.
55. Hale, A.; Heijer, T., Defining resilience. *Resilience engineering: concepts and precepts* **2006**, 35-40.
56. Vogus, T. J.; Sutcliffe, K. M. In *Organizational resilience: towards a theory and research agenda*, Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference on, IEEE: 2007; pp 3418-3422.
57. Aven, T., On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. *Risk Analysis* **2011**, 31 (4), 515-522.
58. Longenecker, R.; Zink, T.; Florence, J., Teaching and learning resilience: building adaptive capacity for rural practice. A report and subsequent analysis of a workshop conducted at the Rural Medical Educators conference, Savannah, Georgia, May 18, 2010. *The Journal of Rural Health* **2012**, 28 (2), 122-127.

59. Speranza, C. I.; Wiesmann, U.; Rist, S., An indicator framework for assessing livelihood resilience in the context of social–ecological dynamics. *Global Environmental Change* **2014**, *28*, 109-119.
60. Sahebjamnia, N.; Torabi, S. A.; Mansouri, S. A., Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research* **2015**, *242* (1), 261-273.
61. Crick, J. M.; Crick, D., Developing entrepreneurial resilience in the UK tourism sector. *Strategic Change* **2016**, *25* (3), 315-325.
62. Fairbanks, R. J.; Wears, R. L.; Woods, D. D.; Hollnagel, E.; Plsek, P.; Cook, R. I., Resilience and resilience engineering in health care. *Joint Commission journal on quality and patient safety* **2014**, *40* (8), 376-383.
63. Praetorius, G.; Hollnagel, E.; Dahlman, J., Modelling Vessel Traffic Service to understand resilience in everyday operations. *Reliability engineering & system safety* **2015**, *141*, 10-21.
64. Anderson, J.; Ross, A.; Jaye, P. In *Resilience engineering in healthcare: moving from epistemology to theory and practice*, proceedings of the fifth resilience engineering symposium. Soesterberg: Resilience Engineering Association, 2013.
65. Azadeh, A.; Salehi, V.; Ashjari, B.; Saberi, M., Performance evaluation of integrated resilience engineering factors by data envelopment analysis: The case of a petrochemical plant. *Process Safety and Environmental Protection* **2014**, *92* (3), 231-241.
66. Azadeh, A.; Salehi, V.; Arvan, M.; Dolatkah, M., Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant. *Safety Science* **2014**, *68*, 99-107.

67. John, A.; Yang, Z.; Riahi, R.; Wang, J., A risk assessment approach to improve the resilience of a seaport system using Bayesian networks. *Ocean Engineering* **2016**, *111*, 136-147.
68. Woods, D. D., Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety* **2015**, *141*, 5-9.
69. Aburn, G.; Gott, M.; Hoare, K., What is resilience? An integrative review of the empirical literature. *Journal of advanced nursing* **2016**, *72* (5), 980-1000.
70. Infurna, F. J.; Luthar, S. S., Re-evaluating the notion that resilience is commonplace: A review and distillation of directions for future research, practice, and policy. *Clinical psychology review* **2018**.
71. Righi, A. W.; Saurin, T. A.; Wachs, P., A systematic literature review of resilience engineering: Research areas and a research agenda proposal. *Reliability Engineering & System Safety* **2015**, *141*, 142-152.
72. Linnenluecke, M. K., Resilience in business and management research: A review of influential publications and a research agenda. *International Journal of Management Reviews* **2017**, *19* (1), 4-30.
73. Leveson, N., A new accident model for engineering safer systems. *Safety science* **2004**, *42* (4), 237-270.
74. Jackson, S., *Architecting resilient systems: Accident avoidance and survival and recovery from disruptions*. John Wiley & Sons: 2009; Vol. 66.
75. Dekker, S.; Hollnagel, E.; Woods, D.; Cook, R., Resilience Engineering: New directions for measuring and maintaining safety in complex systems. *Lund University School of Aviation* **2008**.

76. Jain, P.; Pasman, H. J.; Waldram, S.; Pistikopoulos, E.; Mannan, M. S., Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. *Journal of Loss Prevention in the Process Industries* **2018**, *53*, 61-73.
77. Modarres, M., *Risk analysis in engineering: techniques, tools, and trends*. CRC press: 2006.
78. Zeng, Z.; Zio, E., An integrated modeling framework for quantitative business continuity assessment. *Process Safety and Environmental Protection* **2017**, *106*, 76-88.
79. Kletz, T. A., What you don't have, can't leak. *Chemistry and Industry* **1978**, *6*, 287-292.
80. Rusli, R.; Shariff, A. M., Qualitative assessment for inherently safer design (QAISD) at preliminary design stage. *Journal of Loss Prevention in the Process Industries* **2010**, *23* (1), 157-165.
81. Gentile, M.; Rogers, W.; Mannan, M., Development of a fuzzy logic-based inherent safety index. *Process Safety and Environmental Protection* **2003**, *81* (6), 444-456.
82. Heikkila, A. In *An index-based approach for the evaluation of inherent safety in process plant design*, Proceedings of ESREL, 2000; pp 15-17.
83. Tugnoli, A.; Landucci, G.; Cozzani, V. In *Quantitative inherent safety assessment by key performance indicators (KPIs)*, 9th International Conference on Chemical and Process Engineering17, Citeseer: 2009; pp 457-462.
84. Kletz, T. A., Inherently safer design—its scope and future. *Process Safety and Environmental Protection* **2003**, *81* (6), 401-405.

85. Mannan, M. S.; Reyes-Valdes, O.; Jain, P.; Tamim, N.; Ahammad, M., The evolution of process safety: current status and future direction. *Annual review of chemical and biomolecular engineering* **2016**, *7*, 135-162.
86. CCPS, *Guidelines for Risk Based Process Safety*. John Wiley & Sons, Hoboken, NJ 2007.
87. Mannan, M. S.; West, H. H.; Krishna, K.; Aldeeb, A. A.; Keren, N.; Saraf, S. R.; Liu, Y.-S.; Gentile, M., The legacy of Bhopal: the impact over the last 20 years and future direction. *Journal of Loss Prevention in the Process Industries* **2005**, *18* (4), 218-224.
88. Paté-Cornell, M. E., Uncertainties in risk analysis: Six levels of treatment. *Reliability Engineering & System Safety* **1996**, *54* (2-3), 95-111.
89. Khan, F. I.; Abbasi, S., Techniques and methodologies for risk analysis in chemical process industries. *Journal of loss Prevention in the Process Industries* **1998**, *11* (4), 261-277.
90. Phimister, J. R.; Oktem, U.; Kleindorfer, P. R.; Kunreuther, H., Near-miss incident management in the chemical process industry. *Risk Analysis* **2003**, *23* (3), 445-459.
91. Harms-Ringdahl, L., Relationships between accident investigations, risk analysis, and safety management. *Journal of Hazardous materials* **2004**, *111* (1), 13-19.
92. Reniers, G.; Dullaert, W.; Ale, B.; Soudan, K., The use of current risk analysis tools evaluated towards preventing external domino accidents. *Journal of loss prevention in the process industries* **2005**, *18* (3), 119-126.
93. Ferdous, R.; Khan, F.; Sadiq, R.; Amyotte, P.; Veitch, B., Fault and event tree analyses for process systems risk analysis: uncertainty handling formulations. *Risk Analysis* **2011**, *31* (1), 86-107.

94. Pariyani, A.; Seider, W.; Oktem, U.; Soroush, M., Improving process safety and product quality using large databases. In *Computer Aided Chemical Engineering*, Elsevier: 2010; Vol. 28, pp 175-180.
95. Pariyani, A.; Seider, W. D.; Oktem, U. G.; Soroush, M., Dynamic risk analysis using alarm databases to improve process safety and product quality: Part I—Data compaction. *AIChE Journal* **2012**, *58* (3), 812-825.
96. Pariyani, A.; Seider, W. D.; Oktem, U. G.; Soroush, M., Dynamic risk analysis using alarm databases to improve process safety and product quality: Part II—Bayesian analysis. *AIChE Journal* **2012**, *58* (3), 826-841.
97. Khakzad, N.; Khan, F.; Amyotte, P., Risk-based design of process systems using discrete-time Bayesian networks. *Reliability Engineering & System Safety* **2013**, *109*, 5-17.
98. Rae, A.; Alexander, R.; McDermid, J., Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment. *Reliability Engineering & System Safety* **2014**, *125*, 67-81.
99. Noroozi, A.; Khan, F.; MacKinnon, S.; Amyotte, P.; Deacon, T., Determination of human error probabilities in maintenance procedures of a pump. *Process Safety and Environmental Protection* **2014**, *92* (2), 131-141.
100. Paltrinieri, N.; Khan, F.; Cozzani, V., Coupling of advanced techniques for dynamic risk management. *Journal of Risk Research* **2015**, *18* (7), 910-930.
101. Villa, V.; Paltrinieri, N.; Khan, F.; Cozzani, V., Towards dynamic risk analysis: a review of the risk assessment approach and its limitations in the chemical process industry. *Safety science* **2016**, *89*, 77-93.

102. Pasman, H. J.; Rogers, W. J.; Mannan, M. S., Risk assessment: What is it worth? Shall we just do away with it, or can it do a better job? *Safety Science* **2017**.
103. Hollnagel, E.; Nemeth, C. P.; Dekker, S., *Resilience engineering perspectives: remaining sensitive to the possibility of failure*. Ashgate Publishing, Ltd.: 2008; Vol. 1.
104. Zhao, B.; Tang, T.; Ning, B., System dynamics approach for modelling the variation of organizational factors for risk control in automatic metro. *Safety Science* **2017**, *94*, 128-142.
105. Richmond, B. In *System dynamics/systems thinking: Let's just get on with it*, International systems dynamics conference, Sterling, Scotland, 1994.
106. Black, J.; Koopman, P. In *System safety as an emergent property in composite systems*, Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on, IEEE: 2009; pp 369-378.
107. Lewes, G. H., *Problems of life and mind*. Trübner & Company: 1877.
108. Clark, J. O. In *System of systems engineering and family of systems engineering from a standards, V-model, and dual-V model perspective*, Systems Conference, 2009 3rd Annual IEEE, IEEE: 2009; pp 381-387.
109. Bhamra, R.; Dani, S.; Burnard, K., Resilience: the concept, a literature review and future directions. *International Journal of Production Research* **2011**, *49* (18), 5375-5393.
110. Costella, M. F.; Saurin, T. A.; de Macedo Guimarães, L. B., A method for assessing health and safety management systems from the resilience engineering perspective. *Safety Science* **2009**, *47* (8), 1056-1067.
111. Kassam, S. A.; Poor, H. V., Robust techniques for signal processing: A survey. *Proceedings of the IEEE* **1985**, *73* (3), 433-481.

112. Chin, C. D.; Laksanasopin, T.; Cheung, Y. K.; Steinmiller, D.; Linder, V.; Parsa, H.; Wang, J.; Moore, H.; Rouse, R.; Umvilighozo, G., Microfluidics-based diagnostics of infectious diseases in the developing world. *Nature medicine* **2011**, *17* (8), 1015-1019.
113. Mardor, Y.; Pfeffer, R.; Spiegelmann, R.; Roth, Y.; Maier, S. E.; Nissim, O.; Berger, R.; Glicksman, A.; Baram, J.; Orenstein, A., Early detection of response to radiation therapy in patients with brain malignancies using conventional and high b-value diffusion-weighted magnetic resonance imaging. *Journal of Clinical Oncology* **2003**, *21* (6), 1094-1100.
114. Zolghadri, A., Early warning and prediction of flight parameter abnormalities for improved system safety assessment. *Reliability Engineering & System Safety* **2002**, *76* (1), 19-27.
115. Tillotson, B. J., Systems and methods for early detection of aircraft approach to volcanic plume. Google Patents: 2013.
116. Dorr, R.; Kratz, F.; Ragot, J.; Loisy, F.; Germain, J.-L., Detection, isolation, and identification of sensor faults in nuclear power plants. *IEEE Transactions on Control Systems Technology* **1996**, *5* (1), 42-60.
117. Ma, J.; Jiang, J., Applications of fault detection and diagnosis methods in nuclear power plants: A review. *Progress in nuclear energy* **2011**, *53* (3), 255-266.
118. Sirola, M.; Talonen, J.; Lampi, G. In *SOM based methods in early fault detection of nuclear industry*, ESANN, 2009.
119. Chitra, K.; Subashini, B., Data mining techniques and its applications in banking sector. *International Journal of Emerging Technology and Advanced Engineering* **2013**, *3* (8), 219-226.

120. Van Vlasselaer, V.; Bravo, C.; Caelen, O.; Eliassi-Rad, T.; Akoglu, L.; Snoeck, M.; Baesens, B., APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems* **2015**, *75*, 38-48.
121. Callum, J. L.; Kaplan, H. S.; Merkley, L. L.; Pinkerton, P. H.; Rabin Fastman, B.; Romans, R. A.; Coovadia, A. S.; Reis, M. D., Reporting of near-miss events for transfusion medicine: improving transfusion safety. *Transfusion* **2001**, *41* (10), 1204-1211.
122. Dillon, R. L.; Tinsley, C. H.; Cronin, M., Why Near-Miss Events Can Decrease an Individual's Protective Response to Hurricanes. *Risk Analysis* **2011**, *31* (3), 440-449.
123. Wu, W.; Yang, H.; Chew, D. A.; Yang, S.-h.; Gibb, A. G.; Li, Q., Towards an autonomous real-time tracking system of near-miss accidents on construction sites. *Automation in Construction* **2010**, *19* (2), 134-141.
124. Knegtering, B.; Pasman, H., The safety barometer: how safe is my plant today? Is instantaneously measuring safety level utopia or realizable? *Journal of Loss Prevention in the Process Industries* **2013**, *26* (4), 821-829.
125. Jones, S.; Kirchsteiger, C.; Bjerke, W., The importance of near miss reporting to further improve safety performance. *Journal of Loss Prevention in the process industries* **1999**, *12* (1), 59-67.
126. Leger, R. P.; Garland, W. J.; Poehlman, W. S., Fault detection and diagnosis using statistical control charts and artificial neural networks. *Artificial intelligence in engineering* **1998**, *12* (1), 35-47.
127. Zaldivar-Comenges, J.-M., AWARE Advanced Warning Against Runaway Events. *GIT LABORATORY JOURNAL* **2000**, *4*, 96-97.

128. Misra, M.; Yue, H. H.; Qin, S. J.; Ling, C., Multivariate process monitoring and fault diagnosis by multi-scale PCA. *Computers & Chemical Engineering* **2002**, *26* (9), 1281-1293.
129. Venkatasubramanian, V.; Rengaswamy, R.; Yin, K.; Kavuri, S. N., A review of process fault detection and diagnosis: Part I: Quantitative model-based methods. *Computers & chemical engineering* **2003**, *27* (3), 293-311.
130. Venkatasubramanian, V.; Rengaswamy, R.; Kavuri, S. N.; Yin, K., A review of process fault detection and diagnosis: Part III: Process history based methods. *Computers & chemical engineering* **2003**, *27* (3), 327-346.
131. Qian, Y.; Li, X.; Jiang, Y.; Wen, Y., An expert system for real-time fault diagnosis of complex chemical processes. *Expert Systems with Applications* **2003**, *24* (4), 425-432.
132. Rathnayaka, S.; Khan, F.; Amyotte, P., SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. *Process safety and environmental protection* **2011**, *89* (3), 151-164.
133. Casson, V.; Lister, D. G.; Milazzo, M. F.; Maschio, G., Comparison of criteria for prediction of runaway reactions in the sulphuric acid catalyzed esterification of acetic anhydride and methanol. *Journal of Loss Prevention in the Process Industries* **2012**, *25* (1), 209-217.
134. Yu, J., A nonlinear kernel Gaussian mixture model based inferential monitoring approach for fault detection and diagnosis of chemical processes. *Chemical Engineering Science* **2012**, *68* (1), 506-519.
135. Reniers, G.; Amyotte, P., Prevention in the chemical and process industries: Future directions. *Journal of Loss Prevention in the Process Industries* **2012**, *25* (1), 227-231.

136. Paltrinieri, N.; Øien, K.; Cozzani, V., Assessment and comparison of two early warning indicator methods in the perspective of prevention of atypical accident scenarios. *Reliability Engineering & System Safety* **2012**, *108*, 21-31.
137. Paltrinieri, N.; Tugnoli, A.; Buston, J.; Wardman, M.; Cozzani, V., Dynamic procedure for atypical scenarios identification (DyPASI): a new systematic HAZID tool. *Journal of Loss Prevention in the Process Industries* **2013**, *26* (4), 683-695.
138. Barton, P. I. *Industrial Experience With Dynamic Simulation*; Department of Chemical Engineering Massachusetts Institute of Technology Cambridge, MA MA, 1997.
139. Pistikopoulos, E. N.; Diangelakis, N. A., Towards the integration of process design, control and scheduling: are we getting closer? *Computers & Chemical Engineering* **2016**, *91*, 85-92.
140. Straub, D. A.; Grossmann, I. E., Design optimization of stochastic flexibility. *Computers & Chemical Engineering* **1993**, *17* (4), 339-354.
141. Vassiliadis, C.; Pistikopoulos, E. In *Chemical-process design and maintenance optimization under uncertainty: A simultaneous approach*, Reliability and Maintainability Symposium, 1999. Proceedings. Annual, IEEE: 1999; pp 78-83.
142. Thomaidis, T.; Pistikopoulos, E., Towards the incorporation of flexibility, maintenance and safety in process design. *Computers & chemical engineering* **1995**, *19*, 687-692.
143. Morari, M., Flexibility and resiliency of process systems. *Computers & chemical engineering* **1983**, *7* (4), 423-437.
144. Keller, A.; Al-Madhari, A., Risk management and disasters. *Disaster Prevention and Management: An International Journal* **1996**, *5* (5), 19-22.

145. Rinaldi, S. M. In *Modeling and simulating critical infrastructures and their interdependencies*, System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on, IEEE: 2004; p 8 pp.
146. Qureshi, Z. H.; Ashraf, M. A.; Amer, Y. In *Modeling industrial safety: A sociotechnical systems perspective*, Industrial Engineering and Engineering Management, 2007 IEEE International Conference on, IEEE: 2007; pp 1883-1887.
147. Skogdalen, J. E.; Vinnem, J. E., Combining precursor incidents investigations and QRA in oil and gas industry. *Reliability Engineering & System Safety* **2012**, *101*, 48-58.
148. Reniers, G. L.; Sörensen, K.; Dullaert, W., A multi-attribute Systemic Risk Index for comparing and prioritizing chemical industrial areas. *Reliability Engineering & System Safety* **2012**, *98* (1), 35-42.
149. Ferdous, R.; Khan, F.; Sadiq, R.; Amyotte, P.; Veitch, B., Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach. *Process Safety and Environmental Protection* **2013**, *91* (1), 1-18.
150. Albalawi, F.; Durand, H.; Christofides, P. D., Process operational safety using model predictive control based on a process Safeness Index. *Computers & Chemical Engineering* **2017**, *104*, 76-88.
151. Savage, G.; Franz, A.; Wasek, J. S. In *A holacratic socio-technical system architecture*, Systems Engineering (ISSE), 2016 IEEE International Symposium on, IEEE: 2016; pp 1-6.
152. Cameron, I.; Mannan, S.; Németh, E.; Park, S.; Pasman, H.; Rogers, W.; Seligmann, B., Process hazard analysis, hazard identification and scenario definition: Are

the conventional tools sufficient, or should and can we do much better? *Process Safety and Environmental Protection* **2017**.

153. Hollnagel, E., *FRAM, the functional resonance analysis method: modelling complex socio-technical systems*. Ashgate Publishing, Ltd.: 2012.

154. Hollnagel, E., Is safety a subject for science? *Safety Science* **2014**, *67*, 21-24.

155. Eurocontrol Safety, D., *From Safety-I to Safety-II: A White Paper*. Brussels, Belgium: European Organisation for the Safety of Air Navigation (Eurocontrol): 2013.

156. Bruneau, M.; Chang, S. E.; Eguchi, R. T.; Lee, G. C.; O'Rourke, T. D.; Reinhorn, A. M.; Shinozuka, M.; Tierney, K.; Wallace, W. A.; von Winterfeldt, D., A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake spectra* **2003**, *19* (4), 733-752.

157. Leveson, N. G.; Daouk, M.; Dulac, N.; Marais, K., Applying STAMP in accident analysis. **2003**.

158. Wreathall, J., Properties of resilient organizations: an initial view. *Resilience engineering: Concepts and precepts* **2006**, 275-285.

159. Shirali, G.; Mohammadfam, I.; Motamedzade, M.; Ebrahimipour, V.; Moghimbeigi, A., Assessing resilience engineering based on safety culture and managerial factors. *Process Safety Progress* **2012**, *31* (1), 17-18.

160. Huber, S.; van Wijgerden, I.; de Witt, A.; Dekker, S. W., Learning from organizational incidents: Resilience engineering for high-risk process environments. *Process Safety Progress* **2009**, *28* (1), 90-95.

161. Huber, G. J.; Gomes, J. O.; de Carvalho, P. V. R., A program to support the construction and evaluation of resilience indicators. *Work* **2012**, *41* (Supplement 1), 2810-2816.
162. Jain, P.; Pasman, H. J.; Waldram, S. P.; Rogers, W. J.; Mannan, M. S., Did we learn about risk control since Seveso? Yes, we surely did, but is it enough? An historical brief and problem analysis. *Journal of Loss Prevention in the Process Industries* **2016**.
163. Westerterp, K.; Molga, E., Safety and runaway prevention in batch and semibatch reactors—a review. *Chemical Engineering Research and Design* **2006**, *84* (7), 543-552.
164. Goel, P.; Datta, A.; Mannan, M. S. In *Application of big data analytics in process safety and risk management*, Big Data (Big Data), 2017 IEEE International Conference on, IEEE: 2017; pp 1143-1152.
165. Goel, P.; Datta, A.; Mannan, M. S., Industrial alarm systems: Challenges and opportunities. *Journal of Loss Prevention in the Process Industries* **2017**, *50*, 23-36.
166. McDaniels, T.; Chang, S.; Cole, D.; Mikawoz, J.; Longstaff, H., Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. *Global Environmental Change* **2008**, *18* (2), 310-318.
167. CCPS Process Safety Glossary. <https://www.aisce.org/ccps/resources/glossary> (accessed 01/25/2017).
168. CCPS, C. f. C. P. S., *Guidelines for Process Safety Metrics*. 2010.
169. API, R., 754 Process Safety Performance Indicators for the Refining and Petrochemical Industries. *American Petroleum Institute, Washington DC* **2010**.

170. Tugnoli, A.; Landucci, G.; Salzano, E.; Cozzani, V., Supporting the selection of process and plant design options by Inherent Safety KPIs. *Journal of Loss Prevention in the Process Industries* **2012**, 25 (5), 830-842.
171. Khan, F.; Abunada, H.; John, D.; Benmosbah, T., Development of risk-based process safety indicators. *Process Safety Progress* **2010**, 29 (2), 133-143.
172. HSE; Association, C. I., Developing process safety indicators. A step-by-step guide for chemical and major hazard industries. *Health and Safety Executive* **2006**.
173. CCPS, Process safety leading and lagging metrics. *Center for Chemical Process Safety* **2007**.
174. OECD *Guidance on Developing Safety Performance Indicators Related to Chemical Accident Prevention, Preparedness and Response*; 2008.
175. IOGP, Process safety: recommended practice on key performance indicators. *International Association of Oil and Gas Producers* **2011**, (Report number 456).
176. Wang, M.; Mentzer, R. A.; Gao, X.; Richardson, J.; Mannan, M. S., Normalization of process safety lagging metrics. *Process Safety Progress* **2013**, 32 (4), 337-345.
177. Petroleum Safety Authority, Trends in risk level in the petroleum activity. 2015.
178. Swuste, P.; Theunissen, J.; Schmitz, P.; Reniers, G.; Blokland, P., Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries* **2016**, 40, 162-173.
179. Hollnagel, E., The four cornerstones of resilience engineering. Ashgate: 2009.
180. Øien, K.; Massaiu, S.; Tinmannsvik, R.; Størseth, F. In *Development of early warning indicators based on resilience engineering*, Submitted to PSAM10, International Probabilistic Safety Assessment and Management Conference, 2010; pp 7-11.

181. Tveiten, C. K.; Albrechtsen, E.; Wærø, I.; Wahl, A. M., Building resilience into emergency management. *Safety science* **2012**, *50* (10), 1960-1966.
182. Jain, P.; Pasman, H. J.; Waldram, S.; Pistikopoulos, E.; Mannan, M. S., Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. *Journal of Loss Prevention in the Process Industries* **2017**.
183. Hopkins, A., *Failure to learn: the BP Texas City refinery disaster*. CCH Australia Ltd: 2008.
184. R Development Core Team *R: A language and environment for statistical computing*. R Foundation for Statistical Computing, R Foundation for Statistical Computing: Vienna, Austria, 2014.
185. Fox, J., and Bouchet-Valat, M. *Rcmdr: R Commander*. R package, 2.3-2.; 2017.
186. Mangiafico, S. *rcompanion: Functions to Support Extension Education Program Evaluation*, 1.5. 6. ; 2017.
187. Ogle, D. *FSA: Fisheries stock analysis*. R package 0.8. 13; 2017.
188. Revelle, W. *psych: Procedures for Personality and Psychological Research*. Northwestern University: Evanston, 1.7.5; Illinois, USA, 2017.
189. Sarkar, D., *Lattice: multivariate data visualization with R*. Springer Science & Business Media: 2008.
190. George, D.; Mallery, P., *SPSS for Windows step by step: A simple guide and reference*, 11.0 atualização (4ª edição). Boston: Allyn & Bacon: 2003.
191. Gadermann, A. M.; Guhn, M.; Zumbo, B. D., Estimating ordinal reliability for Likert-type and ordinal item response data: A conceptual, empirical, and practical guide. *Practical Assessment, Research & Evaluation* **2012**, *17* (3), 1-13.

192. Sijtsma, K., On the use, the misuse, and the very limited usefulness of Cronbach's alpha. *Psychometrika* **2009**, 74 (1), 107.
193. Zumbo, B. D.; Gadermann, A. M.; Zeisser, C., Ordinal versions of coefficients alpha and theta for Likert rating scales. *Journal of modern applied statistical methods* **2007**, 6 (1), 4.
194. Viswanathan, S.; Zhao, J.; Venkatsubramanian, V.; Mockus, L.; Vinson, J.; Noren, A.; Basu, P. K., Integrating operating procedure synthesis and hazards analysis automation tools for batch processes. *Computers & Chemical Engineering* **1999**, 23, S747-S750.
195. Field, A., *Discovering statistics using SPSS*. Sage publications: 2009.
196. Bonzo, S. M.; McLain, D.; Avnet, M. S., Process Modeling in the Operating Room: A Socio-Technical Systems Perspective. *Systems Engineering* **2016**, 19 (3), 267-277.
197. Avnet, M. S.; Weigel, A. L., An application of the design structure matrix to integrated concurrent engineering. *Acta Astronautica* **2010**, 66 (5), 937-949.
198. ISA, ANSI/ISA-88.00.01-2010, Batch Control Part 1: Models and Terminology. 2010.
199. Sosa, M. E.; Eppinger, S. D.; Rowles, C. M., The misalignment of product architecture and organizational structure in complex product development. *Management science* **2004**, 50 (12), 1674-1689.
200. Avnet, M. S., A Network-Based Analysis of Team Coordination and Shared Cognition in Systems Engineering. *Systems Engineering* **2016**.
201. Dunj3, J.; Fthenakis, V.; V3lchez, J. A.; Arnaldos, J., Hazard and operability (HAZOP) analysis. A literature review. *Journal of hazardous materials* **2010**, 173 (1), 19-32.

202. Khan, F.; Rathnayaka, S.; Ahmed, S., Methods and models in process safety and risk management: Past, present and future. *Process Safety and Environmental Protection* **2015**, *98*, 116-147.
203. Kaszniak, M., Oversights and omissions in process hazard analyses: Lessons learned from CSB investigations. *Process Safety Progress* **2010**, *29* (3), 264-269.
204. Suokas, J., The role of safety analysis in accident prevention. *Accident Analysis & Prevention* **1988**, *20* (1), 67-85.
205. Suokas, J.; Rouhiainen, V., Quality control in safety and risk analyses. *Journal of loss prevention in the process industries* **1989**, *2* (2), 67-77.
206. Zhao, D.; McCoy, A. P.; Kleiner, B. M.; Smith-Jackson, T. L.; Liu, G., Sociotechnical systems of fatal electrical injuries in the construction industry. *Journal of Construction Engineering and Management* **2015**, *142* (1), 04015056.
207. Katz, D.; Kahn, R. L., The social psychology of organizations. **1978**, *2*.
208. Kleiner, B. M., Macroergonomics: analysis and design of work systems. *Applied ergonomics* **2006**, *37* (1), 81-89.
209. Pasmore, W. A.; Sherwood, J. J., *Sociotechnical systems: A sourcebook*. Pfeiffer & Co: 1978.
210. Gressel, M. G.; Gideon, J. A., An overview of process hazard evaluation techniques. *The American Industrial Hygiene Association Journal* **1991**, *52* (4), 158-163.
211. Hoepffner, L., Analysis of the HAZOP study and comparison with similar safety analysis systems. *Gas Separation & Purification* **1989**, *3* (3), 148-151.

212. Knowlton, R. E., Introduction to hazard and operability studies: the guide word approach. In *Introduction to hazard and operability studies: the guide word approach*, Chemetics International Company: 1987.
213. Lawley, H., Operability studies and hazard analysis. *Chemical Engineering Progress* **1974**, 70 (4), 45-56.
214. Khan, F. I.; Abbasi, S., OptHAZOP—an effective and optimum approach for HAZOP study. *Journal of Loss Prevention in the Process Industries* **1997**, 10 (3), 191-204.
215. Khan, F. I.; Abbasi, S., TOPHAZOP: a knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner. *Journal of loss prevention in the process industries* **1997**, 10 (5), 333-343.
216. Khan, F. I.; Abbasi, S., Towards automation of HAZOP with a new tool EXPERTOP. *Environmental Modelling & Software* **2000**, 15 (1), 67-77.
217. Venkatasubramanian, V.; Zhao, J.; Viswanathan, S., Intelligent systems for HAZOP analysis of complex process plants. *Computers & Chemical Engineering* **2000**, 24 (9), 2291-2302.
218. Wang, F.; Gao, J.; Wang, H., A new intelligent assistant system for HAZOP analysis of complex process plant. *Journal of Loss Prevention in the Process Industries* **2012**, 25 (3), 636-642.
219. Palmer, C.; Chung, P., A computer tool for batch hazard and operability studies. *Journal of Loss Prevention in the Process Industries* **2008**, 21 (5), 537-542.
220. Srinivasan, R.; Venkatasubramanian, V., Petri net-digraph models for automating HAZOP analysis of batch process plants. *Computers & chemical engineering* **1996**, 20, S719-S725.

221. Srinivasan, R.; Venkatasubramanian, V., Automating HAZOP analysis of batch chemical plants: Part I. The knowledge representation framework. *Computers & chemical engineering* **1998**, *22* (9), 1345-1355.
222. Srinivasan, R.; Venkatasubramanian, V., Automating HAZOP analysis of batch chemical plants: Part II. Algorithms and application. *Computers & chemical engineering* **1998**, *22* (9), 1357-1370.
223. Viswanathan, S.; Shah, N.; Venkatasubramanian, V., A hybrid strategy for batch process hazards analysis. *Computers & Chemical Engineering* **2000**, *24* (2), 545-549.
224. Cameron, I.; Hangos, K.; Lakner, R.; Nemeth, E.; Seligmann, B. In *The P3 formalism: A basis for improved diagnosis in complex systems*, Chemeca 2007: Academia and Industry Strengthening the Profession, Engineers Australia: 2007; pp 1077-1088.
225. Cameron, I.; Seligmann, B.; Hangos, K.; Németh, E.; Lakner, R. In *A functional systems approach to the development of improved hazard identification for advanced diagnostic systems*, ESCAPE-18 Conference, Citeseer: 2008.
226. Seligmann, B.; Németh, E.; Hockings, K.; McDonald, I.; Lee, J.; O'Brien, C.; Hangos, K.; Cameron, I. In *A structured, blended hazard identification framework for advanced process diagnosis*, 13th International Symposium on Loss Prevention and Safety Promotion in the Process Industries (Loss Prevention 2010), 2010; pp 6-9.
227. Vaidhyanathan, R.; Venkatasubramanian, V., Digraph-based models for automated HAZOP analysis. *Reliability Engineering & System Safety* **1995**, *50* (1), 33-49.
228. Liu, T.; Chiou, S., The application of Petri nets to failure analysis. *Reliability Engineering & System Safety* **1997**, *57* (2), 129-142.

229. Kennedy, R.; Kirwan, B., Development of a hazard and operability-based method for identifying safety management vulnerabilities in high risk systems. *Safety Science* **1998**, *30* (3), 249-274.
230. Redmill, F.; Chudleigh, M.; Catmur, J., System Safety: HAZOP and Software HAZOP. *Industrial Management & Data Systems* **2000**, *100* (1), 46-48.
231. Baybutt, P., Layers of protection analysis for human factors (LOPA-HF). *Process Safety Progress* **2002**, *21* (2), 119-129.
232. Baybutt, P., Major hazards analysis: An improved method for process hazard analysis. *Process Safety Progress* **2003**, *22* (1), 21-26.
233. Leveson, N.; Dulac, N.; Zipkin, D.; Cutcher-Gershenfeld, J.; Carroll, J.; Barrett, B., Engineering resilience into safety-critical systems. *Resilience Engineering—Concepts and Precepts. Ashgate Aldershot* **2006**, 95-123.
234. Kariuki, S.; Löwe, K., Integrating human factors into process hazard analysis. *Reliability Engineering & System Safety* **2007**, *92* (12), 1764-1773.
235. Jackson, S. In *6.1. 3 System Resilience: Capabilities, Culture and Infrastructure*, INCOSE International Symposium, Wiley Online Library: 2007; pp 885-899.
236. Seligmann, B. J.; Nemeth, E.; Hockings, K.; O'Brien, C.; Cameron, I. T., A blended hazard identification approach to support intelligent diagnosis in process systems. *Engineering Our Future: Are We up to the Challenge?: 27-30 September 2009, Burswood Entertainment Complex* **2009**, 960.
237. Leveson, N.; Dulac, N.; Marais, K.; Carroll, J., Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems. *Organization studies* **2009**, *30* (2-3), 227-249.

238. Khakzad, N.; Khan, F.; Amyotte, P., Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection* **2013**, *91* (1), 46-53.
239. Ericson, C. A., *Hazard analysis techniques for system safety*. John Wiley & Sons: 2015.
240. Xin, P.; Khan, F.; Ahmed, S., Dynamic hazard identification and scenario mapping using Bayesian network. *Process Safety and Environmental Protection* **2017**, *105*, 143-155.
241. Cagno, E.; Caron, F.; Mancini, M., Risk analysis in plant commissioning: the Multilevel Hazop. *Reliability Engineering & System Safety* **2002**, *77* (3), 309-323.
242. Johnson, W. G., MORT: The Management Oversight and Risk Tree. *Journal of safety research* **1975**.
243. Leveson, N. G., Model-based analysis of socio-technical risk. **2004**.
244. Hassall, M. E.; Sanderson, P. M.; Cameron, I. T., The development and testing of SAfER: a resilience-based human factors method. *Journal of Cognitive Engineering and Decision Making* **2014**, *8* (2), 162-186.
245. Hollnagel, E., *FRAM: the functional resonance analysis method: modelling complex socio-technical systems*. CRC Press: 2017.
246. Hollnagel, E., *Barriers and accident prevention*. Routledge: 2016.
247. Baybutt, P., Insights into process safety incidents from an analysis of CSB investigations. *Journal of Loss Prevention in the Process Industries* **2016**, *43*, 537-548.

248. Raman, J.; Gargett, A.; Warner, D. In *Application of Hazop techniques for maintenance safety on offshore installations*, SPE Health, Safety and Environment in Oil and Gas Exploration and Production Conference, Society of Petroleum Engineers: 1991.
249. Schurman, D. L.; Fleger, S. A., Human factors in HAZOPs: Guide words and parameters. *Professional Safety* **1994**, 39 (12), 32.
250. Reiman, T.; Rollenhagen, C., Does the concept of safety culture help or hinder systems thinking in safety? *Accident Analysis & Prevention* **2014**, 68, 5-15.
251. Reason, J., *Human error*. Cambridge university press: 1990.
252. Svenson, O., The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis* **1991**, 11 (3), 499-507.
253. Palazzi, E.; Currò, F.; Fabiano, B., A critical approach to safety equipment and emergency time evaluation based on actual information from the Bhopal gas tragedy. *Process safety and environmental protection* **2015**, 97, 37-48.
254. Venart, J., Flixborough: a final footnote. *Journal of Loss Prevention in the process industries* **2007**, 20 (4), 621-643.
255. Holmstrom, D.; Altamirano, F.; Banks, J.; Joseph, G.; Kaszniak, M.; Mackenzie, C.; Shroff, R.; Cohen, H.; Wallace, S., CSB investigation of the explosions and fire at the BP Texas City refinery on March 23, 2005. *Process safety progress* **2006**, 25 (4), 345-349.
256. Stephans, R. A., *System safety for the 21st century: The updated and revised edition of system safety 2000*. John Wiley & Sons: 2012.
257. Trist, E.; Bamforth, K., Some social and psychological consequences of the Longwall method. *Human relations* **1951**, 4 (3), 3-38.

258. Galán, S. F.; Mosleh, A.; Izquierdo, J., Incorporating organizational factors into probabilistic safety assessment of nuclear power plants through canonical probabilistic models. *Reliability Engineering & System Safety* **2007**, *92* (8), 1131-1138.
259. Giardina, M.; Morale, M., Safety study of an LNG regasification plant using an FMECA and HAZOP integrated methodology. *Journal of Loss Prevention in the Process Industries* **2015**, *35*, 35-45.
260. Beale, C., Recent railway industry accidents: learning points for the process industries. *Process safety and environmental protection* **2002**, *80* (1), 25-32.
261. Vairo, T.; Quagliati, M.; Del Giudice, T.; Barbucci, A.; Fabiano, B., From land-to water-use-planning: a consequence based case-study related to cruise ship risk. *Safety science* **2017**, *97*, 120-133.
262. Cheung, J.-Y.; Stephanopoulos, G., Representation of process trends—Part I. A formal representation framework. *Computers & Chemical Engineering* **1990**, *14* (4), 495-510.
263. Janusz, M. E.; Venkatasubramanian, V., Automatic generation of qualitative descriptions of process trends for fault detection and diagnosis. *Engineering Applications of Artificial Intelligence* **1991**, *4* (5), 329-339.
264. Rengaswamy, R.; Venkatasubramanian, V., A syntactic pattern-recognition approach for process monitoring and fault diagnosis. *Engineering Applications of Artificial Intelligence* **1995**, *8* (1), 35-51.
265. CSB *Williams Geismar Olefins Plant Reboiler Rupture and Fire*; 2013-03-I-LA; 2016.

266. Dawson, D. M.; Brooks, B. J., *The Esso Longford gas plant accident: report of the Longford Royal Commission*. Government Printer, South Africa: 1999.
267. Hopkins, A. In *Lessons from Esso's Gas Plant Explosion at Longford*, Lessons From Disasters: Seminar Notes, Institution of Engineers, Australia: 2000; p 17.
268. Lee, A. V.; Vargo, J.; Seville, E., Developing a tool to measure and compare organizations' resilience. *Natural hazards review* **2013**, *14* (1), 29-41.
269. CCPS, C. f. C. P. S., *Guidelines for Risk Based Process Safety*. 2007.
270. Mannan, M. S.; Mentzer, R. A.; Zhang, J., Framework for creating a Best-in-Class safety culture. *Journal of Loss Prevention in the Process Industries* **2013**, *26* (6), 1423-1432.
271. Olive, C.; O'Connor, T. M.; Mannan, M. S., Relationship of safety culture and process safety. *Journal of hazardous materials* **2006**, *130* (1), 133-140.
272. Díaz-Cabrera, D.; Hernandez-Fernaund, E.; Isla-Díaz, R., An evaluation of a new instrument to measure organisational safety culture values and practices. *Accident Analysis & Prevention* **2007**, *39* (6), 1202-1211.
273. Fernández-Muñiz, B.; Montes-Peón, J. M.; Vázquez-Ordás, C. J., Safety culture: Analysis of the causal relationships between its key dimensions. *Journal of safety research* **2007**, *38* (6), 627-641.
274. Wu, T.-C.; Chen, C.-H.; Li, C.-C., A correlation among safety leadership, safety climate and safety performance. *Journal of loss prevention in the process industries* **2008**, *21* (3), 307-318.
275. Rains, B. D. In *Driving operational discipline through quality written procedures*, 2012 Spring Meeting & 8th Global Congress on Process Safety, 2012.

276. Klein, J. A.; Vaughen, B. K., A revised program for operational discipline. *Process Safety Progress* **2008**, *27* (1), 58-65.
277. Forest, J. J., Management discipline. *Process Safety Progress* **2012**, *31* (4), 334-336.
278. Vaughen, B. K.; Klein, J. A., Improving operational discipline to prevent loss of containment incidents. *Process Safety Progress* **2011**, *30* (3), 216-220.
279. Neogy, P.; Hanson, A.; Davis, P.; Fenstermacher, T., Hazard and barrier analysis guidance document. *Department of Energy, Office of Operating Experience Analysis and Feedback, Report No. EH-33* **1996**.
280. Kecklund, L. J.; Edland, A.; Wedin, P.; Svenson, O., Safety barrier function analysis in a process industry: a nuclear power application. *International journal of industrial ergonomics* **1996**, *17* (3), 275-284.
281. Doe, G., Implementation Guide for Use With DOE Order 225.1 A. Accident Investigations. *Doe G* **1997**, *225*, A1.
282. Sklet, S., Hydrocarbon releases on oil and gas production platforms: Release scenarios and safety barriers. *Journal of Loss Prevention in the Process Industries* **2006**, *19* (5), 481-493.
283. Hollnagel, E., The art of efficient man-machine interaction: Improving the coupling between man and machine. *Expertise and technology: cognition & human-computer cooperation* **1995**, 229-241.
284. Taylor, J., Incorporating human error analysis into process plant safety analysis. *Chem Eng Trans* **2013**, *31*, 301-306.

285. Aelion, V.; Powers, G. J., Risk reduction of operating procedures and process flowsheets. *Industrial & engineering chemistry research* **1993**, 32 (1), 82-90.
286. Chudleigh, M.; Clare, J., The benefits of SUSI: Safety analysis of user system interaction. In *SAFECOMP'93*, Springer: 1993; pp 123-132.
287. Latorella, K. A.; Prabhu, P. V., A review of human error in aviation maintenance and inspection. *International Journal of Industrial Ergonomics* **2000**, 26 (2), 133-161.
288. Marucco, D., Simultaneous Operations Risk Assessment. *CHEMICAL ENGINEERING TRANSACTIONS* **2016**, 53, 115-120.
289. Singh, E. B., SIMOPs – Simultaneous Operations in Oil and Gas Installations and work Sites. *International Journal of Innovative Science, Engineering & Technology* **2016**, 3 (3), 19-23.
290. Jain, P.; Reese, A. M.; Chaudhari, D.; Mentzer, R. A.; Mannan, M. S., Regulatory approaches-Safety case vs US approach: Is there a best solution today? *Journal of Loss Prevention in the Process Industries* **2017**, 46, 154-162.
291. Baybutt, P., Requirements for improved process hazard analysis (PHA) methods. *Journal of Loss Prevention in the Process Industries* **2014**, 32, 182-191.
292. S.W. Ostrowski, K. K. K., A HAZOP Methodology for Transient Operations. In *Mary Kay O'Connor Process Safety Symposium*, Mary Kay O'Connor Process Safety Center International Symposium: College Station, TX, 2008.
293. Sundarraman, A.; Srinivasan, R., Monitoring transitions in chemical plants using enhanced trend analysis. *Computers & chemical engineering* **2003**, 27 (10), 1455-1472.
294. Nimmo, I., Start up plants safely. *Chemical Engineering Progress* **1993**, 89 (12), 66-70.

295. CCPS, C. f. C. P. S., *Guidelines for hazard evaluation procedures*. Third ed.; 2008.
296. Kletz, T. A., *Learning from accidents*. Routledge: 2001.
297. Jain, P.; Rogers, W. J.; Pasman, H. J.; Keim, K. K.; Mannan, M. S., A Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA) approach: Part I plant system layer. *Process Safety and Environmental Protection* **2018**, *116*, 92-105.
298. OSHA, O. S. H. A., Process safety management of highly hazardous chemicals; explosives and blasting agents; final rule (29 CFR 1910.119). *Washington, DC: US Government Printing Office* **1992**.
299. Wei, C.; Rogers, W. J.; Mannan, M. S., Layer of protection analysis for reactive chemical risk assessment. *Journal of hazardous materials* **2008**, *159* (1), 19-24.
300. Lu, Y.; Ng, D.; Mannan, M. S., Prediction of the reactivity hazards for organic peroxides using the QSPR approach. *Industrial & Engineering Chemistry Research* **2010**, *50* (3), 1515-1522.
301. BS25999, B., 25999-2 Business Continuity Management-Part2: Specification Business Continuity Management. July: 2007.
302. Huang, S.; Chiu, C.-H.; Elliot, D., *LNG: Basics of liquefied natural gas*. University of Texas Continuing Education Petroleum Extension Service: 2007.
303. OSHA, O. S. H. A., CFR 1910.119. *Process Safety Management of Highly Hazardous Chemicals, Explosives and Blasting Agents; Final Rule* **1992**.
304. Kohout, A.; Jain, P.; Dick, W., Review, identification and analysis of local impact of projectile hazard in the LNG industry: A LNG storage tanks case study. *Journal of Loss Prevention in the Process Industries* **2018**.

305. National Association of State Fire Marshalls *National Association of State Fire Marshals. Liquefied natural gas: an overview of the LNG industry for fire marshals and emergency responders*; Washington, D.C., 2005.
306. Woodward, J. L.; Pitbaldo, R., *LNG Risk Based Safety: modeling and consequence analysis*. John Wiley & Sons: 2010.
307. C.H. Safety IV *History of international LNG operations – technical document*; CH IV International, Hanover, USA 2014.
308. US Department of Transportation (DOT) *Failure Investigation Report – Liquefied Natural Gas (LNG) Peak Shaving Plant, Plymouth, Washington* Washington D.C., 4/28/2016 2016.
309. Dweck, J.; Boutillon, S.; Asbill, S., Deadly LNG incident holds key lessons for developers, regulators. *PIPELINE AND GAS JOURNAL* **2004**, 39-42.
310. Verwijs, J. W., Reactor start-up and safeguarding in industrial chemical processes. **1994**.
311. Saada, R.; Patel, D.; Saha, B., Causes and consequences of thermal runaway incidents—will they ever be avoided? *Process Safety and Environmental Protection* **2015**, 97, 109-115.
312. Cataldo, M.; Herbsleb, J. D.; Carley, K. M. In *Socio-technical congruence: a framework for assessing the impact of technical and work dependencies on software development productivity*, Proceedings of the Second ACM-IEEE international symposium on Empirical software engineering and measurement, ACM: 2008; pp 2-11.
313. Bolstad, W. M.; Curran, J. M., *Introduction to Bayesian statistics*. John Wiley & Sons: 2016.

314. Khakzad, N.; Yu, H.; Paltrinieri, N.; Khan, F., Reactive approaches of probability update based on Bayesian methods. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry*, Elsevier: 2017; pp 51-61.
315. Lee, J. H.; Shin, J.; Realff, M. J., Machine learning: Overview of the recent progresses and implications for the process systems engineering field. *Computers & Chemical Engineering* **2017**.
316. Argenti, F.; Landucci, G.; Reniers, G.; Cozzani, V., Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. *Reliability Engineering & System Safety* **2018**, *169*, 515-530.
317. Barua, S.; Gao, X.; Pasman, H.; Mannan, M. S., Bayesian network based dynamic operational risk assessment. *Journal of Loss Prevention in the Process Industries* **2016**, *41*, 399-410.
318. Yun, G.; Rogers, W. J.; Mannan, M. S., Risk assessment of LNG importation terminals using the Bayesian–LOPA methodology. *Journal of Loss Prevention in the Process Industries* **2009**, *22* (1), 91-96.
319. Chiang, L. H.; Jiang, B.; Zhu, X.; Huang, D.; Braatz, R. D., Diagnosis of multiple and unknown faults using the causal map and multivariate statistics. *Journal of Process Control* **2015**, *28*, 27-39.
320. Kiparissides, A.; Kucherenko, S.; Mantalaris, A.; Pistikopoulos, E., Global sensitivity analysis challenges in biological systems modeling. *Industrial & Engineering Chemistry Research* **2009**, *48* (15), 7168-7180.
321. Saltelli, A.; Chan, K.; Scott, E. M., *Sensitivity analysis*. Wiley New York: 2000; Vol. 1.

322. Sobol, I. M., Global sensitivity indices for nonlinear mathematical models and their Monte Carlo estimates. *Mathematics and computers in simulation* **2001**, *55* (1-3), 271-280.
323. Halemane, K. P.; Grossmann, I. E., Optimal process design under uncertainty. *AIChE Journal* **1983**, *29* (3), 425-433.
324. Swaney, R. E.; Grossmann, I. E., An index for operational flexibility in chemical process design. Part I: Formulation and theory. *AIChE Journal* **1985**, *31* (4), 621-630.
325. Grossmann, I. E.; Floudas, C. A., Active constraint strategy for flexibility analysis in chemical processes. *Computers & Chemical Engineering* **1987**, *11* (6), 675-693.
326. Pistikopoulos, E.; Mazzuchi, T., A novel flexibility analysis approach for processes with stochastic parameters. *Computers & Chemical Engineering* **1990**, *14* (9), 991-1000.
327. Dimitriadis, V. D.; Pistikopoulos, E. N., Flexibility analysis of dynamic systems. *Industrial & Engineering Chemistry Research* **1995**, *34* (12), 4451-4462.
328. Marseguerra, M.; Zio, E.; Podofilini, L., Condition-based maintenance optimization by means of genetic algorithms and Monte Carlo simulation. *Reliability Engineering & System Safety* **2002**, *77* (2), 151-165.
329. CSB *Incident data: Reactive hazard investigation.*; Chemical Safety Board: 2003.
330. Nolan, P. F.; Barton, J. A., Some lessons from thermal-runaway incidents. *Journal of hazardous materials* **1987**, *14* (2), 233-239.
331. CCPS, C. f. C. P. S., *Layer of protection analysis: simplified process risk assessment.* Wiley: 2011.
332. Kiparissides, A.; Koutinas, M.; Kontoravdi, C.; Mantalaris, A.; Pistikopoulos, E. N., 'Closing the loop' in biological systems modeling—From the in silico to the in vitro. *Automatica* **2011**, *47* (6), 1147-1155.

333. Li, G.; Wang, S.-W.; Rabitz, H., Practical approaches to construct RS-HDMR component functions. *The Journal of Physical Chemistry A* **2002**, *106* (37), 8721-8733.
334. Robert, C., *The Bayesian choice: from decision-theoretic foundations to computational implementation*. Springer Science & Business Media: 2007.
335. Jain, P.; Mentzer, R.; Mannan, M. S., Resilience metrics for improved process-risk decision making: Survey, analysis and application. *Safety Science* **2018**, *108*, 13-28.
336. Nelder, J. A.; Baker, R. J., *Generalized linear models*. Wiley Online Library: 1972.
337. Venkatasubramanian, V., Systemic failures: challenges and opportunities in risk management in complex systems. *AIChE Journal* **2011**, *57* (1), 2-9.
338. Venkatasubramanian, V.; Zhang, Z., TeCSMART: A hierarchical framework for modeling and analyzing systemic risk in sociotechnical systems. *AIChE Journal* **2016**, *62* (9), 3065-3084.
339. Crowl, D. A.; Louvar, J. F., *Chemical process safety: fundamentals with applications*. Pearson Education: 2001.
340. Frank, P. M., Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results. *automatica* **1990**, *26* (3), 459-474.
341. Hyatt, N., *Guidelines for process hazards analysis (PHA, HAZOP), hazards identification, and risk analysis*. CRC press: 2003.
342. Jain, P.; Rogers, W. J.; Pasman, H. J.; Mannan, M. S., A resilience-based integrated process systems hazard analysis (RIPSHA) approach: Part II management system layer. *Process Safety and Environmental Protection* **2018**, *118*, 115-124.
343. Reason, J., Human error: models and management. *Bmj* **2000**, *320* (7237), 768-770.

344. De Dianous, V.; Fiévez, C., ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. *Journal of Hazardous Materials* **2006**, *130* (3), 220-233.
345. Sklet, S., Safety barriers: Definition, classification, and performance. *Journal of loss prevention in the process industries* **2006**, *19* (5), 494-506.
346. Duijm, N. J.; Goossens, L., Quantifying the influence of safety management on the reliability of safety barriers. *Journal of Hazardous Materials* **2006**, *130* (3), 284-292.
347. Guldenmund, F.; Hale, A.; Goossens, L.; Betten, J.; Duijm, N. J., The development of an audit technique to assess the quality of safety barrier management. *Journal of hazardous materials* **2006**, *130* (3), 234-241.
348. Hollnagel, E. In *Accidents and barriers*, Proceedings of lex valenciennes, Presses Universitaires de Valenciennes: 1999; pp 175-182.
349. Hollnagel, E., Risk+ barriers= safety? *Safety science* **2008**, *46* (2), 221-229.
350. Hayes, J., Use of safety barriers in operational safety decision making. *Safety science* **2012**, *50* (3), 424-432.
351. Léger, A.; Farret, R.; Duval, C.; Levrat, E.; Weber, P.; Iung, B., A safety barriers-based approach for the risk analysis of socio-technical systems. *IFAC Proceedings Volumes* **2008**, *41* (2), 6938-6943.
352. Babcock, G. A., Because temperature matters: maintaining cooling towers. *ASHRAE Journal* **2005**, *47* (3), 46.
353. Dhillon, B. S., *Engineering maintenance: a modern approach*. cRc press: 2002.
354. Mobley, R. K., *An introduction to predictive maintenance*. Butterworth-Heinemann: 2002.

355. Dekker, R., Applications of maintenance optimization models: a review and analysis. *Reliability engineering & system safety* **1996**, *51* (3), 229-240.
356. Tan, J. S.; Kramer, M. A., A general framework for preventive maintenance optimization in chemical process operations. *Computers & Chemical Engineering* **1997**, *21* (12), 1451-1469.
357. Pistikopoulos, E. N.; Vassiliadis, C. G.; Papageorgiou, L. G., Process design for maintainability: an optimization approach. *Computers & Chemical Engineering* **2000**, *24* (2-7), 203-208.
358. Vassiliadis, C.; Pistikopoulos, E., Maintenance scheduling and process optimization under uncertainty. *Computers & Chemical Engineering* **2001**, *25* (2-3), 217-236.
359. Pistikopoulos, E. N.; Vassiliadis, C. G.; Arvela, J.; Papageorgiou, L. G., Interactions of maintenance and production planning for multipurpose process plants a system effectiveness approach. *Industrial & engineering chemistry research* **2001**, *40* (14), 3195-3207.
360. Banjevic, D.; Jardine, A.; Makis, V.; Ennis, M., A control-limit policy and software for condition-based maintenance optimization. *INFOR: Information Systems and Operational Research* **2001**, *39* (1), 32-50.
361. Goel, H. D.; Grievink, J.; Weijnen, M. P., Integrated optimal reliable design, production, and maintenance planning for multipurpose process plants. *Computers & chemical engineering* **2003**, *27* (11), 1543-1555.

362. Mirghani, M. A., Application and implementation issues of a framework for costing planned maintenance. *Journal of Quality in Maintenance Engineering* **2003**, 9 (4), 436-449.
363. Mathew, S., Optimal inspection frequency: A tool for maintenance planning/forecasting. *International Journal of Quality & Reliability Management* **2004**, 21 (7), 763-771.
364. Nguyen, D.; Bagajewicz, M., Optimization of preventive maintenance in chemical process plants. *Industrial & Engineering Chemistry Research* **2010**, 49 (9), 4329-4339.
365. Brooke, A.; Kendrick, D.; Meeraus, A.; Raman, R.; Rasenthal, R., A user's guide, GAMS software. *GAMS Development corporation* **1998**.
366. Crawley, M. J., *The R book*. John Wiley & Sons: 2012.
367. Cooling Technology Institute Cooling Tower Operation and Maintenance for Improved Energy Efficiency. <https://www.cti.org/cgi-bin/download.pl> (accessed 03/27/2018).
368. Donnellan, P. In *Condition monitoring of cooling tower fan gearboxes*, IMECHE CONFERENCE TRANSACTIONS, Professional Engineering Publishing; 1998: 2000; pp 195-204.
369. Raghuvanshi, N. S.; Singh, A., Development of Maintenance Strategy to Improve Performance of Natural Draft Cooling Tower. *International Journal Of Scientific And Research Publications* **2014**, 4 (8), 1-7.
370. OEE Foundation OEE Industry Standard. <http://oeeindustrystandard.oeefoundation.org/definition/scope/> (accessed 03/27/2018).

371. Straub, D.; Grossmann, I., Integrated stochastic metric of flexibility with discrete states and continuous uncertain parameters. *Computers and Chemical Engineering* **1990**, *29* (3), 967.
372. Sahinidis, N.; Tawarmalani, M., BARON: The GAMS Solver Manual. *GAMS Development Corporation, Washington, DC* **2004**, 9-20.
373. Misener, R.; Floudas, C. A., ANTIGONE: algorithms for continuous/integer global optimization of nonlinear equations. *Journal of Global Optimization* **2014**, *59* (2-3), 503-526.
374. Wang, J.-G.; Shieh, S.-S.; Jang, S.-S.; Wu, C.-W., Discrete model-based operation of cooling tower based on statistical analysis. *Energy conversion and management* **2013**, *73*, 226-233.
375. Plummer, M.; Best, N.; Cowles, K.; Vines, K.; Sarkar, D., coda: Output Analysis and Diagnostics for MCMC. *R package version 0.13-3*, URL <http://CRAN.R-project.org/package=coda> **2008**.
376. Lam, W., Ensuring business continuity. *IT professional* **2002**, *4* (3), 19-25.
377. Spremic, M.; Popovic, M., Emerging issues in IT Governance: implementing the corporate IT risks management model. *WSEAS Transactions on Systems* **2008**, *7* (3), 219-228.
378. Tammineedi, R. L., Business continuity management: A standards-based approach. *Information Security Journal: A Global Perspective* **2010**, *19* (1), 36-50.
379. Winkler, U.; Fritzsche, M.; Gilani, W.; Marshall, A. In *A model-driven framework for process-centric business continuity management*, Quality of Information and

Communications Technology (QUATIC), 2010 Seventh International Conference on the, IEEE: 2010; pp 248-252.

380. Sikdar, S. K., Sustainable development and sustainability metrics. *AIChE journal* **2003**, 49 (8), 1928-1932.

381. CSB, C. S. B. *FINAL INVESTIGATION REPORT CHEVRON RICHMOND REFINERY PIPE RUPTURE AND FIRE*; 2015, 2015.

382. Feng, X.-j.; Hooshangi, S.; Chen, D.; Li, G.; Weiss, R.; Rabitz, H., Optimizing genetic circuits by global sensitivity analysis. *Biophysical journal* **2004**, 87 (4), 2195-2202.

383. Serna-González, M.; Ponce-Ortega, J. M.; Jiménez-Gutiérrez, A., MINLP optimization of mechanical draft counter flow wet-cooling towers. *Chemical Engineering Research and Design* **2010**, 88 (5-6), 614-625.

APPENDIX A
SOBOL SENSITIVITY INDICES

Sobol's GSA Indices³²⁰

The basis of the Sobol' global indices is an ANOVA-like decomposition of the total variability of the model into summands of increasing dimensionality. This decomposition takes place within the boundaries of the n-dimensional unit cube, where n is the number of input factors. Let us define the output variable as $Y = f(X)$, where X is the vector of input factors. It is possible to decompose $f(X)$ into summands of increasing dimensionality,

$$f(X_1, \dots, X_n) = f_0 + \sum_{i=1}^n f_i(X_i) + \sum_{1 \leq i < j \leq n} f_{ij}(X_i, X_j) + \dots + f_{1,2,\dots,n}(X_1, \dots, X_n) \quad (A.1)$$

The decomposition presented in eqn. (A.1) is termed ANOVA if f_0 is constant and the integral of every summand over any of the variables it contains is equal to zero.

$$\int f(x) dx = f_0 \quad (A.2)$$

and

$$\int_0^1 f_{i_1, \dots, i_n}(X_{i_1}, \dots, X_{i_n}) dX_{i_k} = 0, \quad 1 \leq k \leq s \quad (A.3)$$

It can be easily proven that eqns. (A.2) and (A.3) uniquely define all the terms in eqn. (A.1). In order to define the one-dimensional terms, eqn. (A.1) is integrated over all variables except x_i .

$$\int f(x) \prod_{k \neq i} dx_k = f_0 + f_i(x_i) \quad (A.4)$$

This can be extended to include all higher order terms as well. Assuming $f(x)$ to be square integrable implies that all the f_{i_1, \dots, i_s} are square integrable as well. Squaring and integrating eqn. (A.1) we obtain

$$\int f^2(x)dx - f_0^2 = \sum_{s=1}^n \sum_{i_1 < \dots, i_s}^n \int f_{i_1, \dots, i_s}^2 dx_{i_1} \dots dx_{i_s} \quad (\text{A.5})$$

If x were a random point uniformly distributed within the unit hypercube I^n , then $f(x)$ and $f_{i_1, \dots, i_s}(x_{i_1}, \dots, x_{i_s})$ would become random variables with variances D and D_{i_1, \dots, i_s} , respectively. Hence, the following constants from eqn. (A.5) are named variances:

$$D = \int f^2 dx - f_0^2 \quad D_{i_1, \dots, i_s} = \int f_{i_1, \dots, i_s}^2 dx_{i_1} \dots dx_{i_s} \quad (\text{A.6})$$

A measure of the main effect of each factor on the model output can be now defined, namely the Sobol' global sensitivity indices, as

$$S_{i_1, \dots, i_s} = \frac{D_{i_1, \dots, i_s}}{D} \quad (\text{A.7})$$

It is obvious that

$$\sum_{s=1}^n \sum_{i_1 < \dots, i_s}^n S_{i_1, \dots, i_s} = 1 \quad (\text{A.8})$$

Apart from sensitivity indices for individual input factors, the Sobol method allows indices to be evaluated for subsets of factors. Therefore, after an initial screening of the model parameters, those indicated as less important can be grouped into subsets, thus gaining in computational time. Input factors can also be grouped and studied according to their physical or biological nature³⁸².

Let us now consider a subset of m input factors, where $1 \leq m \leq n - 1$, namely $y = (x_{k_1}, \dots, x_{k_m})$. Let z denote the set of $n - m$ remaining input factors. The variance corresponding to the subset y can be defined as

$$D_y = \sum_{s=1}^m \sum_{(i_1 < \dots, i_s) \in K} D_{i_1, \dots, i_s}; \quad K = (k_1, \dots, k_m) \quad (\text{A.9})$$

Equation (A.9) can be rewritten for the variance of the second subgroup, D_y . The total variance corresponding to the group of input factors y is

$$D_y^{total} = D - D_y \quad (A.10)$$

It is now possible to define the two global sensitivity indices for the subset of input factors y . The S_y term represents the main effect of the subset on the output variance, whereas the term S_y^{total} corresponds to the TSI. The latter includes both the individual effect of the subset y and the effects originating from its interactions with other subsets or individual factors.

$$S_y = \frac{D_y}{D} \quad \text{and} \quad S_y^{total} = \frac{D_y^{total}}{D} \quad (A.11)$$

From eqns. (A.10) and (A.11) one can easily derive that $S_y^{total} = 1 - S_y$ and that $0 \leq S_y \leq S_y^{total} \leq 1$. Two extreme cases exist for the values of S_y and S_y^{total} . Either they are both 0, in which case they do not have any effect on the model output, or they are both equal to 1, in which case the model output variance is a direct result of the variance of this specific subset of input factors.

APPENDIX B
STATISTICAL METHODS

Bayes' theorem

For two events A and B Bayes' theorem states that $P(A | B) = P(B | A) P(A)/P(B)$. Consider a statistical model P_θ used to describe the data X_1, \dots, X_n . The parameter $\theta \in \Theta$ is an index for the family of models $\{P_\theta: \theta \in \Theta\}$. Let p_θ be the joint distribution of X_1, \dots, X_n , usually termed as the likelihood. Suppose there is a prior distribution $\pi(\cdot)$ on Θ . Then by the application of Bayes' theorem the posterior distribution of $\theta | X_1, \dots, X_n$ is given by,

$$p(\theta | X_1, \dots, X_n) = \frac{p_\theta(X_1, \dots, X_n) \pi(\theta)}{m(X_1, \dots, X_n)} \quad (\text{B.1})$$

where $m(\cdot)$ is the marginal distribution of X_1, \dots, X_n under the prior $\pi(\cdot)$.

Conjugate priors

Inferential summaries in a Bayesian framework are usually averages taken over the posterior distribution. For example, the posterior mean $\theta_B = \int \theta p(\theta | X)$ or the predictive distribution for a new observation $X_{\text{new}} = \int p(x_{\text{new}} | \theta) p(\theta | X)$ where we write X to denote the observed data. Thus it is desirable to have an explicit form of the posterior $p(\theta | X)$, so that integrals of the above form may be computed without having to use numerical approximation. Conjugate priors are priors π over θ so that the posterior $p(\theta | X)$ belongs to the same family of probability distributions.

Gibbs sampling

Suppose we want to sample from $p(\theta_1, \theta_2)$, a joint distribution on (θ_1, θ_2) . Often, the joint distribution will be mathematically intractable making it impossible to draw samples. In such cases the general Gibbs sampling algorithm defines a simple Markov chain scheme

to sample from this complicated distribution when the conditional distributions $p(\theta_1 | \theta_2)$ and $p(\theta_2 | \theta_1)$ are easy to sample from. The Markov chain steps are:

1. Draw $\theta_1 \sim p(\theta_1 | \theta_2)$.
2. Draw $\theta_2 \sim p(\theta_2 | \theta_1)$.

Standard Markov chain algebra can then be used to prove that such a draw (θ_1, θ_2) is indeed coming from the desired distribution $p(\theta_1, \theta_2)$. The algorithm is easily extended to settings where there are more than two variables. Suppose we want to draw samples from $p(\theta_1, \dots, \theta_k)$. We display below a generic t^{th} step to sample from this joint distribution. Let $(\theta_1^{(t-1)}, \dots, \theta_k^{(t-1)})$ be the draw at the $(t-1)^{\text{th}}$ iteration.

Input: $(\theta_1^{(t-1)}, \dots, \theta_k^{(t-1)})$.

for $j=1:k$

 Draw $(\theta_j^{(t)} \sim p(\theta_j | \theta_1^{(t)}, \dots, \theta_{j-1}^{(t)}, \theta_{j+1}^{(t-1)}, \dots, \theta_k^{(t-1)})$

end

Output: $(\theta_1^{(t)}, \dots, \theta_k^{(t)})$.

APPENDIX C

EULERS METHOD

Euler's method is a basic numerical method for solving differential equations. The approximate solution is derived by approximating the derivative in the differential equation by the slope of a secant line.

Let's denote the time at the n^{th} time-step by t_n and the solution at the n^{th} step by y_n , *i.e.*,

$$y_n \equiv y(t = t_n)$$

The step size h (assumed to be constant) is then given by,

$$h = t_n - t_{n-1}$$

Given the (t_n, y_n) , the (explicit) forward Euler method computes y_{n+1} as,

$$y_{n+1} = y_n + hf(y_n, t_n)$$

The forward Euler method is based on a truncated Taylor series expansion.

The approximate solution approach the exact solution as the number discretization points increase.

APPENDIX D

RELIABILITY AND MAINTAINABILITY

System reliability

The reliability of a system in series (R_{ss}) with n components can be mathematically written as,

$$R_{ss} = \prod_{i=1}^n R_i \quad (D.1)$$

where R_i represents the reliability of component i.

The reliability of a system in parallel (R_{sp}) with n components can be mathematically written as,

$$R_{sp} = 1 - \prod_{j=1}^n (1 - R_j) \quad (D.2)$$

where R_j represents the reliability of component j.

R_i or R_j is calculated as follows,

$$R = e^{-\left(\frac{t}{\alpha}\right)^\beta} \quad (D.3)$$

The reliability of the system under study is mathematically written as,

$$R_s = \prod_{i=1}^2 R_i \quad (D.4)$$

R_1 : reliability of fan (R_{fan})

R_2 : reliability of pump network (R_{pn})

$$R_{pn} = 1 - \prod_{j=1}^3 (1 - R_{pj}) \quad (D.5)$$

R_{p1}, R_{p2}, R_{p3} : reliability of pump

α : scale parameter

β : shape parameter

t:time

Generic algorithm: maintenance action selection

Function: Action decision (Ground truth, input parameter sequence)

Assign arrays 'M' and 'I' to store the values of truth and parameters input.

Map the values high and low as '1' and '0'.

Binarize the truth and input values.

Run the for loop to check if values of input array match with the truth. Initialize another array 'Count' and increase it if there is a match.

Repeat the above step to find if the highest match score.

The one with the highest matched score is the alternative to be selected.

If there are multiple highest matched scores, ask the user to input the cost of each action.

Choose the final action with minimum cost.

Return the final maintenance action selected.

System states: structural classification

System state, s	Equipment state (w_1^s, w_2^s, w_3^s)	Availability/Operability, $\phi(w^s)$
1	1,1,1	Available/Operable
2	0,1,1	Available/Operable
3	1,0,1	Available/Operable
4	1,1,0	Available/Operable
5	0,0,1	Available/Operable
6	0,1,0	Available/Operable
7	1,0,0	Available/Operable
8	0,0,0	Unavailable/Inoperable

APPENDIX E

COOLING TOWER PROCESS MODEL

The following equations³⁸³ refer to the cooling tower example presented in Section 6.4 and schematically depicted in Figure VI.4.

Equations:

Heat load:

$$Q = c_{pw}m_w(TW_{in} - TW_{out}) \quad (E.1)$$

Power consumption: (E.2)

$$P = \frac{mav_{out}\Delta P_t}{\rho_{out}\eta_f}$$

Water consumption:

$$m_{wev} = m_a(w_{out} - w_{in}) \quad (E.3)$$

$$m_{bw} = \frac{m_{mw}}{n_{cycles}} - m_{wd} \quad (E.4)$$

$$m_{wd} = 0.002m_w \quad (E.5)$$

$$m_{mw} = m_{wev} + m_{bw} + m_{wd} \quad (E.6)$$

$$m_{mw} = \frac{n_{cycles}m_{wev}}{n_{cycles} - 1} \quad (E.7)$$

Physical Properties:

$$ha_{in} = -6.38887667 + 0.86581791 TWB_{in} + 15.7153617e^{(0.05439778 TWB_{in})} \quad (E.8)$$

$$w_{in} = \left(\frac{2501.6 - 2.3263 (TWB_{in})}{2506 + 1.8577 (TA_{in}) - 4.184 (TWB_{in})} \right) \left(\frac{0.62509 (PV_{wbin})}{P_{tot} - 1.005 (PV_{wbin})} \right) - \left(\frac{1.00416 (TA_{in} - TWB_{in})}{2506 + 1.8577 (TA_{in}) - 4.184 (TWB_{in})} \right) \quad (E.9)$$

$$hsa_{out} = ha_{in} + \frac{c_{pw}m_w}{m_a} (TW_{in} - TW_{out}) \quad (E.10)$$

$$w_{out} = \frac{0.62509 PV_{out}}{P_{tot} - 1.05 PV_{out}} \quad (E.11)$$

$$\ln(PV) = \sum_{n=-1}^3 c_n T^n + 6.5459673 \ln(T) \quad (\text{E.12})$$

$$\rho = \frac{P_{\text{tot}}}{287.08 T} \left[1 - \frac{w}{w+0.62198} \right] [1 + w] \quad (\text{E.13})$$

Feasibility constraints:

$$TW_{\text{out}} - TW_{\text{B}_{\text{in}}} \geq 2.8 \quad (\text{E.14})$$

$$TW_{\text{out}} \leq TMPO - \Delta T_{\text{min}} \quad (\text{E.15})$$

$$TW_{\text{in}} \leq TMPI - \Delta T_{\text{min}} \quad (\text{E.16})$$

$$TW_{\text{in}} \leq 50^\circ\text{C} \quad (\text{E.17})$$

$$TW_{\text{in}} > TW_{\text{out}} \quad (\text{E.18})$$

$$TA_{\text{out}} > TA_{\text{in}} \quad (\text{E.19})$$

$$0.5 \leq \frac{m_w}{m_a} \leq 2.5 \quad (\text{E.20})$$

$$2.9 \leq \frac{m_w}{A_{\text{fr}}} \leq 5.96 \quad (\text{E.21})$$

$$1.2 \leq \frac{m_a}{A_{\text{fr}}} \leq 4.25 \quad (\text{E.22})$$

$$m_w > 0 \quad (\text{E.23})$$

$$m_a > 0 \quad (\text{E.24})$$

APPENDIX F

VALUES OF CONSTANTS AND COST NUMBERS

Cost values used in the model

Safety impact (USD, per unit hours of operation)				
Tier 1	S₁	E₁	A₁	L₁
	50	45	47.5	32.5
Tier 2	S₂	E₂	A₂	L₂
	25	20	27.5	17.5
Maintenance activities (Pump, USD, per unit hours of operation)				
	C_{CM} > C_{PdM} (M1)	C_{CM} >> C_{PdM} (M2)	C_{CM} = C_{PdM} (M3)	C_{CM} < C_{PdM} (M4)
Preventive maintenance	25	25	150	300
Corrective maintenance	70	1000	500	400
Predictive maintenance	55	100	500	800
Inspection cost	10			
Maintenance activities (Fan, USD, per unit hours of operation)t				
	C_{CM} > C_{PdM} (M1)	C_{CM} >> C_{PdM} (M2)	C_{CM} = C_{PdM} (M3)	C_{CM} < C_{PdM} (M4)
Preventive maintenance	37.5	37.5	225	450
Corrective maintenance	105	1500	750	600
Predictive maintenance	82.5	150	750	1200
Inspection cost	15			
Process operations				
C _p : cost in USD per kg cooling water flowrate			0.0000763	
E _c : cost in USD per kWh			0.085	
C _{p1} :cost in USD per kg product flowrate (batch reactor)			1.5	
C _{p2} :cost in USD per kg product flowrate (overhead vapor condensation)			2	
C _{rm1} :making cost in USD per kg product flowrate (batch reactor)			0.5	
C _{rm2} :making cost in USD per kg product flowrate (overhead vapor condensation)			0.8	

List of various constants

Scalar	Description	Value
H	number of hours of operations in a year	2000
pc_1	pump 1 design capacity	33
pc_2	pump 2 design capacity	42
pc_3	pump 3 design capacity	50
η_{p1}	pump 1 efficiency	0.63
η_{p2}	pump 2 efficiency	0.56
η_{p3}	pump 3 efficiency	0.71