Modeling and Analyzing Systemic Risk in Complex Sociotechnical Systems

The Role of Teleology, Feedback, and Emergence

Zhizun Zhang

Submitted in partial fulfillment of the
requirements for the degree
of Doctor of Philosophy
in the Graduate School of Arts and Sciences

COLUMBIA UNIVERSITY

2018

ABSTRACT

Modeling and Analyzing Systemic Risk in Complex Sociotechnical Systems

Zhizun Zhang

Recent systemic failures such as the BP Deepwater Horizon Oil Spill, Global Financial Crisis, and Northeast Blackout have reminded us, once again, of the fragility of complex sociotechnical systems. Although the failures occurred in very different domains and were triggered by different events, there are, however, certain common underlying mechanisms of abnormalities driving these systemic failures. Understanding these mechanisms is essential to avoid such disasters in the future. Moreover, these disasters happened in sociotechnical systems, where both social and technical elements can interact with each other and with the environment. The nonlinear interactions among these components can lead to an "emergent" behavior – i.e., the behavior of the whole is more than the sum of its parts – that can be difficult to anticipate and control. Abnormalities can propagate through the systems to cause systemic failures. To ensure the safe operation and production of such complex systems, we need to understand and model the associated systemic risk.

Traditional emphasis of chemical engineering risk modeling is on the technical components of a chemical plant, such as equipment and processes. However, a chemical plant is more than a set of equipment and processes, with the human elements playing a critical role in decision-making. Industrial statistics show that about 70% of the accidents are caused by human errors. So, new modeling techniques that go beyond the classical equipment/process-oriented approaches to include the human elements (i.e., the "socio" part of the sociotechnical systems) are needed for analyzing systemic risk of complex sociotechnical systems. This thesis presents such an approach.

This thesis presents a new knowledge modeling paradigm for systemic risk analysis that goes beyond chemical plants by unifying different perspectives. First, we develop a

unifying teleological, control theoretic framework to model decision-making knowledge in a complex system. The framework allows us to identify systematically the common failure mechanisms behind systemic failures in different domains. We show how cause-and-effect knowledge can be incorporated into this framework by using signed directed graphs. We also develop an ontology-driven knowledge modeling component and show how this can support decision-making by using a case study in public health emergency. This is the first such attempt to develop an ontology for public health documents. Lastly, from a control-theoretic perspective, we address the question, "*how do simple individual components of a system interact to produce a system behavior that cannot be explained by the behavior of just the individual components alone?*" Through this effort, we attempt to bridge the knowledge gap between control theory and complexity science.

Table of Contents

List of Figures

List of Tables

Glossary

aggregate complexity underscores the complex behavior resulting from the interactions of system components, both social and technical. 1

algorithmic complexity describes the effort required to solve a well-defined technical problem. 1

bank-dealer is a bank operates as a securities dealer when it underwrites, trades, or deals in securities. 20

deterministic complexity describes chaotic behaviors and highlights the general inability to predict the future behavior of a nonlinear dynamical system. 1

fire sale refers to a sale of goods or assets at heavily discounted prices to avoid a financial disaster or to satisfy the debts of an insolvent or bankrupt firm. 20

funding run describes a situation in which a company faces an increasing amount of redemptions, causing the sell positions to meet the withdrawals. 20

public health promotes and protects the health of people and the communities where they live, learn, work and play. 71

sociotechnical system is a system that comprises of social elements as well as technical elements, usually organized as a hierarchy. 1

spatial complexity refers to a system's large physical scale and geographical complexity. 1

systemic risk emphasizes the risk of the entire system rather than individual components. 5

systemic failure is the failure at system level which cannot be simply described from the individual component failures of the system. 1

teleodynamics is the dynamics of rational agents driven by their goals. 104

teleology describes things in terms of their purpose, directive principle, or goal. 105

temporal complexity refers to the various time scales of processes, events, and decision-making in a system. 1

Acronyms

AIG American International Group. 37

BP British Petroleum. 1

CSB Chemical Safety and Hazard Investigation Board. 42

CSTR Continuous Stirred-Tank Reactor. 51

DAE Differential and Algebraic Equations. 3

DOE Department of Energy. 11

EID Emerging Infectious Disease. 72

EMS Emergency Management System. 42

EPA Environmental Protection Agency. 27

FDA Food and Drug Administration. 27

FE First Energy. 31

FED Federal Reserve. 27

FERC Federal Energy Regulatory Commission. 27

FTA Fault Tree Analysis. 3

H1N1 Influenza A (H1N1) virus. 79

HAZOP Hazard and Operability Analysis. 2

HEDIS Healthcare Effectiveness Data and Information Set. 91

HSC Health Security Committee. 93

HSE Health and Safety Executive. 11

ISO Independent System Operator. 43

ISOM Isomerization Process Unit. 37

LKIF Legal Knowledge Interchange Format. 80

LMICs Low- and Middle-Income Countries. 97

MFM Multi-level Flow Modeling. 6

MISO Midcontinent Independent System Operator, Inc.. 43

MMS Minerals Management Service. 11

NASA National Aeronautics and Space Administration. 12

NERC North American Electric Reliability Corporation. 44

NLP Natural Language Processing. 79

NYC New York City. 93

NYCDOH New York Department of Health. 93

ODE Ordinary Differential Equation. 49

OntoPH Public Health Ontology. 73

OSHA Occupational Safety and Health Administration. 27

OWL Web Ontology Language. 81

PCA Principle Component Analysis. 5

PDE Partial Differential Equation. 49

PHA Process Hazard Analysis. 2

PLS Partial Least Square. 5

PRA Probability Risk Assessment. 2

QDE Qualitative Differential Equation. 123

QSIM Qualitative Simulation. 102

ROE Return On Equity. 25

ROI Return On Investment. 25

RTO Regional Transmission Operator. 43

SDG Signed Directed Graphs. 3

SEC Securities and Exchange Commission. 27

STAMP Systems-Theoretic Accident Model and Processes. 6

SWRL Semantic Web Rule Language. 84

TeCSMART Teleo-Centric System Model for Analyzing Risks and Threats. 14

WHO World Health Organization. 76

WNV West Nile Virus. 79

Acknowledgments

I would like to express my great appreciation to my advisor Professor Venkat Venkatasubramanian, for giving me the opportunity to learn new knowledge and solve challenging problems. He convinced me that pursuing a doctoral degree is one of the most valuable experiences of one's life. I have enjoyed my doctoral study very much because of his support. He guided me through many conceptual challenges and celebrated my successes with me. He gave me not only insightful research advice but also wise life suggestions. I am very grateful that he teaches me how to think, how to write, and more importantly, how to overcome difficulties with enthusiasm.

I am very thankful to my committee members. Professor Garud Iyengar and Professor Shivaram Rajgopal advised me in different stages of my PhD journey. I have enjoyed the collaborations very much. Professor Alan West taught me Electro-chemistry, which became the topic of my doctoral qualification exam. Thanks to Professor West's teaching, I successfully passed the exam and became a doctoral candidate. I also want to thank Professor Kyle Bishop. He kindly agrees to sit on my committee and gives me helpful advice to my thesis. The time and effort are much appreciated.

I would like to thank Dr. Richard Bookstaber and Professor Paul Glasserman for their contributions to the process systems engineering in financial system work. They taught me the financial knowledge and how to work with people from different backgrounds.

I would like to thank Professor Stephen Morse and Ms. Mila Gonzalez. Without their public health knowledge, I would not have built the public health ontology. Their professional opinions provided me insightful details about public health.

I would like to express my special thanks to Dr. Yu Luo, a great friend and good colleague of mine. We spent the entire grad school years together. I enjoyed all the coffee breaks and the intellectual discussions. I will miss all the Chick-Fil-A lunches we had. I am grateful for his help in both study and life.

My time at Columbia would not have been so joyful without my friends here. I am thankful for my startup journey with Ziyan Feng, Xiaozheng Li, Ying Li, and Ruixing Zhu. I am grateful for all my gym buddies and all the fun nights I spent with my board game buddies.

I especially thank my family for their support and love. Without them, I would not have made it this far. They always trust me and give me the freedom to explore my own interests. Their love helps me overcome all the challenges. Thank you very much!

This dissertation is dedicated to my parents.

Chapter 1

Introduction

All are good at first, but few prove themselves to be so at the last.

Shih-ching

Modern technological advances have created an increasing number of complex *sociotechnical* systems, such as offshore oil platforms, power grids, and financial networks, which bring us comfort and convenience. At the same time, we have paid the cost for the rapid social and technological developments. Recent systemic failures, such as the British Petroleum (BP) Deepwater Horizon Oil Spill (2010), Indian Power Outage (2012), and Global Financial Crisis (2007-09), are a few well known examples.

Systemic failures occur when an entire sociotechnical system collapses, where the system is typically a large entity, whose failure negatively impacts people and the environment, causing enormous economic losses. "Sociotechnical" means that these systems consist of social elements (i.e., humans) as well as technical elements (such as pumps, valves, reactors, etc.). Unlike technical systems, sociotechnical systems involve human decision-making that can alter the systems' behaviors. Typically, sociotechnical systems have a very large number of inter-dependent components with nonlinear interactions that can lead to "emergent" behavior - i.e. the behavior of the whole is more than the sum of its parts – that can be difficult to anticipate and control [Ottino, 2004]. Moreover, these systems are not static and isolated - they are constantly changing and interacting with the environment.

Sociotechnical systems are usually complex. Complexity arises from their scale, interconnectedness, nonlinear interactions, and feedback. Typically, a sociotechnical system exhibits several types of complexities, namely, spatial complexity, temporal complexity, algorithmic complexity, deterministic complexity, and aggregate complexity. *Spatial complexity* refers to a system's large physical scale and geographical complexity. Epidemics and pandemics exhibit this type of complexity. *Temporal complexity* is related to the various time scales of processes, events, and decision-making in a system. *Algorithmic complexity* describes the effort required to solve a well-defined technical problem [Manson, 2001]. This type of complexity usually exists in the mechanical processes of a sociotechnical system, such as the control process of a reactor. *Deterministic complexity* describes chaotic behavior, which highlights the general inability to predict the future behavior of a nonlinear dynamical system [Manson, 2001]. Typical examples include the stock market and weather forecast. *Aggregate complexity* underscores the complex behavior resulting from the interactions of system components, both social and technical [Manson, 2001]. The cumulative effect of the different types of complexities makes these sociotechnical systems potentially fragile and susceptible to systemic failures.

To ensure safe operations over the life cycles of sociotechnical systems, we need to understand their complexity and manage their potential systemic instability and fragility to mitigate risk [Centeno *et al.*, 2015; Fouque and Langsam, 2013].

1.1 Risk Modeling in Chemical Plants

Chemical industry was born with risk management. Chemical industrial accidents can result in very severe consequences. In fact, the worst industrial accident is from chemical industry, namely, the Bhopal Gas Tragedy, resulted an estimated 5000 deaths, and about 100,000 serious injuries. Chemical engineers, having a long history of managing risk in complex chemical plants, are the pioneers of risk modeling and control. Risk management is rooted deeply in chemical industry practice and chemical engineering curriculum. Every chemical engineer is trained a number of techniques to assess risk in chemical equipment and processes, such as Process Hazard Analysis (PHA), Hazard and Operability Analysis (HAZOP), and Probability Risk Assessment (PRA). These methods help chemical engineers build robust chemical processes and pinpoint potential stress and instability in a systematic manner.

Risk modeling in chemical engineering mainly focuses on how to detect and diagnose abnormal events in equipment and chemical processes. Chemical engineers have actively studied this problem for decades. Many techniques have been developed, focusing on abnormality detection, fault diagnosis and correction. Risk modeling within chemical plants always addresses following three main questions [Apostolakis, 2004; Kaplan and Garrick, 1981]:

- What can go wrong?
- How likely it is?
- What would be the consequence?

The objective of risk modeling is to identify, prioritize, and reduce risk associated with equipment and processes [Saleh *et al.*, 2014]. Venkatasubramanian [Venkatasubramanian and Rengaswamy, 2003] has classified the risk modeling methods to three categories: quantitative methods, qualitative methods, and process history based methods, as shown in Figure 1.1.

Quantitative methods typically assess risks on the event probability or on the state-space models of the underlying technical system [Millot, 2014]. State-space models and statistical fault diagnosis usually identify the system inconsistencies, then explain the inconsistencies in terms of the process variables [Venkatasubramanian and Rengaswamy, 2003]. System is modeled as algebraic equations [Gertler, 1991; Gertler, 1993]. Probabilistic risk assessment such as root cause analysis usually uses a Bayesian approach. It takes observations as prior knowledge to infer the truthfulness of a hypothesis [Garvey, 2008].

Qualitative methods, on the other hand, focus on causal relations between variables or structural properties of the system. Among them, Signed Directed Graphs (SDG) is a popular causal inference technique used in various chemical industrial safety applications. Adopting graph theoretical ideas, SDG represents the *cause and effect* relationships in a process or equipment [Maurya *et al.*, 2003a; Maurya *et al.*, 2003b; Maurya *et al.*, 2004]. The *qualitative* models are easier to develop and analyze, in comparison with the Differential and

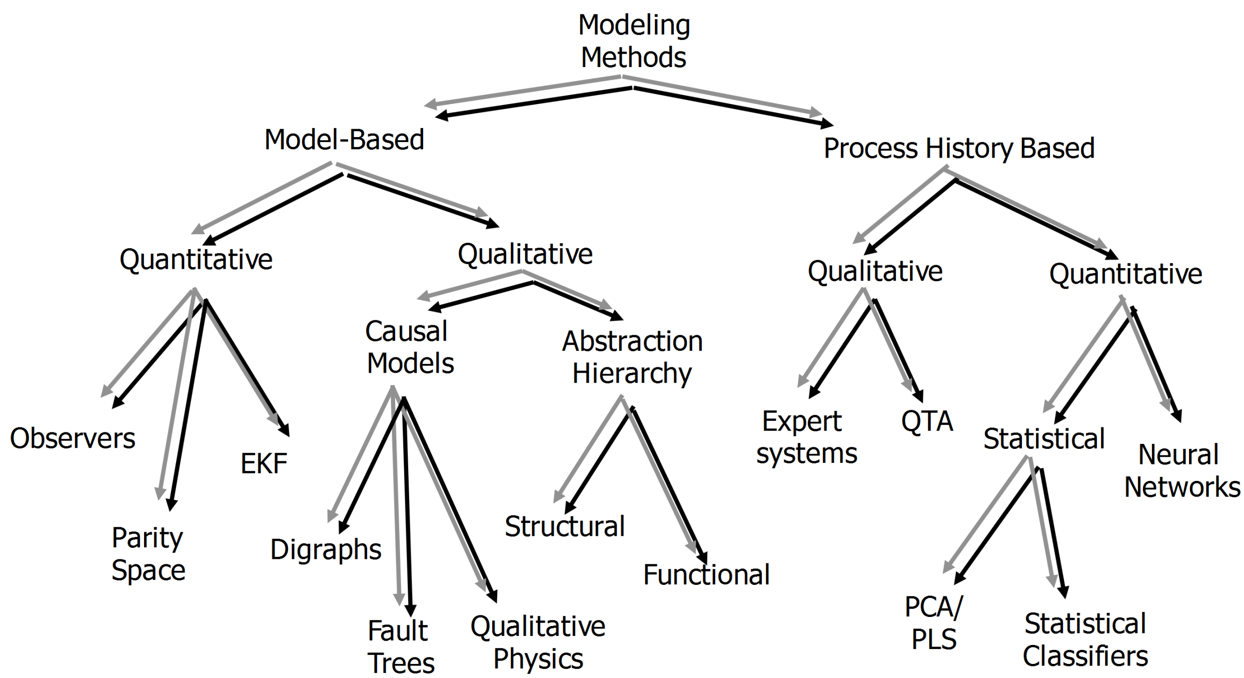


Figure 1.1: Classification of diagnostic algorithms (adapted from [Venkatasubramanian and Rengaswamy, 2003])

Algebraic Equations (DAE) models, particularly for modeling and analyzing failure modes and hazards [Venkatasubramanian *et al.*, 2000; Venkatasubramanian and Vaidhyanathan, 1994]. However, since they are qualitative in nature, they are limited to certain kinds of queries and can lead to ambiguities. Another important qualitative analysis method is Fault Tree Analysis (FTA), invented by Bell Laboratories in 1961. Fault tree is a logic tree that decomposes a critical event to basic events with the help of logic operators such as "AND," "OR," and "XOR" [Lapp and Powers, 1977]. The fault tree is developed by asking the question "what could cause this event?" [Venkatasubramanian *et al.*, 2003b] A basic event has a probability of occurrence. Propagating through the tree, probability of a top event can be computed.

Recent years, artificial intelligence and data science advances have enabled computer-aided risk assessment. As a result, process history based approaches become popular. It is effective to use historical data and machine learning techniques to evaluate or predict the status of equipment or processes. This category includes neural networks and statistical approaches such as Principle Component Analysis (PCA) and Partial Least Square (PLS) [Venkatasubramanian *et al.*, 2003a], which formulate the fault diagnostic as a pattern recognition problem. Data points are classified into different classes, indicating different system variable inconsistencies. The inconsistencies are usually correlated with faults [MacGregor *et al.*, 1991; MacGregor *et al.*, 1994; MacGregor and Kourti, 1995]. Neural networks have been used in chemical engineering for fault diagnosis [Venkatasubramanian and Chan, 1989; Watanabe *et al.*, 1989; Watanabe *et al.*, 1994]. In each case, fault diagnosis is treated as a classification problem. Training data and number of hidden layers are critical to the diagnosis performance.

1.2 Risk Modeling beyond Chemical Plants

Risk modeling within chemical plants mainly analyzes risks of equipment and processes. However, a chemical plant is more than a set of equipment and processes. It is a sociotechnical system comprising of both technical processes and human decision-making processes. Systemic risk analysis of such a system needs to *go beyond the modeling of equipment and processes* by focusing on interactions among humans, machines, and the environment. Developing such a broad framework to analyze systemic failures is one of the main contributions of this thesis.

Many methods have been developed to understand risk from this boarder perspective. For example, FTA was extensively used in safety critical aerospace missions in NASA to understand root causes of a failure. Multi-level Flow Modeling (MFM) models flows of mass, energy, and information of sociotechnical systems [Lind, 1994; Lind, 2005; Heussen and Lind, 2010a; Heussen and Lind, 2010b]. Systems-Theoretic Accident Model and Processes (STAMP) is another example that takes human factors into account to assess system's risk [Leveson, 2004; Leveson and Stephanopoulos, 2014; Leveson, 2015]. In addition, human interactions in complex systems have also been modeled as networks via agent based simulations [Amaral and Ottino, 2004; Battiston *et al.*, 2016; Luo *et al.*, 2016; Natarajan and Srinivasan, 2014]. Government officials study systemic risk associated with policy-making [Freixas *et al.*, 2000]. Econophysicists use network theory to analyze systemic risk in financial systems [Catanzaro and Buchanan, 2013; Caldarelli *et al.*, 2013]. Our prior work stressed the need for modeling cause-and-effect knowledge explicitly as well as the need for a multi-scale modeling framework in understanding systemic risk in sociotechnical systems [Maurya *et al.*, 2003a; Maurya *et al.*, 2003b; Maurya *et al.*, 2004; Srinivasan and Venkatasubramanian, 1998c; Venkatasubramanian and Vaidhyanathan, 1994; Venkatasubramanian *et al.*, 2000; Venkatasubramanian, 2011].

These studies have made considerable progress in modeling risk. However, an understanding about systemic risk in sociotechnical systems is still lacking. The major intellectual challenge is how to model multiple levels of sociotechnical systems and understand their emergent behaviors [Venkatasubramanian, 2011]. This requires a modeling of sociotechnical system that focuses on not only machines and processes, but also the knowledge and mechanisms that generate complex system behaviors [Rasmussen, 1997].

1.3 Organization

In this thesis, we *model different kinds of knowledge* by studying the role of teleology, feedback, and emergence. *Teleology*, i.e., goal-driven behavior, provides a unifying perspective to investigate sociotechnical systems. *Feedback control* helps us understand the nonlinear interactions among the heterogeneous agents of sociotechnical systems. *Emergence* underscores how simple components' interactions lead to a system's complex behaviors.

This thesis unfolds as follows. In Chapter 2, we develop a unifying framework to model system knowledge and analyze the common failure mechanisms behind different systemic failures. Chapter 3 applies SDG to model cause-and-effect knowledge and understand systemic risk of a financial network. Chapter 4 develops ontological models for heuristic knowledge that is critical in public health decision-making. In Chapter 5, we try to answer the question, "*how do simple individual components interact to result in a system behavior that cannot be explained by just the behavior of its components considered individually?*" This helps us gain a fundamental understanding about emergent behavior of sociotechnical systems. Chapter 6 concludes this thesis.

Chapter 2

A Hierarchical Framework for Modeling and Analyzing Systemic Risk in Sociotechnical Systems

> To have faults and not to reform them,
> – this, indeed, should be pronounced
> having faults.
>
> Confucius

We have seen many industrial catastrophes of different sociotechnical systems, including refineries, inter-state power grids, country-wide financial networks, large organizations, etc. Sociotechnical systems consist of different mechanical processes, agents, organizations, and stakeholders. Systemic failures in different sociotechnical systems appear to be very different, but they all resulted in very severe consequences. For example, Union Carbide's Bhopal Gas Tragedy in 1984, in which an estimated 5000 died and about 100,000 were seriously injured by the accidental release of methyl isocynate was a systemic failure of chemical plants. Another example is the Piper Alpha disaster in 1988, where an offshore oil platform operated by Occidental Petroleum in the North Sea, U.K., exploded killing 167 and resulting in about $2 billion in losses. The Challenger (1986) and Columbia (2003) space shuttle disasters, Schering Plough inhaler recall (1999), the Northeast electrical power blackout (2003), the spread of SARS (2003), the BP Texas City Refinery Explosion (2005), and the Johnson & Johnson multi-drug recall (2010) are all examples of systemic failures in different domains. Examples of financial systemic failures include Enron (2001) and World-Com (2002) collapses, the Madoff Ponzi scheme (2008), and the Subprime Crisis (2007-09). The collapse of the News of the World newspaper organization (2011) is an example of systemic failure in the media domain. The Wells Fargo Accounts Scam (2016) and Volkswagen Emissions Scandal (2016) are examples from last year.

In each case, an official *post mortem* inquiry was conducted and reports of the accidents were produced after each systemic failure. Chemical engineers might study the BP Deep-water Oil Spill Report [Drilling, 2011], and people from the financial world may browse the Financial Crisis Inquiry Report [Commission, 2011], but rarely does one compare failures across the different domains to study their commonalities and differences. But when one undertakes such a comparative study, one is struck by the commonality across different domains. There is an alarming sameness about such disasters, which can teach us important fundamental lessons. Although the failures occurred in different domains, in different facilities, triggered by different events, there are, however, common failure mechanisms that often underlie such events. Systematically identifying and understanding these mechanisms are essential to avoid such disasters in the future.

To do so, we propose a conceptual framework that captures system knowledge and failure mechanisms. Our analysis models multiple levels of a system, both social and technical, and identifies the potential failure modes of equipment, humans, policies and institutions. With the aid of three major recent disasters, we demonstrate how this framework could help us compare systemic failures in different domains and identify the common failure mechanisms at all levels of the system.

2.1 Common Patterns of Failures at Multiple Levels

Postmortem investigations of many disasters have shown that systemic failures rarely occur due to a single failure of a component or personnel. Even though the senior management of a company typically tried to spin the blame on some unanticipated equipment failure, operator error, or a rogue trader, that is rarely the case for major disasters. For instance, Union Carbide initially claimed that the Bhopal Gas Tragedy was caused by a disgruntled employee, who had sabotaged the equipment [Jasanoff, 1994]. Enron management initially blamed Andrew Fastow, Enron's CFO, as the sole culprit [Plotz, 2002]. But, again and again, investigations have shown that there are always several layers of failures, ranging from low-level personnel to senior management to regulatory agencies, that have led to major disasters.

Such investigations have shown that the safety procedures had been deteriorating at the failed facilities for months, if not years, prior to the accident. For example, in the case of Piper Alpha, the Permit-to-Work system had been dysfunctional for months [CCPS, 2005]. In Bhopal, regular maintenance of safety backup systems had not been conducted for months [Jasanoff, 1994]. Massey Energy ran up about 600 safety violations in its Upper Big Branch mine during 2009-2010 [MSNBC, 2010]. OSHA statistics show that BP ran up 760 "egregious, willful" safety violations during 2008-2010 in Ohio and Texas. Compare this with the corresponding numbers for the other oil companies: Sunoco (8), Conoco-Phillips (8), Citgo (2) and Exxon (1) [Thomas *et al.*, 2010]. These are clear evidences of a breakdown of the corporate safety culture for months or years. One sees a similar pattern in financial disasters as well. For example, in Enron, its senior management, led by Ken Lay and Jeff Skilling, created an extreme performance-oriented risky culture that seems to have tolerated unethical behavior, which resulted in many violations, market manipulations, and so on [Plotz, 2002]. In the subprime crisis, the perverted incentive mechanisms in mortgage lending and its subsequent securitization and trading, caused individuals and corporations to make highly-leveraged bets that resulted in risk extremes which were unsustainable. Thus, it was not a question of if a disaster would occur but when.

Another common pattern is that people had not identified all the serious potential hazards. They had often failed to conduct a thorough process hazards analysis that would have exposed the serious hazards, which resulted in the disasters later. Such incomplete hazards analysis was highlighted in the Cullen Inquiry of Piper Alpha [CCPS, 2005]. Failure to perform such a hazards analysis was partially responsible for the meltdown of Lehman Brothers and others in the subprime market fiasco [Johnson and Neave, 2007]. However, the few who had performed such hazards analysis did see the crash coming and profited billions of dollars, as described in Michael Lewis' book, now a movie, *The Big Short* [Lewis, 2011]. Yet another common cause is the inadequate training of the plant personnel to handle serious emergencies.

All in all, typically, the responsibility for a systemic failure goes all the way to the top levels of company management, who had only paid a lip service to safety, tolerated non-compliant behavior, even encouraged excessive risk taking and unethical behavior, all of which resulted in a poor corporate culture of safety [Baker *et al.*, 2007; Olive *et al.*, 2006; CSB, 2005; Hopkins, 2008], which in turn paved the way for the disasters.

We also find that serious failings by regulatory, ratings, and auditing agencies, tolerated, sometimes even encouraged, by a *laissez-faire* political environment, playing a significant role. First and foremost, it does not matter whether the systems are chemical, petrochemical, or financial – self policing does not work. This seems so obvious that people should not have to die, or lose all their money, to make us realize this. Sensible regulations are essential, but, more importantly, they must be audited and enforced by suitably trained personnel who have no conflicts of interest. The betrayal of public trust by Arthur Andersen, the supposedly independent auditor of Enron, whose aiding and abetting of Enron's cooked books was instrumental in its systemic failure [Plotz, 2002]. The subprime market failures showed us that the rating agencies, which were supposed to make an independent assessment of the subprime-mortgage-backed securities, were so dependent on their Wall Street clients for their business that they merrily went stamping AAA ratings on junk instruments. Of the AAA-rated securities issued in 2006, an astonishing 93% were later downgraded to junk status [Krugman, 2010].

It is the same lesson we were taught by the BP Deepwater Horizon oil spill – how the Minerals Management Service (MMS) was inherently conflicted between its goals of awarding leases and enforcing safety regulations [Urbina, 2010]. But, this lesson should have been learnt a long time ago after the Piper Alpha disaster. Based on the Cullen Report's findings in 1988, the British government moved the responsibility for safety oversight from the Department of Energy (DOE) to the Health and Safety Executive (HSE), the independent watchdog agency for work-related health, safety and illness. A separate division was created within the HSE to monitor safety of the offshore oil and gas industry [CCPS, 2005].

Indeed, the importance of addressing non-technical common causes, as those described above, as an integral part of systems safety engineering, was pointed out as far back as 1968 by Jerome Lederer, the former director of the National Aeronautics and Space Administration (NASA) Manned Flight Safety Program for Apollo, who wrote:

> System safety covers the entire spectrum of risk management. It goes beyond the hardware and associated procedures to system safety engineering. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored.

To understand systemic failures and learn from them, *one needs to go beyond analyzing them as independent one-off accidents, and examine them in the broader perspective of the potential fragility of all complex systems.* One needs to study the disasters from *a unifying sociotechnical systems engineering perspective*, so that one can thoroughly understand the commonalities as well as the differences, gain insights about the system-wide breakdown mechanisms in order to better design, control and manage such systems in the future.

It is quite clear that to properly model and analyze systemic risk, one not only needs to model failures at the lowest level of a sociotechnical system (such as at the failures of equipment) but also, more importantly, model the human and institutional failures that occur at the higher levels of the system. The human elements are not only an integral part of the system, they are also often the cause of major failures. Hence, it is important to account for them, as explicitly as possible, in any risk modeling framework. This has not always been the case in the engineering modeling literature. For instance, most modeling studies in the process control literature do not account for errors committed by humans in their methodologies. HAZOP analysis, as another example, considers only equipment and operation failures in its guide-word based approach. We need a systematic methodology that can identify potential failure mechanisms, due to equipment, process, human, and institutional failures, at different levels of a sociotechnical system. This chapter is largely a conceptual contribution, describing a new modeling framework that articulates how the different levels of a complex sociotechnical system may be formally approached using control-theoretic ideas. Building on the prior work [Venkatasubramanian, 2011; Venkatasubramanian *et al.*, 2000], we present such an integrative multi-scale modeling framework, which addresses the role of the human element explicitly, and discuss its implications in the context of several prominent systemic failures in different domains.

2.2 TeCSMART Framework

While it may be hard to state exactly what a complex system, is, there is consensus, however, as to what features are typically associated with a complex sociotechnical system. As we have discussed in Chapter 1, complex systems typically consist of many diverse, autonomous, and adaptive components that interact with one another, and their environment, in nonlinear, dynamical ways to produce a very large set of potential future states or outcomes. Interactions between such parts at a given scale typically give rise to "emergent" properties at larger scales in space and/or time, sometimes through self-organization, without any global knowledge or central control, that are hard to predict from the properties of the parts. They tend to have many feedback loops (both positive and negative), among their components as well as with their environment, which can cause adaptation and induce a goal-directed (i.e. teleological) behavior, either intentionally or implicitly, thereby potentially altering the course of their future behavior. Hence, their characteristics are typically not reducible to an elementary level of description.

Thus, the essential features of a complex sociotechnical system may be summarized as: (i) goal-driven behavior, (ii) many homogeneous or heterogeneous agents (or components), (iii) organized in a multi-layered hierarchy or network, (iv) nonlinear dynamical interactions among its agents (or components) and with the environment, (v) feedback loops, (vi) decentralized control (i.e., local decision-making), and (vii) emergent behavior.

In this section, we develop the modeling framework that captures the characteristics aforementioned. We call it *Teleo-Centric System Model for Analyzing Risks and Threats (TeCSMART)*. *Telos* means goal or purpose in Greek. *The central theme of our approach is the emphasis on recognizing and modeling goals of different agents, at different levels of abstraction, in a complex sociotechnical system.* Both individual players and groups are *goal-oriented*, driven to act by their goals and incentives, in a complex system. Therefore, it is important to recognize and model this goal-driven behavior. Individuals (or groups) usually have different goals, or even goals with conflicts of interests with each other or with goals from other individuals. The dynamics of how goals across the system interact, transform and disperse in the hierarchy, affects both individual and systemic performances. We use a simple feedback control module as a model for representing this goal-driven behavior as we discuss below.

We propose an integrative framework that tries to capture the essential features of a complex teleological system with the purpose of modeling, analyzing, and managing systemic risk by accounting for the effects of both autonomous (i.e., human) and non-human (i.e., "machines" or "mechanical") entities in a unified and systematic manner. We model a complex teleological system as a sociotechnical entity that is embedded in a society, affected by the society's goals and political environment. This leads to a multi-scale modeling framework, having *seven layers* organized as a hierarchy, as shown in Figure 2.1, that naturally arise and represent different perspectives of the entire system. Each layer above is a zoomed-out, aggregate, view of the immediate layer below. For example, the block representing process unit in the network of Plant View contains the individual feedback loop in Equipment View. The bottom layer of the stack is the basic building block of a system (e.g., equipment and processes). The top layer of the stack is the macroscopic view of a society.

Each layer has its own set of goals, which drive the decision-making and actions taken by the agents in that level. The decisions are taken based on the inputs the layer receives from the layers immediately above and below it. Similarly, the actions are communicated to these adjacent layers as outputs. These decisions/actions are indicated, in Figure 2.1, by the arrows that capture these information flows, up and down the hierarchy. These information flows are the feedback loops between the layers (i.e., *inter-layer* feedback loops). There are also feedback loops within a given layer, as depicted in Figure 2.1, which are *intra-layer* loops. Associated with each layer is a set of agents (autonomous and non-autonomous), organized in a particular configuration that is appropriate for the goals of that layer (e.g., the layout of equipment in a chemical plant, called a flowsheet). Such a multi-layered representation lends itself naturally to account for emergent phenomena that arise from one scale to another.

We propose a uniform and unified input-output modeling framework, that is conceptually the same across all levels. This elementary input-output model structure that serves as a building block in our framework is shown in Figure 2.2. Specifying such a uniform modeling structure across all levels has the advantage of integrating and unifying the analysis of the outcomes at different levels in a consistent manner. Such a template structure allows us to systematically identify the various failure modes of the different elements at different levels of the hierarchy as we discuss below. There are five key elements in this control-theoretic information modeling building block: (i) sensor, (ii) actuator, (iii) controller, (iv) "process" unit that transforms inputs to outputs, (v) connection (e.g., wires and pipes). These combined with input and output complete the picture. The functions of these elements, as well as their failure modes, at different levels of the hierarchy are illustrated with examples in the discussion below, using examples from chemical engineering. It is relatively easy to generalize this discussion to other engineering domains. The domain of finance requires a special treatment and we make that connection wherever needed.

As an organized group, these entities collect, decide, act on, report, and receive a variety of performance information and metrics. At any level, the layer below act as sensors, actuators, and processes in the inter-layer feedback loop, while the layer above it behaves like a controller that evaluates the lower level performance and sets new goals. In a chemical plant, for example, in the Equipment View layer (Chapter 2.2.1), they collect, decide, and act on individual process and equipment performance data and metrics (such as temperature, pressure, flow rate, batch times, etc.), that are vital for safe, efficient and profitable operation, and report them to the Plant View layer (Section 2.2.2), and receive, in turn,

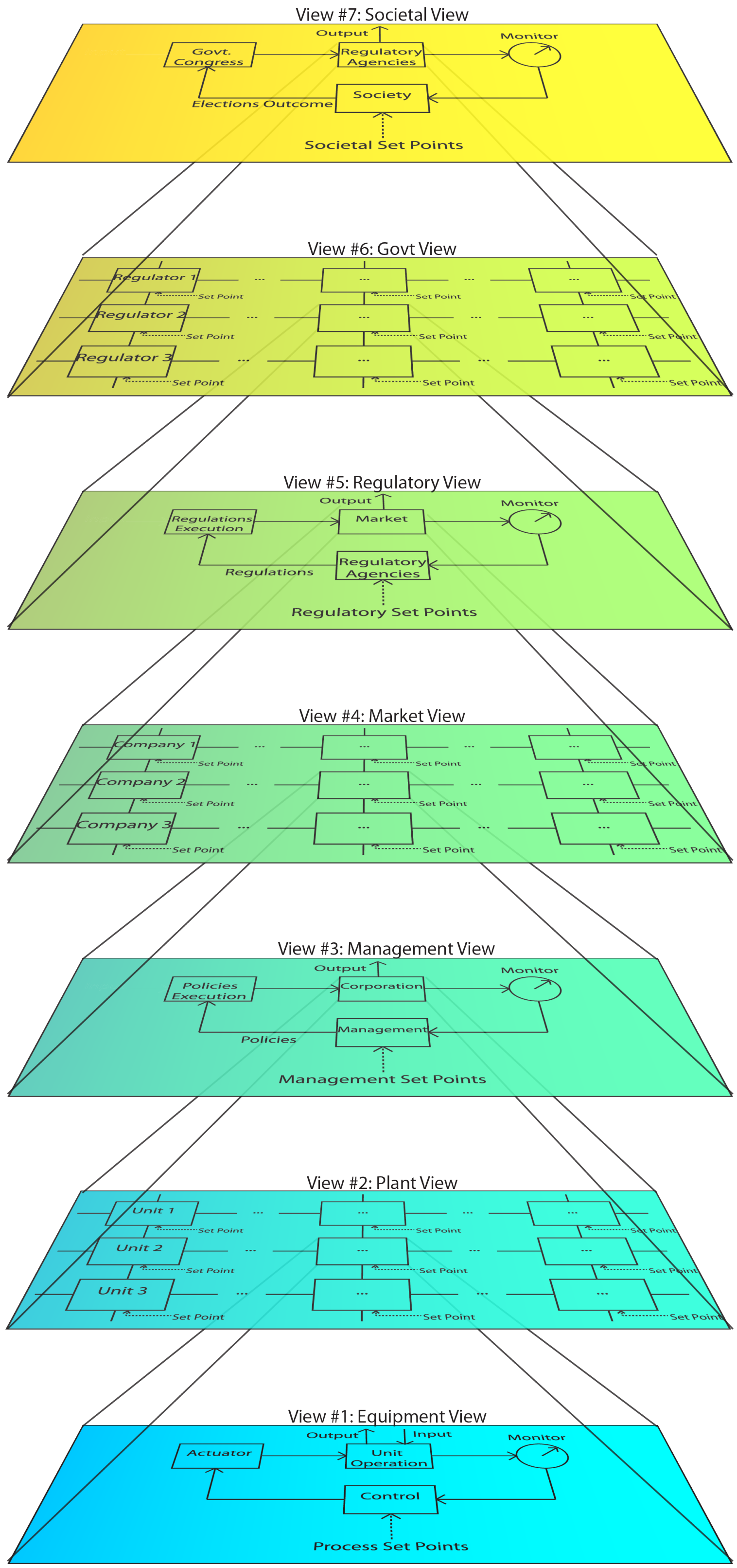


Figure 2.1: TeCSMART framework

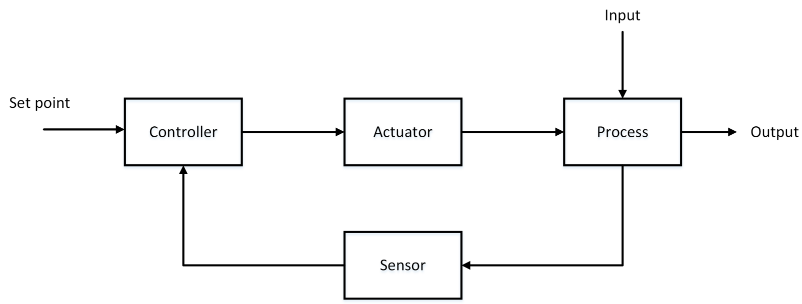


Figure 2.2: Schematic of a feedback control system (adapted from [Stephanopoulos, 1984], fig. 13.1b, pp. 241)

local control specifications (such as temperature and pressure set points) from Plant View layer. The Plant View layer agents make these decisions by considering information from all the processes and equipment under its purview as well as by considering manufacturing targets (such as what to make, how much to make, when to make, etc.). These targets, in turn, are decided by the agents in the Management View (Chapter 2.2.3), which get translated into the associated set points and constraints by the agents in the Plant View, and communicated down to the Equipment View as inputs. The target metrics are decided by the agents in Management View by responding to competitive market conditions as dictated by the Market View (Chapter 2.2.4). In a similar manner, relevant information regarding market or company stability, performance, fair competition, etc. are monitored and acted on by the agents in the Regulatory View (Chapter 2.2.5), by enacting and enforcing appropriate regulations approved by the agents in the Government View (Chapter 2.2.6) (such as the Congress in the U.S.). In an ideal democracy, a government is elected by the citizens of that society, the Society View (Chapter 2.2.7), who have the final word in determining what kind of government and laws they would like to live by.

Similar activities occur within layers through intra-layer feedback loops. In the Equipment View layer, for example, a stirred tank heater depicted in Figure 2.3 has sensors to measure temperature and tank level. Controllers evaluate these metrics, and send new control signals to valves. In the Management View layer, a firm's accounting team collects the performance data and share with the Board of Directors. The Board sets company's goal based on the data. Each division follows the goal and carry out its daily operations.

Periodically, new performance data is collected and the goal updated. At each layer, if autonomous or non-autonomous agents do not comply with the goal, disturbances arise at that layer. Controllers take the disturbance into account and set goals accordingly. Such intra-layer feedback loops exist in all seven layers. Details of each layer will be presented in the following discussion.

2.2.1 Perspective I: Equipment View Layer

In the Equipment View layer, the focus is on individual equipment such as reactors and distillation columns in the context of a chemical plant and their operating conditions. A chemical plant is a collection of such process units suitably organized (called a flowsheet) to meet the plant-wide goal of manufacturing a desired chemical product at targeted levels of quality, quantity, cost, time of delivery, etc., safely and optimally. This collection is seen in Perspective II, the Plant View layer. The time scale for the Equipment View layer is typically in seconds and minutes as process dynamics happens in real-time.

In the Equipment View layer, the autonomous agents involved are typically engineers and operators, and the non-autonomous agents are equipment including control systems. While regulatory control systems can exhibit a certain degree of autonomy, that is negligible compared to the range of autonomy exhibited by humans. Hence, we classify regulatory controllers as non-autonomous.

Consider, for example, a stirred tank heater process (Figure 2.3) where the goal is to control the level h and temperature T of the fluid in the tank that is subject to fluctuations in the inlet flow rate F_i and temperature T_i. The desired level of the fluid is referred to as the set point level h_{set} and the desired temperature T_{set}. These are accomplished by the two feedback controllers (loops 1 and 2), which receive the current F and T in real-time from the sensors (level gauge and thermocouple), by suitably manipulating the outlet flow rate F and steam flow rate, F_{steam}, by opening or losing the respective control valves (actuators). The seven elements of the information modeling block for this system are: (i) input: F_i, T_i, F_{set}, T_{set}, F_{steam}, (ii) output: h and T, (iii) sensors: level gauge and thermocouple, (iv) actuator: outlet flow and steam valves, (v) controller, (vi) “core” process unit: tank and heater, and (vii) connection: pipes and wires. The constraints are lower and upper limits on the level and the temperature of the fluid in the tank.

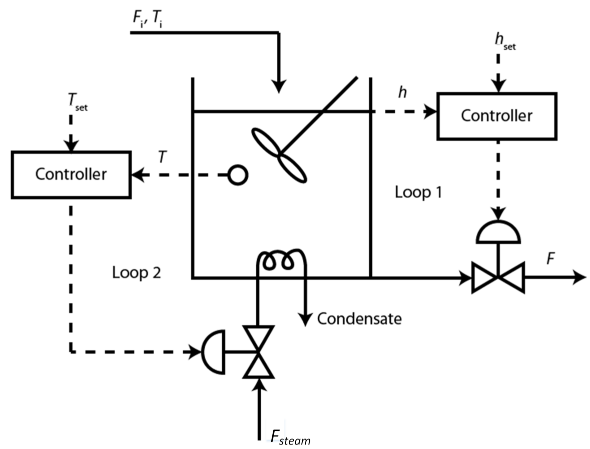


Figure 2.3: Stirred tank heater example (adapted from [Stephanopoulos, 1984], pp. 89)

The goal at the Equipment View is centered on the performance of individual equipment such as heaters, reactors, distillation columns, etc. – i.e., each equipment has its goal of operating at the set point(s). At this level of granularity, typically, for engineering applications, one can develop detailed dynamical models of the equipment and processes. These tend to be a set of DAE which are solved to simulate process/equipment behavior. Since the purpose of this chapter is not to discuss these models at length, we refer the interested reader to several standard sources in the literature [Stephanopoulos, 1984; Seborg *et al.*, 2011; Ogunnaike and Ray, 1994; Bequette and Bequette, 1998]. As an example, we list below the dynamical model equations for the stirred tank heater.

$$A\frac{dh}{dt} = F_i - F$$
$$Ah\frac{dT}{dt} = F_i(T_i - T) + \frac{Q}{\rho C_p}$$

Another kind of model used at this level, called SDG, is based on graph theoretical ideas to represent *cause and effect* relationships in a process or equipment. The SDG model for the heater example is shown in Figure 2.4. The nodes represent input and output variables. The arcs represent either positive (solid lines) or negative (dotted lines) relations between nodes. The figure is read as follows: a change in the inlet temperature T_i positively affects the temperature T in the stirred tank, e.g., if T_i increases, T will increase. T negatively affects the temperature difference T_ϵ, which is the set point temperature T_{set} minus stirred tank temperature T. As T increases, T_ϵ decreases. It means that less steam F_{steam} is needed in the stirred tank, because T gets close to the set point temperature T_{set}. This positive relation between T_ϵ and F_{steam} is depicted by a solid arc between the two nodes. F_{steam}, in turn, positively affects the temperature T in the stirred tank. This causal behavior among T, T_ϵ, and F_{steam} refers to loop 2 in Figure 2.3.

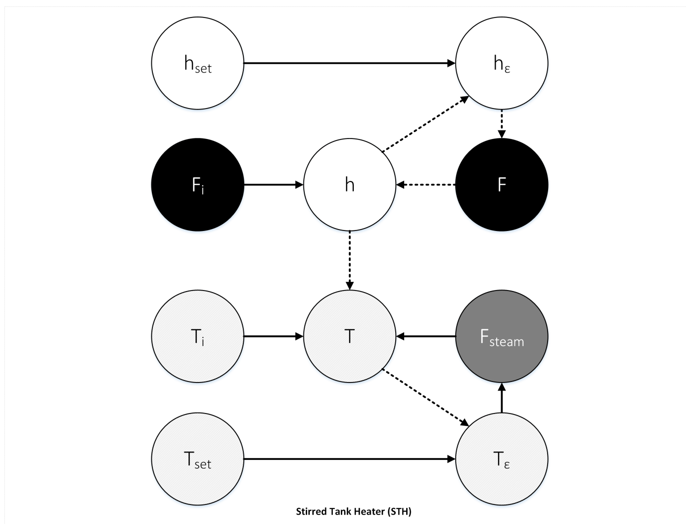


Figure 2.4: SDG for the tank heater example

Nevertheless, such cause-and-effect based qualitative models are very useful when modeling a social system, where DAE models are usually hard to develop, such as a bank-dealer system (which will be explained in detail in Chapter 3.3). In this case, the nodes are variables related to a bank-dealer's investment and lending activities. In Figure 2.5, the left-hand side depicts the connections and activities within the bank-dealer, while the right-hand side shows the SDG model. A bank-dealer system consists of three major desks, among which the finance desk determines where money should go; the prime broker determines how much money to lend based on the collateral collected; and the trading desk determines whether sell to the market or buy from the market based on money received from the finance desk and the leverage ratio it holds. The SDG model is read as follows: finance desk collateral C_{FD} positively affects the funding capacity V_{FD}. V_{FD} in turn positively affects the loan capacity of prime broker V_{PB} and the leverage set point of trading desk $\lambda_{\text{TD}}^{\text{SP}}$. In the prime broker, both the collateral amount C_{PB} and the margin rate χ_{PB} positively affect the loan capacity V_{PB}. In the trading desk, the leverage set point $\lambda_{\text{TD}}^{\text{SP}}$ and current leverage λ_{TD} determine the leverage different ϵ_{TD}, which positively affects the inventory quantity of trading desk Q_{TD}. Using the SDG model, one can quickly examine the causal relations of a social system like the bank-dealer system, and study unstable conditions and risks such as the fire sale and funding run scenarios.

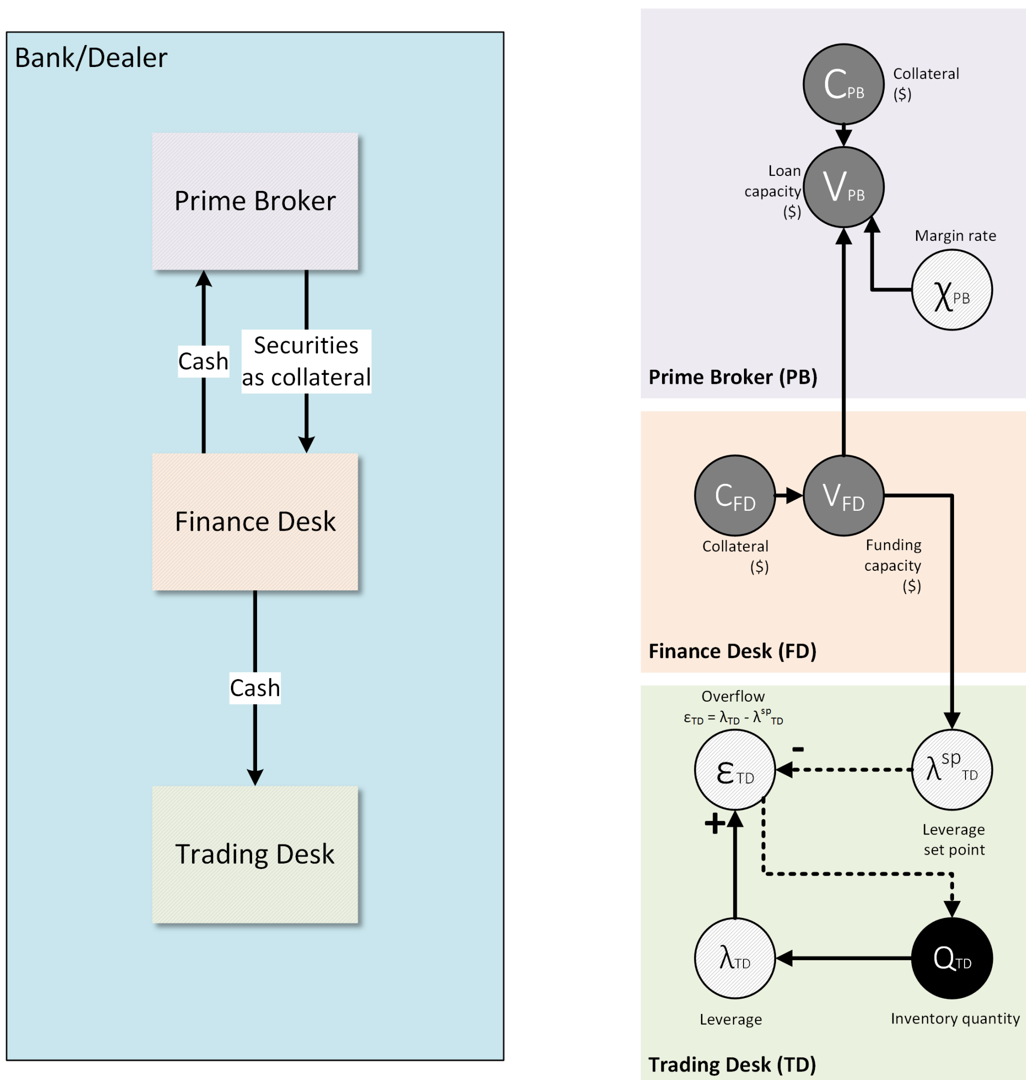


Figure 2.5: SDG for the bank/dealer example

One can always incorporate other modeling methods with the TeCSMART framework. Usually, in order to develop a quantitative model (DAE model) or a qualitative model

(SDG model), one needs to determine the initial conditions of a system. System initial conditions at this level are values associated with equipment, such as sensor readings or controller parameters. Examining failure modes using TeCSMART framework provides a systematic way for identifying system initial conditions. By giving different system initial conditions, modelers can develop suitable models to describe the system and conduct in-depth risk analysis. Therefore, no matter what modeling methods or risk assessment tools one will use, a HAZOP-like systematic analysis using TeCSMART framework is feasible for analyzing risks in a sociotechnical system. It enables a systematic hazard identification for the risk assessment of a sociotechnical system.

The basic functional building block in Figure 2.2 allows us to model systematically the potential failures at different levels of both human and non-human elements. In the Equipment View layer, let us consider a sensor, for example. Using a commonly used model of its failure modes, we can state that a sensor can fail high, low, or zero (i.e., no response, sensor is dead). Similarly for an actuator (a valve can fail high, low, or zero) and a controller. A process might have more failure modes depending on its complexity, but it is usually not in hundreds, more like a dozen or so. The connections can fail, too, again high, low, zero, or reverse (in the case of flow rate in pipes, for example). One can modify these to make the set of failure modes more sophisticated, if needed, but even this elementary set goes a long way as we discuss below. We will show below how these failure modes can be generalized to accommodate typical human failures as well at different levels of the hierarchy.

2.2.2 Perspective II: Plant View Layer

The Plant View layer is a collection of all the equipment and processes organized in a particular configuration (or flowsheet) in order to manufacture a desired product safely and optimally. The autonomous agents involved in this layer are managers and supervisors, and the non-autonomous agents are equipment clusters. These clusters are usually grouped as critical process steps or unit operations [Seider *et al.*, 2009], such as reaction, distillation, etc., which are needed in the manufacture of the desired product. Similarly, in the financial system example, the left figure in Figure 2.5 is the simplified "flowsheet" of a bank-dealer system. The Plant View agents collect and report metrics regarding aggregate production performance and safety to Management View and receive, in turn, plant-wide target specifications from Management View, as noted above. Although this level is also operating in real time, the Plant View decisions typically have a larger time scale (hours or even days).

The goal at this level is to ensure meeting production performance targets (typically, product quantity and quality, cost, and time of delivery) safely and optimally at the overall plant level. These plant-wide targets would translate into equipment specific targets implemented as set points and constraints that are communicated to the Equipment View level. Models at this level tend to be DAE models from Perspective I integrated together reflecting the overall flowsheet organization of the plant. The flowsheet is then simulated to obtain plant-wide process and equipment behavior. One can also formulate such connected models using the SDG models from the lower level as well to explicitly capture the cause-and-effect relationships which are then used for applications such as PHA [Venkatasubramanian *et al.*, 2000; Venkatasubramanian and Vaidhyanathan, 1994; Srinivasan and Venkatasubramanian, 1996; Srinivasan and Venkatasubramanian, 1998a; Srinivasan and Venkatasubramanian, 1998b; Vaidhyanathan and Venkatasubramanian, 1995; Vaidhyanathan and Venkatasubramanian, 1996].

The input-output information model at this aggregate level is shown in Figure 2.1. From this level onward, going up to the higher levels, the emphasis shifts from decisions/actions made by individual equipment to those made by personnel, and from real-time sensor data to aggregate information concerning the overall plant performance. It moves from a *data-centric* to *information-centric* perspective. This is required to reflect the goal of this layer – to make the desired products at the targeted level of quality, quantity, cost, time of delivery, safely and optimally. That is the charge of the Plant Manager, given to her by the senior management at the next layer above.

The seven elements here, therefore, reflect this aggregate nature of information needed and used at this level: (i) input: aggregate, plant level, information on target as well as actual performance metrics, (ii) output: schedule, set points, resource allocation, etc., (iii) sensors: product quality and quantity, resource utilization data, etc., (iv) actuator: plant personnel, (v) controller: Plant Manager, (vi) “core” process unit: the entire plant, and (vii) connection: various communication channels among plant personnel such as the Managers, Supervisors, Engineers, and Operators.

The failure modes associated with the elements at this level are conceptually similar to their counterparts at the lower Equipment View layer. For instance, sensors in this layer are *not physical entities* like thermocouples, but *informational entities* that aggregate and transform relevant data into actionable information such as the projection made about the plant's product output for the current month. This transformation is carried out by a human, such as a process engineer. The engineer can also "fail" high, low, or zero in the sense that the estimation reported to the Plant Manager can be erroneous along these lines – e.g., the projection may be too optimistic (i.e., failing high), too conservative (i.e., failing low), or no projection is made (i.e., failing zero). Likewise, communication can also fail along these lines – perhaps the projection was made, but the Manager was not informed. Similarly, in a bank-dealer system, this layer represents the aggregation of investment and funding activities of different asset classes. The three major desks are divided into groups (actuators) to handle portfolios consisting of different assets. Sensors (i.e., analysts monitoring the metrics) in the lower Equipment View layer for a bank-dealer system report leverage ratios or collateral collected; while sensors in this layer are risk models of portfolios, which aggregate and transform individual risk factors into a comprehensive picture that describes the portfolio's risk. We, thus, see that this template helps us identify systematically where and how things can fail at different levels of the hierarchy.

It is important to note that we are not claiming that our framework would capture all things that go wrong in a complex system. We are only suggesting that such a systematic approach could capture many of the typical failures seen in practice and we demonstrate this with the aid of three case studies.

2.2.3 Perspective III: Management View Layer

The next level up is the Management View, where the agents involved are the critical decision makers such as the CEO, Senior Vice Presidents, and Board of Directors. Their goal is to maximize profitability and create value for the shareholders by making sure the company's business performance metrics (including safety) meet the expectations from the Market (which is the next level up). Influenced by the nature of business and accounting cycles, this layer operates in a time scale of quarter (i.e. 3-month period) to a year.

As seen in the control-theoretic information model of this level in Figure 2.6, this group of decision-makers (Management team) set the overall policies that "control" (i. e., manage) the behavior and outcomes of the corporation including its autonomous and non-autonomous assets. Autonomous agents at this layer include managers and supervisors of each division, while the non-autonomous agents are corporate assets. The Market at the next level up sets and demands certain performance targets be met by the company for its survival and growth. These metrics are usually financial at this level such as Return On Investment (ROI), Return On Equity (ROE), market share, sales growth, etc. These are the *set points* and *constraints* given to the Management team.

The Management team, in turn, translates these targets into actionable *quantitative* information such as production performance metrics, strategic deployment of resources, etc., at different plants (the corporation might have several plants distributed all over the world) as well as more *qualitative* ones that define the company culture including the safety culture. They also set the incentive policy to encourage better performance from the employees. These are communicated to the Plant View layer as their *set points* and *constraints*. The Management team decides on these targets by taking into account of all relevant information concerned with the survival, profitability and growth of the company in a competitive and regulatory environment. Thus, the information flow is not only from the company's internal sources but also from the environment, which are the two levels immediately above.

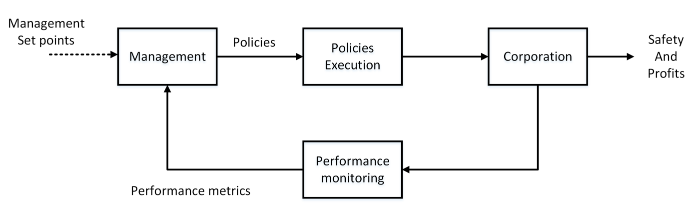


Figure 2.6: Control theoretic model of company/management layer

Differing from the control policies at the lower levels, which mainly focus on controlling equipment (i.e., non-autonomous agents), the policies from this layer onward, at the higher levels, focus more on achieving the desired behavior and outcomes from autonomous agents (i.e., humans). As a result, while the lower level control policies can be based on precise models of process/equipment (as captured by DAE models), the higher level policies will necessarily have to deal with imperfect models of human behavior which cannot be reduced to a set of equations. Consider, for instance, the difficulties involved in "modeling" the culture of a corporation. At best, we might be able to identify certain key features or characteristics that define a corporation's culture. From this level onward, we have to rely more on graph theoretic, game theoretic and agent-based modeling frameworks. Thus, from this level onward modeling becomes trickier, and the notion of "control" of agents transitions to the "management" of agents. Moreover, the importance of TeCSMART failure modes-based examination becomes more obvious. Such a systemic risk analysis of human decision-making would help improving safety-related management activities, among other things.

The Management team acts as a "controller" to monitor the various performance metrics (e.g., sales, expenses, revenue, profits, ROI, ROE, etc.), compare them with the set points, and take appropriate actions by manipulating the relevant variables (e.g., cost cutting, acquisition, etc.) in order to meet the set point targets. The Management level deals with the big picture and general strategy for the corporation as a whole. These get translated into more detailed prescriptions and recommendations as they are communicated from this layer to the lower layers. The failure of the elements in Figure 2.6 can be modeled along the lines of Equipment View and Plant View layers. For example, the Performance Monitoring task (i.e., "sensor") may fail because of errors in the measurements or estimations (e.g., fail high, low, or zero) or they may be communicated (or not communicated at all) erroneously. One can methodically identify similar failure modes for the other elements including the connections (which are the communication channels).

2.2.4 Perspective IV: Market View Layer

Similar to the Plant View, the Market View is a collection of companies that compete, in the appropriate product/service categories, for economic survival, profitability and growth in a free market environment. The agents at this level are mainly the customers and corporations. Market is a well-studied concept in economics. It usually refers to the exchange activities that many parties engage in. In this chapter, we won't discuss the economic aspect of Market, but interpret Market as a collection of companies and their activities. Market activities such as cooperation and competition can be explained using the input-output model structure and intra-layer feedback loops. From this layer and above, activities mainly involve autonomous agents such as humans and human organizations. The information generated at this level (e.g., stability of individual companies and the market, fairness practices, etc.) are communicated to the Regulatory View and from there receive regulatory requirements and enforcement actions. While the market dynamics is in real-time, as with the Plant View, the relevant time scale is of the order of months.

2.2.5 Perspective V: Regulatory View Layer

As noted, regulatory agencies oversee the market and control the market behavior through the enforcement of regulatory policies (Figure 2.7). The primary goal at this level is to ensure the security, stability, and wellbeing of the society where these companies operate. This means, of course, the security and wellbeing of the citizens and their environment. This also means ensuring that the free market, where these companies compete, is stable, efficient and fair. The autonomous agents are regulatory agencies such as Occupational Safety and Health Administration (OSHA), Environmental Protection Agency (EPA), Securities and Exchange Commission (SEC), Federal Reserve (FED), Federal Energy Regulatory Commission (FERC), Minerals Management Service (MMS), Food and Drug Administration (FDA), and so on, and the appropriate executives from the companies.

These agencies receive from the agents in Government View, namely, lawmakers and their staff, regulations which they enforce on the market participants. They also monitor the market and companies, collect information, and report the effects of regulations to the agents in Government View for potential improvements. This feedback control loop acts at a time scale of years.

One typical example of this view is the activity of the SEC which regulates the securities industry (Figure 2.8). SEC receives laws and regulatory directives from the agents in Government View, such as the President, the Congress, and the FED Board. Through its 5 divisions and 23 Offices, SEC enforces federal securities laws, issues new rules, and oversees securities related activities. For instance, SEC regularly monitors the market for unusual

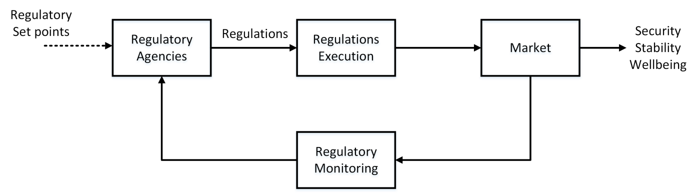


Figure 2.7: Control theoretic model of regulatory layer

trading patterns that might reveal illegal acts such as insider trading, and take corrective actions, playing its role as a "controller" here, to ensure fairness in the security markets. While SEC should be praised for its post-financial crisis actions on successfully going after various Wall Street entities for their misconduct, various failures of the SEC before and during the crisis contributed to the crisis, as Judge Rakoff argues persuasively [Rakoff, 2014]. Many of these failures are faults of the elements in Figure 2.7 that can be modeled using our template of failure modes. In a similar manner, many of the failures at the MMS [Eilperin and Higham, 2010] that contributed to the BP Oil Spill disaster can be modeled using our approach. While we do not get into all the details, as that would make this chapter too long, we do provide a summary of these failures in a series of tables that compare regulatory failures in three different domains later in the chapter.

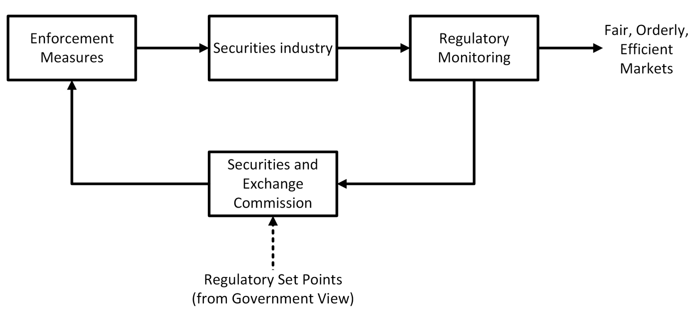


Figure 2.8: Control theoretic model of Securities and Exchange Commission

2.2.6 Perspective VI: Government View Layer

The Government View, like the Plant and Market Views, is a collection of various agencies particularly organized to govern a society of autonomous and non-autonomous agents (e.g., physical assets). The objectives here are security, stability, and the overall wellbeing of the agents and their environment against a variety of risks and threats. Depending on the societal preference for capitalism, communism, socialism, monarchy, or dictatorship, the institutions and their structure can be widely different. The objective of this chapter is not to discuss these in any detail (there are vast resources on this subject in sociology and political science) but only to show how our control theoretic framework accommodates the structures and functions at this level in a uniform and consistent manner which is helpful for a system-theoretic analysis of system-wide risks and threats. In the context of the U.S., this structure is the three branches of government - executive, congress, and judiciary – with the associated agencies they supervise. The agents are the members of these branches. The time scale is typically four years, the presidential election cycle, but institutional memory in congress and judiciary can prolong this to decades. That is, it can take that long to make significant changes in governance.

2.2.7 Perspective VII: Societal View Layer

Finally, we arrive at the top most level in this modeling hierarchy. The primary agents (autonomous) are the citizens and elected officials in a democracy such as the U.S. It is, of course, very different for other political structures, as noted. Again, while the presidential election cycle imposes a certain natural characteristic time, institutional memories can prolong this to decades. The societal "set points" are the preferences of its citizenry, which can vary over time, typically, of the order of decades or generations. In an ideal democracy, the citizens get to decide what kind of society or country they all would like to live in. The overall goals of the citizens in the U.S., as expressed in the Declaration of Independence document, are Life, Liberty and the Pursuit of Happiness [Jefferson, 1776]. Given these goals, in every election, the citizens get to vote on a number of issues related to economy, environment, education, health, security, privacy, race relations, etc.

This is the top most layer of the model. In its feedback loop, there are citizens, elected government officials and regulators involved. In the Government View layer, the three branches of the U. S. government act as the "controller" of a collection of regulatory agencies and the country. In the Societal View layer, citizens oversee and influence the society through elections. It usually takes decades for a society to adapt and evolve in any significant fashion. The societal set point is related to the history and culture of a nation.

In all systemic failures, such as the ones mentioned above, we all play a role, through the Societal View layer, and are accountable for some of the blame, as it was our collective decision to elect (in the case of U.S.) a particular party, and its political and regulatory views, to govern us. This accountability is a direct consequence of our responsibility. Consider, for example, the responsibility of a CEO of a large petrochemical company with many plant sites and tens of thousands of employees. The CEO may not know everything about what goes on in all her plant sites, on a daily basis, but when a disaster strikes she and her c-suite executives are held accountable. Time and again, in all the official inquiries of major disasters, whether it was Bhopal, Piper Alpha, BP Oil Spill, Global Financial Crisis, Northeast Power Blackout, and so on, the management was help responsible and accountable for their companies failures. In fact, in a historic first, establishing an encouraging precedent, recently in April 2016, former Massey Energy CEO was sentenced to twelve months in prison as a result of the mining company's disaster [Blinder, 2016; Steinzor, 2014]. Thus, the people in charge have to be held accountable for part of the blame. In a democratic society, the people in charge are, ultimately, us, the citizens who elected the government.

Therefore, we are responsible, in some part, for the failures resulting from its policies. We are thus responsible for Bhopal, BP Oil Spill, Subprime Crisis, and so on. This is why it is vitally important for the citizens to stay informed, engaged and active in the political process. This is particularly important to remember as we begin to address the mother of all systemic failures, the Climate Change Crisis, which has been in the works for decades.

2.3 Failure Analysis and Comparison

In this section, we discuss the results of applying the TeCSMART framework to three prominent systemic failures, namely, the BP Texas City Refinery Explosion (2005), Global Financial Crisis (2008-09), and the Northeast Power Blackout (2003). We in fact studied the following twelve systemic failures: (i) the Bhopal Disaster (1984), (ii) the Space Shuttle Challenger Disaster (1986), (iii) the Piper Alpha Disaster (1988), (iv) the SARS

Outbreak (2002-03), (v) the Space Shuttle Columbia Disaster (2003), (vi) the Northeast Power Blackout (2003), (vii) the BP Texas City Refinery Explosion (2005), (viii) Global Financial Crisis (2008-09), (ix) the BP Deepwater Horizon Oil Spill (2010), (x) the Upper Big Branch Mine Disaster (2010), (xi) the Fukushima Daiichi Nuclear Disaster (2011), and (xii) the India Blackouts (2012), by carefully reviewing the official *post mortem* reports of these disasters as well as other relevant sources. However, we are presenting the comparative analysis of only these three disasters for the sake of brevity. The other cases have similar failure patterns as well, more details can be found in Appendix A. We analyzed and classified over 700 failures mentioned in these reports [Drilling, 2011; Commission, 2011; CSB, 2005; Browning, 1993; Representative and of, 1986; Cullen, 1993; Organization, 2006; Board, 2003; Force, 2004; Baker *et al.*, 2007; McAteer *et al.*, 2011; Kurokawa *et al.*, 2012; CERC, 2012]. We categorize these failures into 5 primary classes, and 19 subclasses, that are consistent with the typical failure modes presented in Chapter 2.2.

The five classes are as follows:

1. Monitoring Failures; 2. Decision-Making Failures; 3. Action Failures; 4. Communication Failures; and 5. Structural Failures. Each category has sub-categories that define more detailed failures. Subclass details are listed in Table 2.1 - 2.4. The five-class failure taxonomy reveals "what can go potentially wrong" in a complex sociotechnical system. It summarizes the failure modes modeled using the TeCSMART framework. Different failure modes give rise to systemic failures in different domains. However, there are common failure modes shared by many, if not, all the systemic failures. Such common failure pathways help us identify, *proactively*, how things can potentially go wrong in a complex system. By studying these common failure mechanisms, people could become more vigilant for new systems. Thus, the common patterns identified by our comparative analysis are helpful *not only diagnostically but also prognostically.*

The comparative analysis of the three case studies is performed in following three steps. (i) Carefully review the official *post mortem* reports and classify the failures into different classes/subclasses mentioned in Tables 2.1 - 2.4. For example, the level control valve was accidentally turned off by an operator in BP Texas City Refinery. This failure is classified as a flawed action (3.1 in Table 2.3). The over-grown tree is a known problem for all power grid operators. But First Energy (FE) failed to trim the over-grown trees, which led to line trips. The inadequate tree trimming is classified as a late response failure (3.2 in Table 2.3). (ii) Once failures are classified properly, they are organized in the TeCSMART framework according to the relevant agents and the failure mechanisms. Relevant agents indicate the level of the failure in the TeCSMART framework, and the failing mechanisms explain which control component the failure is associated with. One layer can have multiple failures, and one failure can appear multiple times at different levels. Therefore, the level control valve failure is a flawed action of actuator at the Process View, and the inadequate tree trimming is due to late response of actuator at the Plant View. (iii) Compare failures across domains to identify common patterns.

Table 2.1: Failure taxonomy part I

Class	**Definition**	**Examples**
1. Monitoring Failures	Failure to monitor the key parameters effectively or having significant errors in the monitored data	
1.1 Fail to Monitor	Failure to monitor key performance indicators (“failing zero”)	In **BP Texas City Refinery Explosion**, numerous measures for tracking various types of operational, environmental and safety performance, but no clear focus on the leading indicators for the potential catastrophic or major incidents. In **Northeast Blackout**, MISO did not discover that Harding- Chamberlin had tripped until after the blackout, when MISO reviewed the breaker operation log that evening. In **Subprime Crisis**, Moodys did not sufficiently account for the deterioration in underwriting standards or a dramatic decline in home prices. And Moodys did not even develop a model specifically to take into account the layered risks of subprime securities until late 2006, after it had already rated nearly 19,000 subprime securities.
1.2 Failure to monitor effectively	Failure to detect/report problems in a timely manner	In **Northeast Blackout**, the Cleveland-Akron areas voltage problems were well-known and reflected in the stringent voltage criteria used by control area operators until 1998. **BP Texas City** did not effectively assess changes involving people, policies, or the organization that could impact process safety.
1.3 Significant errors in monitoring	Monitored data is significantly inaccurate. It is either over-reporting (“failing high”) or under-reporting (“failing low”) the actual trend	In **BP Texas City Refinery Explosion**, a lack of supervisory oversight and technically trained personnel during the startup, an especially hazardous period, was an omission contrary to BP safety guidelines. An extra board operator was not assigned to assist, despite a staffing assessment that recommended an additional board operator for all ISOM startups. In **Northeast Blackout**, from 15:05 EDT to 15:41 EDT, during which MISO did not recognize the consequences of the Hanna-Juniper loss, and FE operators knew neither of the lines loss nor its consequences. PJM and AEP recognized the overload on Star-South Canton, but had not expected it because their earlier contingency analysis did not examine enough lines within the FE system to foresee this result of the Hanna- Juniper contingency on top of the Harding-Chamberlin outage.
2. Decision Making Failures	Failure to provide the correct decisions in a timely manner	
2.1 Model failures	Decisions are not supported by the local system (i.e., “plant-model mismatch”)	In **Subprime Crisis**, financial institutions and credit rating agencies embraced mathematical models as reliable predictors of risks, replacing judgment in too many instances. In **Northeast Blackout**, one of MISOs primary system condition evaluation tools, its state estimator, was unable to assess system conditions for most of the period between 12:15 and 15:34 EDT, due to a combination of human error and the effect of the loss of DPLs Stuart- Atlanta line on other MISO lines as reflected in the state estimators calculations.
2.2 Inadequate or incorrect local decisions	Decisions made are unfavorable to the local system under supervision	In **BP Texas City Refinery Explosion**, the process unit was started despite previously reported malfunctions of the tower level indicator, level sight glass, and a pressure control valve. In **Subprime Crisis**, financial institutions’ inadequate decisions of using excessive leverage and complex financial instruments. In **Northeast Blackout**, FE uses minimum acceptable normal voltages which are lower than and incompatible with those used by its interconnected neighbors.
2.3 Inadequate or incorrect global decisions	Decisions made are unfavorable for the global system, but could be locally right	In **Subprime Crisis**, the banks had gained their own securitization skills and didnt need the investment banks to structure and distribute. So the investment banks moved into mortgage origination to guarantee a supply of loans they could securitize and sell to the growing legions of investors. But they are lack of global views of the entire market. In **Northeast Blackout**, many generators had pre-designed protection points that shut the unit down early in the cascade, so there were fewer units on-line to prevent island formation or to maintain balance between load and supply within each island after it formed. In particular, it appears that some generators tripped to protect the units from conditions that did not justify their protection, and many others were set to trip in ways that were not coordinated with the regions under-frequency load-shedding, rendering that UFLS scheme less effective.

Table 2.2: Failure taxonomy part II

Class	Definition	Examples
2.4 Resource Failures	Failure to acquire, allocate and manage the required resources properly to complete the tasks safely and achieve the goal(s)	
2.4.1 Lack of resources	Failure to acquire the necessary resources, such as funds, man power, time, etc.	In **BP Texas City Refinery Explosion**, BP has not always ensured that it identified and provided the resources required for strong process safety performance at its U.S. refineries, including both financial and human resources. In **Subprime Crisis**, in an interview with the FCIC, Greenspan went further, arguing that with or without a mandate, the Fed lacked sufficient resources to examine the nonbank subsidiaries. Worse, the former chairman said, inadequate regulation sends a misleading message to the firms and the market. But if resources were the issue, the Fed chairman could have argued for more. It was always mindful, however, that it could be subject to a government audit of its finances. In **Northeast Blackout**, there is no UVLS system in place within Cleveland and Akron; had such a scheme been implemented before August, 2003, shedding 1,500 MW of load in that area before the loss of the Sammis-Star line might have prevented the cascade and blackout.
2.4.2 Inadequate allocation of resources	Resources are deployed incorrectly. E.g., over-staffing ("failing high") in some areas while under-staffing ("failing low") elsewhere	In **BP Texas City Refinery Explosion**, the incident at Texas City and its connection to serious process safety deficiencies at the refinery emphasize the need for OSHA to refocus resources on preventing catastrophic accidents through greater PSM enforcement. In **Northeast Blackout**, on August 14, the lack of adequate dynamic reactive reserves, coupled with not knowing the critical voltages and maximum import capability to serve native load, left the Cleveland- Akron area in a very vulnerable state.
2.4.3 Training failures	Failures related to the lack of organized activity(ies) aimed at helping employees attain a required level of knowledge and skill needed in their current job. This includes emergency response training	In **BP Texas City Refinery Explosion**, BP has not adequately ensured that its U.S. refinery personnel and contractors have sufficient process safety knowledge and competence. In **Subprime Crisis**, in theory, borrowers are the first defense against abusive lending. But many borrowers do not understand the most basic aspects of their mortgage. Borrowers with less access to credit are particularly ill equipped to challenge the more experienced person across the desk. In **Northeast Blackout**, the FE operators did not recognize the information they were receiving as clear indications of an emerging system emergency.
2.5 Conflict of Interest	Incorrect decisions reached due to a conflict of interest arising from competing goals that can affect proper judgment and execution of tasks. E.g., safety vs financial gain, ethical failures such as corruption	In **BP Texas City Refinery Explosion**, cost-cutting, failure to invest and production pressures from BP Group executive managers impaired process safety performance at Texas City. In **Subprime Crisis**, many Moodys former employees said that after the public listing, the company [Moodys] culture changedit went from [a culture] resembling a university academic department to one which values revenues at all costs, according to Eric Kolchinsky, a former managing director. In **Northeast Blackout**, these protections should be set tight enough to protect the unit from the grid, but also wide enough to assure that the unit remains connected to the grid as long as possible. This coordination is a risk management issue that must balance the needs of the grid and customers relative to the needs of the individual assets.

Table 2.3: Failure taxonomy part III

Class	Definition	Examples
3. Action Failures	Actions carried out incorrectly or inadequately	
3.1 Flawed actions including supervision	Failure to perform the right actions, or performing no action, or performing the wrong actions. Failure to follow standard operating procedures	In **BP Texas City Refinery Explosion**, numerous heat exchanger tube thickness measurements were not taken. Some pressure vessels, storage tanks, piping, relief valves, rotating equipment, and instruments were overdue for inspection in six operating units evaluated. In **Subprime Crisis**, struggling to remain dominant, Fannie and Freddie loosened their underwriting standards, purchasing and guaranteeing riskier loans, and increasing their securities purchases. Yet their regulator, the Office of Federal Housing Enterprise Oversight (OFHEO), focused more on accounting and other operational issues than on Fannies and Freddies increasing investments in risky mortgages and securities. In **Northeast Blackout**, numerous control areas in the Eastern Interconnection, including FE, were not correctly tagging dynamic schedules, resulting in large mismatches between actual, scheduled, and tagged interchange on August 14.
3.2 Late response	Failure to take the right actions at the right time	In **BP Texas City Refinery Explosion**, Neither Amoco nor BP replaced blowdown drums and atmospheric stacks, even though a series of incidents warned that this equipment was unsafe. In the years prior to the incident, eight serious releases of flammable material from the ISOM blowdown stack had occurred, and most ISOM startups experienced high liquid levels in the splitter tower. Neither Amoco nor BP investigated these events. In **Subprime Crisis**, declining underwriting standards and new mortgage products had been on regulators radar screens in the years before the crisis, but disagreements among the agencies and their traditional preference for minimal interference delayed action. In **Northeast Blackout**, the alarm processing application had failed on occasions prior to August 14, leading to loss of the alarming of system conditions and events for FEs operators. However, FE said that the mode and behavior of this particular failure event were both first time occurrences and ones which, at the time, FEs IT personnel neither recognized nor knew how to correct.
4. Communication Failures	Failures that are associated with the system of pathways (informal or formal) through which messages flow to different levels and different people in the organization	
4.1 Communication failure with external entities	Failures of communication between an individual and/or a group/organization and an external individual and/or organization	In **BP Texas City Refinery Explosion**, BP and Amoco did not cooperate well to investigate previous incidents and replace blowdown drum. In **Subprime Crisis**, the leverage was often hidden. Lenders rarely discuss the leverage and the associated high risk with their investors. Investors relied on the credit rating agencies, often blindly. In **Northeast Blackout**, the Stuart-Atlanta 345-kV line, operated by DPL, and monitored by the PJM reliability coordinator, tripped at 14:02 EDT. However, since the line was not in MISOs footprint, MISO operators did not monitor the status of this line and did not know it had gone out of service. This led to a data mismatch that prevented MISOs state estimator (a key monitoring tool) from producing usable results later in the day at a time when system conditions in FEs control area were deteriorating.
4.2 Peer to Peer communication failure	Failures of communication between an individual and another individual within a group and/or organization	In **BP Texas City Refinery Explosion**, the night lead operator left early but very limited information about his control cations was given to day board operator. In **Northeast Blackout**, FE computer support staff did not effectively communicate the loss of alarm functionality to the FE system operators after the alarm processor failed at 14:14, nor did they have a formal procedure to do so.
4.3 Inter-level communication failure	Failures of communication between an individual and another individual at a greater or lower level of authority within the same group and/or organization	In **BP Texas City Refinery Explosion**, Supervisors and operators poorly communicated critical information regarding the startup during the shift turnover. In **Northeast Blackout**, ECAR and MISO did not precisely define critical facilities such that the 345-kV lines in FE that caused a major cascading failure would have to be identified as critical facilities for MISO. MISOs procedure in effect on August 14 was to request FE to identify critical facilities on its system to MISO.

Table 2.4: Failure taxonomy part IV

Class	**Definition**	**Examples**
5. Structural Failures	Deficient structures and/or models	
5.1 Design failures	Defects or deficiencies in the design of the system/component/model, or just wrong design of the system/component/model	In **BP Texas City Refinery Explosion**, occupied trailers were sited too close to a process unit handling highly hazardous materials. All fatalities occurred in or around the trailers. In **Subprime Crisis**, where were Citigroups regulators while the company piled up tens of billions of dollars of risk in the CDO business? Citigroup had a complex corporate structure and, as a result, faced an array of supervisors. The Federal Reserve supervised the holding company but, as the Gramm-Leach-Bliley legislation directed, relied on others to monitor the most important subsidiaries: the Office of the Comptroller of the Currency (OCC) supervised the largest bank subsidiary, Citibank, and the SEC supervised the securities firm, Citigroup Global Markets. Moreover, Citigroup did not really align its various businesses with the legal entities. An individual working on the CDO desk on an intricate transaction could interact with various components of the firm in complicated ways. In **Northeast Blackout**, although MISO received SCADA input of the lines status change, this was presented to MISO operators as breaker status changes rather than a line failure. Because their EMS system topology processor had not yet been linked to recognize line failures, it did not connect the breaker information to the loss of a transmission line. Thus, MISOs operators did not recognize the Harding-Chamberlin trip as a significant contingency event and could not advise FE regarding the event or its consequences. Further, without its state estimator and associated contingency analyses, MISO was unable to identify potential overloads that would occur due to various line or equipment outages.
5.2 Maintenance failures	Failure to adequately repair and maintain equipment at all times	In **BP Texas City Refinery Explosion**, deficiencies in BPs mechanical integrity program resulted in the run to failure of process equipment at Texas City. In **Northeast Blackout**, FE had no periodic diagnostics to evaluate and report the state of the alarm processor, nothing about the eventual failure of two EMS servers would have directly alerted the support staff that the alarms had failed in an infinite loop lockup.
5.3 Operating procedure failures	Failure to develop and execute standard operating procedures for all tasks	In **BP Texas City Refinery Explosion**, outdated and ineffective procedures did not address recurring operational problems during startup, leading operators to believe that procedures could be altered or did not have to be followed during the startup process. In **Subprime Crisis**, in addition to the rising fraud and egregious lending practices, lending standards deteriorated in the final years of the bubble. In **Northeast Blackout**, the PJM and MISO reliability coordinators lacked an effective procedure on when and how to coordinate an operating limit violation observed by one of them in the others area. The lack of such a procedure caused ineffective communications between PJM and MISO regarding PJMs awareness of a possible overload on the Sammis-Star line as early as 15:48.

2.4 TeCSMART Case Studies

In this section, we briefly introduce the three prominent systemic failures: Northeast Blackout (2003), BP Texas City Refinery Explosion (2005), and Subprime Crisis (2008), and compare their failures applying TeCSMART framework. The comparison study shows the similarities and differences of the three systemic failures. Moreover, the common patterns indicate important failure modes, which can help improve system design, control, and risk management.

The Northeast Blackout, happened on August 14, 2003, was the largest blackout of North America power grid. With many generating units tripping and transmission lines disconnected at noon, the cascading sequence essentially complete around 4:13 p.m. A shut-down cascade triggered the blackout. Supply/Demand mismatch and poor vegetation management triggered the power surges in transmission lines. FE's operators didn't pay attention to the warning signs, and poorly communicated with other line operators. Finally, the power surges spread and the blackout emerged [Force, 2004].

BP Texas City refinery is the third largest refinery in the United States. The refinery employs approximately 1,800 BP workers. On March 23, 2005, the refinery initiated the startup of the Isomerization Process Unit (ISOM) raffinate splitter section. During the startup, the control valve was turned off by an operator accidentally and so the tower was filled with flammable liquid for over three hours. The pressure relief valve was activated by high pressure in the tower and discharged liquid to the blowdown drum. The blowdown drum overfilled and the stack vented flammable liquid to the atmosphere, which formed a vapor cloud. When the flammable vapor cloud reached an idling diesel pickup truck, whose engine was on, an explosion happened. The explosion and fires occurred at the site killed 15 people, injured 180 others, and resulted in financial losses exceeding $1.5 billion [CSB, 2005].

In the summer of 2007, leading banks in the U.S. started to fail as a result of falling real estate prices. Bear Stearns, the fifth largest investment bank, whose stock had traded at $172 a share as late as January 2007 was sold to JP Morgan Chase for a fire sale price of $2 on March 16, 2008; Lehman Brothers, the fourth largest, went bankrupt; Fannie Mae and Freddie Mac were taken over by government; American International Group (AIG), the

Table 2.5: Agents of each view

View	Agents		
	BP Texas City Refinery Explosion	**Subprime Crisis**	**Northeast Blackout**
Societal View	U.S. citizens	Citizens worldwide	U.S. and Canada citizens
Government View	Employees of different branches of Government	Employees of U.S. and Foreign Governments	Employees of U.S. and Canada Governments
Regulatory View	Employees of OSHA	Employees of FED, SEC, FDIC, OCC, OTC	Employees of NERC and FERC of U.S.; Employees National Energy Board of Canada
Market View	Companies in oil & gas refining industry	Institutions in financial industry	MAAC-ECAR-NPCC power grid
Management View	BP senior management	Senior management of financial institutions & credit rating agencies	Senior management of FE, AEP, MISO, PJM
Plant View	BP Texas City refinery management	Dealers, investors, managers of financial products	Eastlake 5 generation, Harding-Chamberlin line
Equipment View	Engineers and operators, equipment	Borrowers, lenders, brokers, subprime loans	Engineers and operators, equipment

issuance giant, was bailed out by tax payers [Blackburn, 2008]. Over half million families lost their homes to foreclosure. Nearly \$11 trillion household wealth vanished. Between January 2007 and March 2009, stock market lost half its value [Jickling, 2011]. The final cost to the U.S. economy as a result of the biggest financial crisis since Great Depression was about \$*22 trillion*! To get a sense of its magnitude, compare it with the U.S. GDP in 2014 which was \$17.4 trillion.

A cross domain comparison, shown in Figure 2.9, has been conducted by analyzing and comparing failures of these three prominent systemic failures. Figure 2.9 is a table where rows are TeCSMART views and failure classes, and columns are the three systemic failures. Table 2.5 lists agents of the three systemic failures. As discussed before, we classify failure evidences found in the *post mortem* investigation reports as different failure classes, related to specific control components at the appropriate levels. Then we mark the failure class as a colored cell in the table, with a color code that blue represents BP Texas City Refinery Explosion; yellow represents Subprime Crisis; and brown represents Northeast Blackout. If the three colors appear in the same row, it means that particular failure class had occurred in all three cases. Therefore, by comparing the colored cells, we are able to study the failure mechanisms, their similarities and differences. Figure 2.10 highlights failure classes classified in the comparison table (Figure 2.9). Failures were found at every level in all the three cases. Operational failures are more common at low levels; controller failures dominate at high levels. Among the many important observations and insights from the comparison, we highlight a few and discuss them in depth.

		Cross Domain Comparison			
View	Component	Failure	Subprime Crisis	Northeast Blackout	BP Texas City Explosion
Societal View	Sensor	*1.3 Significant errors in monitoring*	■		
		2.5 Conlict of interests	■		
	Controller	*3.1 Flawed actions including supervision*	■		

		Cross Domain Comparison			
View	Component	Failure	Subprime Crisis	Northeast Blackout	BP Texas City Explosion
Regulatory View	Acutator	*2.2 Inadequate or incorrect local decisions*	■		
		2.4.1 Lack of resources			■
		3.1 Flawed actionsincluding supervision	■	■	■
		3.2 Late response	■		
	Sensor	*1.1 Fail to monitor*	■		
	Controller	*1.2 Failure to monitor effectively*	■		
		2.1 Model failures			■
		2.3 Inadequate or incorrect global decisions	■		
		2.4.1 Lack of resources	■		■
		2.4.2 Inadequately allocate resources			■
		2.5 Conflict of interests	■		
		3.1 Flawed actions including supervision	■	■	■
		3.2 Late response	■		■
		5.3 Operating procedure failures	■	■	

		Cross Domain Comparison			
View	Component	Failure	Subprime Crisis	Northeast Blackout	BP Texas City Explosion
Government View	Actuator	*5.3 Operating procedure failures*		■	
	Controller	*3.1 Flawed actions including supervision*	■		
		5.1 Design failures	■		
		5.3 Operating procedure failures		■	

		Cross Domain Comparison			
View	Component	Failure	Subprime Crisis	Northeast Blackout	BP Texas City Explosion
Market View	Controller	*2.1 Model failures*	■		
		2.3 Inadequate or incorrect global decisions		■	
		2.4.1 Lack of resources		■	
		2.4.2 Inadequately allocate resources		■	
		2.5 Conflict of interests	■	■	
		3.1 Flawed actions including supervision	■		
		5.1 Design failures		■	
		5.3 Operating procedure failures	■		
	Communications	*4.2 Peer to Peer communication failure*	■		

		Cross Domain Comparison			
View	Component	Failure	Subprime Crisis	Northeast Blackout	BP Texas City Explosion
Management View	Actuator	*2.3 Inadequate or incorrect global decisions*	■		
		2.5 Conlict of interests	■		■
		3.1 Flawed actions including supervision	■	■	■
	Sensor	*1.1 Fail to monitor*	■	■	■
		1.2 Failure to monitor effectively	■	■	■
		1.3 Significant errors in monitoring	■	■	■
		2.2 Inadequate or incorrect local decisions	■		
		3.1 Flawed actions including supervision	■		
	Controller	*2.1 Model failures*	■		
		2.2 Inadequate or incorrect local decisions	■		■
		2.3 Inadequate or incorrect global decisions	■		
		2.4.1 Lack of resources		■	■
		2.4.3 Training failures			■
		2.5 Conlict of interests	■		■
		3.1 Flawed actions including supervision	■	■	■
		5.1 Design failures		■	■
		5.3 Operating procedure failures	■	■	
	Communications	*4.3 Inter-layer communication failure*		■	■

		Cross Domain Comparison			
View	Component	Failure	Subprime Crisis	Northeast Blackout	BP Texas City Explosion
Plant View	Actuator	*2.2 Inadequate or incorrect local decisions*		■	■
		2.4.3 Training failures			■
		3.1 Flawed actions including supervision		■	■
	Unit Operation	*3.1 Flawed actions including supervision*	■	■	
		5.3 Operating procedure failures	■	■	
	Sensor	*1.1 Failure to monitor*		■	■
		1.2 Failure to monitor effectively		■	
		1.3 Significant errors in monitoring		■	
		5.1 Design failures		■	
	Controller	*1.3 Significant errors in monitoring*			■
		2.1 Model failures		■	
		2.2 Inadequate or incorrect local decisions		■	■
		2.4.1 Lack of resources		■	
		3.1 Flawed actions including supervision	■	■	■
		3.2 Late response		■	■
		5.1 Design failures		■	■
		5.2 Maintenance failures		■	■
		5.3 Operating procedure failures	■	■	■
	Communications	*4.1 External entities communication failure*	■	■	■
		4.3 Inter-layer communication failure		■	■

		Cross Domain Comparison			
View	Component	Failure	Subprime Crisis	Northeast Blackout	BP Texas City Explosion
Equipment View	Actuator	*2.2 Inadequate or incorrect local decisions*		■	■
		2.4.3 Training failures	■	■	■
		2.5 Conflict of interest			■
		3.1 Flawed actions including supervision		■	■
		4.2 Peer to Peer communication failure		■	■
	Unit Operation	*2.4.3 Training failures*	■	■	
		2.5 Conflict of interest	■		
		3.1 Flawed actions including supervision	■	■	■
	Sensor	*1.1 Failure to monitor*		■	■
		3.1 Flawed actions including supervision		■	
	Controller	*2.2 Inadequate or incorrect local decisions*	■		
		2.4.3 Training failures	■	■	■
		3.1 Flawed actions including supervision	■	■	
		5.2 Maintenance failures			■
	Communications	*4.2 Peer to Peer communication failure*		■	■

Figure 2.9: Cross-domain comparison table

TeCSMART Failure Classification

View	Component	Failure
Societal View	Sensor	*1.3 Significant errors in monitoring*
		2.5 Conlict of interests
	Controller	*3.1 Flawed actions including supervision*

TeCSMART Failure Classification

View	Component	Failure
Government View	Actuator	*5.3 Operating procedure failures*
	Controller	*3.1 Flawed actions including supervision*
		5.1 Design failures
		5.3 Operating procedure failures

TeCSMART Failure Classification

View	Component	Failure
Regulatory View	Acutator	*2.2 Inadequate or incorrect local decisions*
		2.4.1 Lack of resources
		3.1 Flawed actionsincluding supervision
		3.2 Late response
	Sensor	*1.1 Fail to monitor*
	Controller	*1.2 Failure to monitor effectively*
		2.1 Model failures
		2.3 Inadequate or incorrect global decisions
		2.4.1 Lack of resources
		2.4.2 Inadequately allocate resources
		2.5 Conflict of interests
		3.1 Flawed actions including supervision
		3.2 Late response
		5.3 Operating procedure failures

TeCSMART Failure Classification

View	Component	Failure
Market View	Controller	*2.1 Model failures*
		2.3 Inadequate or incorrect global decisions
		2.4.1 Lack of resources
		2.4.2 Inadequately allocate resources
		2.5 Conflict of interests
		3.1 Flawed actions including supervision
		5.1 Design failures
		5.3 Operating procedure failures
	Communications	*4.2 Peer to Peer communication failure*

TeCSMART Failure Classification

View	Component	Failure
Management View	Actuator	*2.3 Inadequate or incorrect global decisions*
		2.5 Conlict of interests
		3.1 Flawed actions including supervision
	Sensor	*1.1 Fail to monitor*
		1.2 Failure to monitor effectively
		1.3 Significant errors in monitoring
		2.2 Inadequate or incorrect local decisions
		3.1 Flawed actions including supervision
	Controller	*2.1 Model failures*
		2.2 Inadequate or incorrect local decisions
		2.3 Inadequate or incorrect global decisions
		2.4.1 Lack of resources
		2.4.3 Training failures
		2.5 Conlict of interests
		3.1 Flawed actions including supervision
		5.1 Design failures
		5.3 Operating procedure failures
	Communications	*4.3 Inter-layer communication failure*

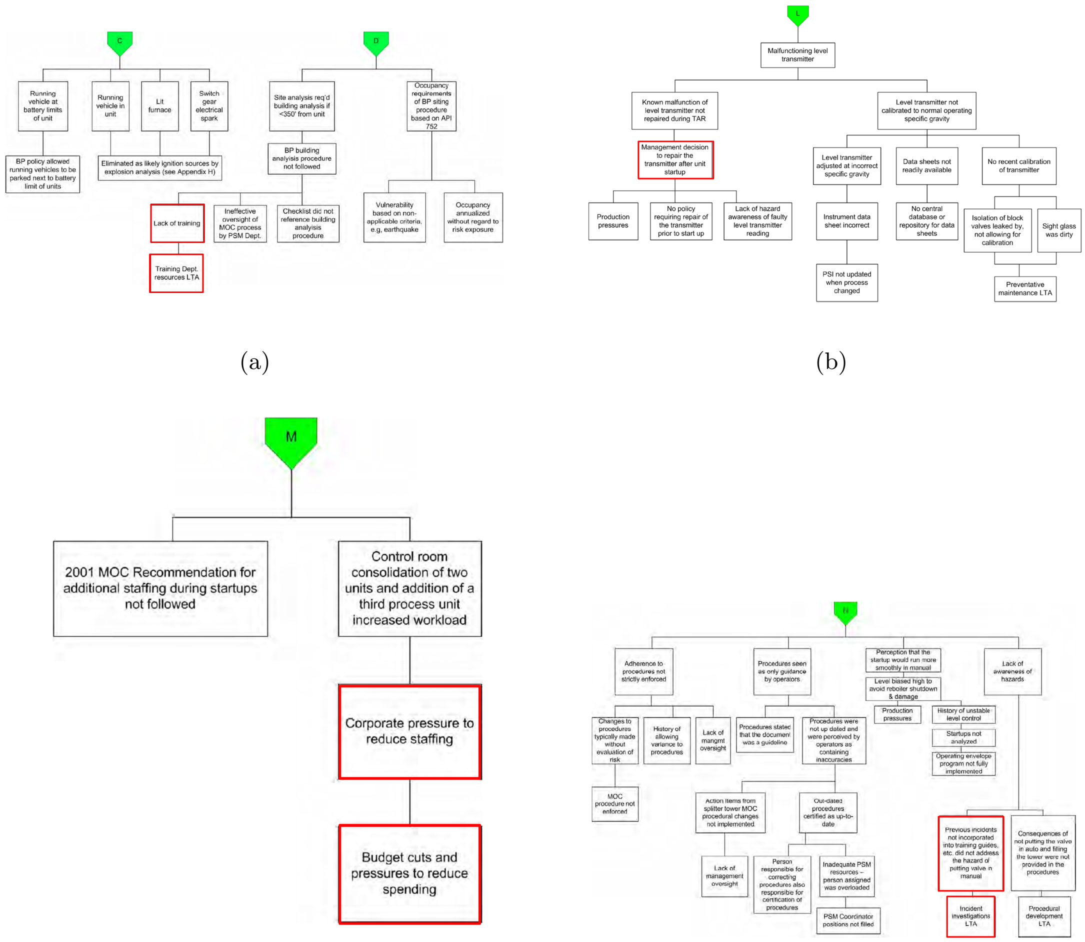
TeCSMART Failure Classification

View	Component	Failure
Plant View	Actuator	*2.2 Inadequate or incorrect local decisions*
		2.4.3 Training failures
		3.1 Flawed actions including supervision
	Unit Operation	*3.1 Flawed actions including supervision*
		5.3 Operating procedure failures
	Sensor	*1.1 Failure to monitor*
		1.2 Failure to monitor effectively
		1.3 Significant errors in monitoring
		5.1 Design failures
	Controller	*1.3 Significant errors in monitoring*
		2.1 Model failures
		2.2 Inadequate or incorrect local decisions
		2.4.1 Lack of resources
		3.1 Flawed actions including supervision
		3.2 Late response
		5.1 Design failures
		5.2 Maintenance failures
		5.3 Operating procedure failures
	Communications	*4.1 External entities communication failure*
		4.3 Inter-layer communication failure

TeCSMART Failure Classification

View	Component	Failure
Equipment View	Actuator	*2.2 Inadequate or incorrect local decisions*
		2.4.3 Training failures
		2.5 Conflict of interest
		3.1 Flawed actions including supervision
		4.2 Peer to Peer communication failure
	Unit Operation	*2.4.3 Training failures*
		2.5 Conflict of interest
		3.1 Flawed actions including supervision
	Sensor	*1.1 Failure to monitor*
		3.1 Flawed actions including supervision
	Controller	*2.2 Inadequate or incorrect local decisions*
		2.4.3 Training failures
		3.1 Flawed actions including supervision
		5.2 Maintenance failures
	Communications	*4.2 Peer to Peer communication failure*

Figure 2.10: Failure modes in the comparison table



(a) (b) (c) (d)

Figure 2.11: The logic tree of BP Texas City Refinery Explosion (adapted from [CSB, 2005])

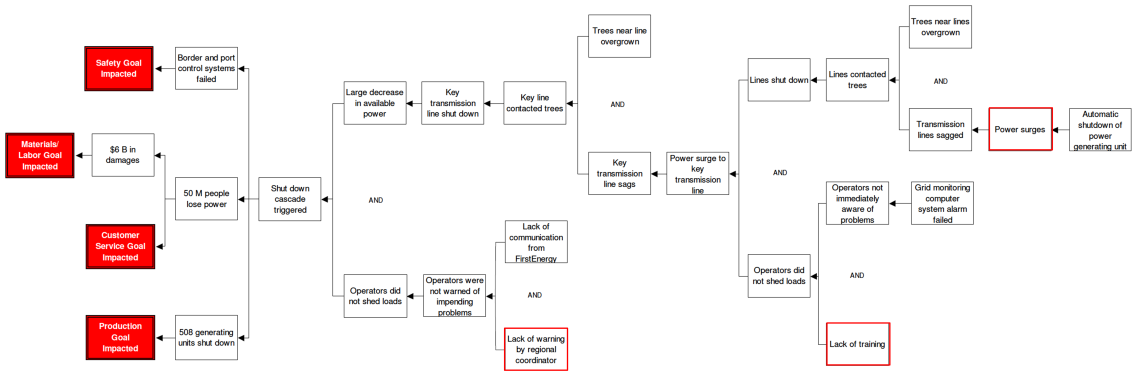


Figure 2.12: The cause map of Northeast Blackout (adapted from [ThinkReliability, 2008])

The comparison shows that lack of appropriate training was a widespread problem. In Figure 2.9, we have seen training failures in the bottom three views of all three cases. Evidence shows that operators, even managers, haven't received appropriate and sufficient training prior to the accidents. The operator training program was inadequate at BP Texas City Refinery. The training department staff had been reduced from 28 to 8; there were no simulators for operators to practice handling abnormal events [CSB, 2005]. the training failure of BP is confirmed by the logic tree created by the Chemical Safety and Hazard Investigation Board (CSB), highlighted in Figure 2.11(a). Similar things happened in the Northeast Blackout. FE operators were poorly trained to recognize emergency information. They received signals indicating line trips, but made poor decisions by relying solely on the Emergency Management System (EMS). Unfortunately, EMS failed at this time. FE engineers' poor judgment and lack of training played a significant role in the failure. Their lack of training was also highlighted by ThinkReliability in their causal map, depicted in Figure 2.12. Such a pattern was also seen in the financial system failure [Commission, 2011; Schumer and Maloney, 2007].

Decision-makers are "controllers" in the TeCSMART framework. In all three cases, almost every layer has shown decision-making failures. For example, the decision of initializing the ISOM despite previously reported malfunctions of the raffinate tower level indicator, pressure control valve, and level sight glass, was a serious failure, which directly triggered the overall disaster [CSB, 2005]. Moreover, BP's cost-cutting decisions that led to the layoff of experienced workers from Amoco contributed to the accident as well [Baker *et al.*, 2007].

These failures are highlighted by CSB in Figure 2.11(b) and Figure 2.11(c). In Subprime Crisis, fund managers' decision to invest in subprime securities without fully understanding the embedded risks was an important cause of the financial system to collapse [Commission, 2011]. FE's decision of using minimum acceptable normal voltages (highlighted in Figure 2.12), which are lower than and incompatible with those of its neighbors, directly caused power surges and transmission lines sag [Force, 2004]. At the management level, demonstrated by both our comparison study and the CSB analysis (Figure 2.11(a) and Figure 2.11(c)), a critical failure was BP not providing enough resources for strong process safety performance in its U.S. refineries [CSB, 2005]. At the same level, CEOs of financial institutions decided to maintain a large quantity of subprime related assets by using a very high leverage. The high leverage magnified the scale of the crisis dramatically. Moreover, sometimes a locally favorable decision may bring undesired consequences to the system. In the North America Power Grid, the pre-protection point that protects single operators won't work for the whole system. When single operators dropped out from the grid, the pressure was all on the other part of the system. Finally the system had no options but to fail systemically [Force, 2004].

Monitoring problems often play a major role in sociotechnical disasters. Monitoring failures were observed at the management level in all three cases. As discussed in the preceding section and in Table 2.1, a sensor or a monitoring task can fail low, high, zero, or fail to detect in time. BP was not aware of hazards at Texas City Refinery, because BP failed to incorporate previous incidents; even worse, the incidents investigations were missing [Baker *et al.*, 2007] ("failing zero"). The monitoring failure of BP is particularly mentioned by CSB in Figure 2.11(d). On the other hand, prior to the Subprime Crisis, Moody's did not account for the deterioration in underwriting standards and was not aware of the plummeting home prices. Moody's did not develop a model specifically to look into layered risks of subprime securities, after it had rated nearly 19,000 subprime securities [Commission, 2011] ("failing zero"). Deregulation and self-policing by financial institutions had stripped away key safeguards [Commission, 2011] ("failing low"). Moreover, in Northeast Blackout, the Midcontinent Independent System Operator, Inc. (MISO) failed to recognize the consequence of Hanna-Juniper line loss, while other operators recognized the overload but had not expected it because the contingency analysis earlier did not examine enough lines to foresee the Hanna-Juniper contingency. The failure of not recognizing the line loss in a timely manner worsened the situation. When the operators finally figured out the situation, it was too late to respond [Force, 2004] ("failing to detect in time"). MISO's monitoring failure not only was highlighted by ThinkReliability (in Figure 2.12) as lack of warning, but also raised concerns of U.S.–Canada Power System Outage Task Force. The Task Force report [Force, 2004] recommends FERC should not approve the operation of a new Regional Transmission Operator (RTO) or Independent System Operator (ISO) until the applicant has met the minimum functional requirements for reliability coordinators. This recommendation directly addressed the issue of MISO's, as a reliability coordinator, failing to recognize line loss in its region.

Beyond the decision-making or monitoring failures, the flawed actions of regulators and their limited oversight always contribute to sociotechnical system collapses. The reports [Baker *et al.*, 2007; CSB, 2005] mention that OSHA did not conduct a comprehensive inspection of any of the 29 process units at the Texas City Refinery. Knowing the high leverage and vast sums of subprime loans, the FED did not begin routinely examining subprime subsidiaries until a pilot program in July 2007. FED even did not issue new rules until July 2008, a year after the subprime market had shut down [Commission, 2011]. North American Electric Reliability Corporation (NERC), the power grid self-regulator, knowing FE's potential risk, did not enforce any changes or regulate FE's activities [Force, 2004]. All these flawed actions contributed to the disasters. Regulators also experience conflict of interest. Especially financial regulators, who face challenges from powerful financial institutions.

These observations are just a few examples of what we studied in the TeCSMART comparison. Comparing with the logic tree and the causal map, TeCSMART comparison is able to capture high-level failures such as regulatory failures, which are not covered in the logic tree or causal map. More importantly, TeCSMART comparison can systematically identify potential risks in a sociotechnical system by identifying possible failure modes associated with different components at different levels.

2.5 Chapter Conclusions

Analyzing systemic risk in a complex sociotechnical system requires modeling the system at multiple levels, at multiple perspectives, using a systematic and unified framework. It is not enough to focus only on equipment failures. It is important to systematically examine the potential failures associated with humans and institutions at all levels in a society. We have proposed the TeCSMART framework, which models sociotechnical systems in seven layers using control-theoretic concepts. Using this framework, a HAZOP-like hazards identification can be conducted for every layer of a sociotechnical system. The failure modes identified using TeCSMART framework, at all levels, serve as a common platform to compare systemic failures from different domains to elicit and understand common failure mechanisms which can help with improved design and risk management in the future. They also serve as the input information for developing other types of models (e.g., DAE, SDG, ontological, agent-based) for more detailed studies.

We carried out such a comparative analysis of 12 major systemic events from different domains, analyzing over 700 failures discussed in official *post mortem* reports. Even though we are only highlighting the results from three of them, for the sake of brevity, the common failure patterns we identify were found in the other events as well. The over 700 failures can be systematically classified into the five categories (and their subcategories) that can occur at all levels of the system. Using a unifying control-theoretic framework, we show how these correspond to common failure modes associated with the elements of a control system, namely, sensor, controller, actuator, process unit, and communication channels. Even though every systemic failure happens in some unique manner, and is not an exact replica of a past event, we show that the underlying failure mechanism can be traced back to similar patterns associated with other events.

Chapter 3

Process Systems Engineering as a Modeling Paradigm for Analyzing Systemic Risk in Financial Networks

There is nothing stable in the world;
uproar's your only music.

John Keats

In Chapter 2, we have shown that multiple levels of a sociotechnical system can be modeled by TeCSMART framework (Figure 2.1). For example, equipment and processes at the equipment layer are modeled by DAE models. However, at the higher layers, such as the plant, management, and market layers, where DAE knowledge is not easy to develop, other types of knowledge can be modeled.

In this chapter, we introduce SDG to capture system's cause-and-effect knowledge. Specifically, we develop a SDG model for the market layer of a financial system. Financial system is a typical sociotechnical system where interactions among financial entities are very complex and cannot be explained by DAE models. We model its cause-and-effect knowledge to investigate the interactions among a financial system, hence, understand its systemic risk.

3.1 Financial Systems and its Instability

Modern financial systems are constantly adapting and changing. Financial systems are characterized by a very complex set of interdependencies among a large number of institutions. Stress to one part of the system can spread to others, often threatening the stability of the entire financial system. The recent financial crisis that was precipitated by counterparty exposures revealed by the Lehman bankruptcy, the near bankruptcy of AIG, and the European debt crisis that was caused by the exposure of European banks to sovereign default risk emphasizes the critical need for a fundamental understanding of the structure and dynamics of this system. In the aftermath of the 2008 crisis, regulators have come to recognize that interconnectedness can pose substantial threats to the stability of the financial system.

Financial instability typically results from *positive feedback loops* that are intrinsic to the operation of the financial system, that is, the instability results from responses to shocks that reinforce and amplify the initial shock. The structures and mechanisms that create these positive feedbacks must, therefore, be the focus of any analysis of financial stability, and new tools are needed to identify and model these structures and mechanisms.

Furthermore, financial systems have the particular feature that the steps taken by a single agent to mitigate its risk, under extreme circumstances, can become the very source of destabilizing positive feedback through the interaction of multiple agents. We refer to these steps as *locally* stabilizing yet *globally* destabilizing. This phenomenon is illustrated by the phenomenon of the bank run. Suppose a bank is weakened by losses, the prudent action for each individual depositor is to withdraw funds; yet this very response will drive the bank to failure if followed by every depositor [Diamond and Dybvig, 1983]. The longer the line of customers outside grows, the greater the incentive for more customers to join the line and the stronger the amplifying feedback.

The problem of traditional bank runs was largely solved through deposit insurance, which effectively eliminates any reason for depositors to react to news about a bank. Yet similar dynamics operate throughout the financial system. For example, a bank-dealer facing a shortfall in funding might reduce the lending it provides to hedge funds, and to control their risk the hedge funds might respond by liquidating positions. But this circuit of actions, reasonable and prudent for each of the two sectors, can lead to global instability: the resulting decline in prices reduces the value of collateral, reducing the cash provided to the bank-dealer on one hand, and leading to further margin calls and demand for forced liquidation by the hedge funds on the other.

Examples of these patterns have been identified as fire sale dynamics [Shleifer and Vishny, 2011], liquidity spirals [Brunnermeier and Pedersen, 2009], leverage cycles [Adrian and Shin, 2014; Fostel and Geanakoplos, 2008], and panics [Gorton, 2010]. But to understand these critical aspects of the financial system comprehensively, we need a systematic way to identify the paths of feedback globally, wherever they may arise. In order to do so, one must understand the conduits for the transmission of information and the control mechanisms applied by the various financial entities based on their observations of flows and the financial environment. A further complicating fact is that the nature of this feedback is scale dependent. For example, a small change in prices, funding, or a bank's financial condition might be absorbed by the system, whereas a large shock might trigger a destabilizing cascade.

In engineering systems, the safety and stability of an assembled system is a design criterion. In contrast, the financial system is self-organized. Individual financial entities generally have risk-management procedures and controls to preserve their own stability, but the system as a whole was never engineered for safety and stability. Because of this, it is all the more critical to understand the paths of positive and negative feedback, alternative routes for funding, and securities flows in the event of a shock to one node or edge of the network, and more generally how the interactions of the system can create vulnerabilities and instability.

This chapter shows how the SDG framework makes this possible through a systemwide view of transformations and dynamical interactions in the financial system. With an SDG representation, it becomes possible to automate the systematic identification and monitoring of vulnerabilities. In particular, this approach contributes to the critical task of systemic financial risk management: it can highlight and help us monitor dynamics such as fire sales and funding runs where actions that are locally stabilizing might cascade to be globally destabilizing.

3.2 Financial Network as a Process Plant: Systems Engineering Framework

An appropriate process systems engineering analogy is to view each financial entity as a production or manufacturing plant, for example, a chemical process plant, that takes securities and funding as inputs and creates new financial products as outputs that are delivered to other processing units. This analogy opens the possibility of using tools that are applied in engineering for network analysis to gain a better understanding of the dynamic process underlying the financial system. Though researchers have suggested the Internet, electrical power grid, and transportation network as potential models for the financial system, none of these has the richness of phenomena seen in a large-scale chemical process plant. We demonstrate in this chapter that phenomena such as various physical or chemical transformations, feedback and recycle loops, and so on can serve as relevant and useful analogies for modeling the financial system. In the existing network-based models, risk travels along edges; however, these models ignore the financial transformations executed within the nodes that generate and compound risk. Although flows and connections are important, the picture of risk creation and contagion is incomplete without understanding the production process.

In order to gain further insight into the underlying dynamics, one needs a richer, more detailed, modeling framework [Venkatasubramanian *et al.*, 2000; Venkatasubramanian, 2009]. This is carried out in process systems engineering at three levels of increasing sophistication and effort: (1) qualitative causal models, such as SDGs, capture the underlying cause-and-effect relationships, (2) quantitative steady-state models, represented as a system of algebraic equations, capture the steady-state behavior of the process, and (3) quantitative dynamic models, generally represented as a system of Ordinary Differential Equations (ODEs) and Partial Differential Equations (PDEs), predict the transient behavior of the process. The particular choice for the model depends on the need. For instance, for performing PHA, where one systematically identifies the potential hazards, their causes, and adverse consequences, it is often adequate to use the qualitative causal SDG models. On the other hand, for making process control decisions, one requires a detailed dynamic model that is derived from first principles (as ODEs or PDEs) or from a data-driven perspective as an input-output model. Generally speaking, in many industrial settings, given the complexity of the underlying process, it is often quite difficult or expensive to develop the quantitative dynamic models, particularly from first principles.

Network models, in this case, are more applicable. Financial systems emphasize the activities at the Management View (Chapter 2.2.3) and the Market View (Chapter 2.2.4), where DAE models are difficult to derive. Network models typically describe payment obligations and flows, and they can be effective in quantifying the degree and complexity of the connections among the financial entities. Standard network models represent financial entities as nodes and the flows between them as edges; research questions in this area focus on which types of networks provide robust structures for the financial system [Kleindorfer and Wind, 2009; Battiston *et al.*, 2013; Gai and Kapadia, 2010]. But these models lack a representation for the flow of information and responses to information; they do not provide a vehicle for understanding how responses and controls of multiple agents interact or the inner workings of an institution summarized by a single node. They only capture the Market View. Modeling financial institutions as black boxes fails to illustrate the "locally stable but globally unstable" effect.

Therefore, we introduce SDG as a tool for understanding the feedback effects in financial systems. SDGs are extensively used in process systems engineering. An SDG representation captures the information transmission, the environmental state, and the causal relationships that underlie feedback. It encodes the control rules and responses followed by individual units within a financial system and provides a framework for systematically investigating the resulting interactions between these units. In particular, the SDG representation can be used to identify cycles of positive feedback that may not be immediately apparent. Moreover, subjecting SDG to a PHA [Venkatasubramanian *et al.*, 2000; Venkatasubramanian, 2011] pinpoints areas of potential stress and instability in a system-

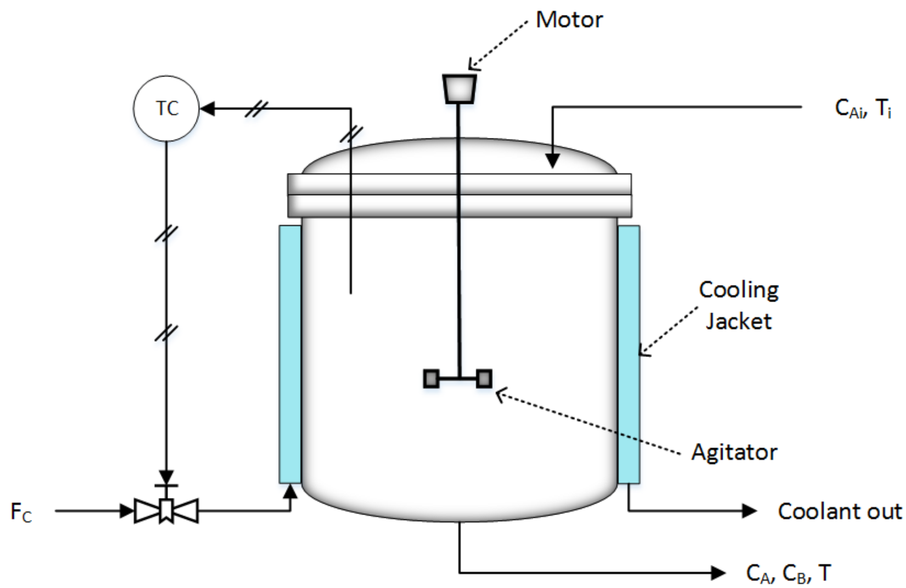


Figure 3.1: CSTR Example (Adapted from [Stephanopoulos, 1984], fig. 23.5c)

atic manner. The SDG framework is able to represent and reveal information missed by more traditional network models of financial interconnections.

We now illustrate the SDG framework with the aid of a simple process engineering example, a Continuous Stirred-Tank Reactor (CSTR) process (see Figure 3.1 and Stephanopoulos [Stephanopoulos, 1984]) where an exothermic (that is, heat generating) reaction, A→B, takes place. The heat generated by the reaction is removed by passing a coolant through the jacket of the reactor (shaded), thereby controlling the temperature T inside the reactor. If the temperature is not controlled, it could lead to a runaway reaction and explosion. The temperature is controlled by a feedback control loop that manipulates the coolant flow rate F_c to achieve the desired set point temperature.

We next build an SDG model for the CSTR process. A digraph is a graph with directed arcs between the nodes, and a SDG is a graph in which the directed arcs have a positive (shown as solid lines) or negative sign (shown as dotted lines) attached to them. The nodes represent events or variables and edges relationship between the nodes. The directed arcs lead from the cause nodes to effect nodes, showing the direction of causality. In the typical use of SDG models, each node corresponds to a deviation from the steady-state value of a variable. SDG models are much more compact than truth tables, decision tables, or finite state models, and are, therefore, quite efficient in capturing the causes and effects represented in a process or equipment. The qualitative SDG models are easier to develop and analyze, in comparison to the dynamic models, and can yield quick and useful results in certain decision-making tasks such as process fault diagnosis and process hazards analysis [Maurya *et al.*, 2003a; Maurya *et al.*, 2003b; Maurya *et al.*, 2004; Vaidhyanathan and Venkatasubramanian, 1996; Venkatasubramanian and Vaidhyanathan, 1994; Venkatasubramanian *et al.*, 2000; Viswanathan *et al.*, 1998a; Viswanathan *et al.*, 1998b; Zhao *et al.*, 2005a; Zhao *et al.*, 2005b]. Even when a dynamic model is available, it is generally faster and more efficient to use an SDG model to perform cause-and-effect reasoning for such applications. However, since SDG models are qualitative in nature, they can lead to ambiguities and hence are limited to certain kinds of tasks [Venkatasubramanian and Rengaswamy, 2003; Venkatasubramanian *et al.*, 2003a; Venkatasubramanian *et al.*, 2003b].

The SDG model for the CSTR example is shown in Figure 3.2. The figure is read as follows: a change in the inlet concentration of A, C_{Ai} positively affects the concentration of A inside the reactor, C_A; that is, if C_{Ai} increases, C_A will increase, and if C_{Ai} decreases, C_A will decrease. This is shown by the solid edge between these two nodes. And if C_A increases, then the reaction rate r will increase, which is shown by the solid edge between these two nodes. However, an increase in the reaction rate will increase the conversion of A$\rightarrow$B, thereby reducing the concentration of A (a negative feedback here). This is captured by the negative edge in dotted line between r and C_A. An increase in the reaction rate r results an increase in T, which in turn causes an increase in r, potentially leading to a runaway reaction if the coolant flow fails to control this. The rest of the SDG is to be interpreted by following the direction of causality, as shown earlier. Maurya *et al.* [Maurya *et al.*, 2003a; Maurya *et al.*, 2003b; Maurya *et al.*, 2004] discuss how the SDG model can be derived systematically from the underlying equations of the process or from a detailed causal understanding of the process.

Although the SDG model of the entire process unit network (that is, flowsheet) for an industrial process is naturally more complicated, with hundreds of nodes and edges, it can

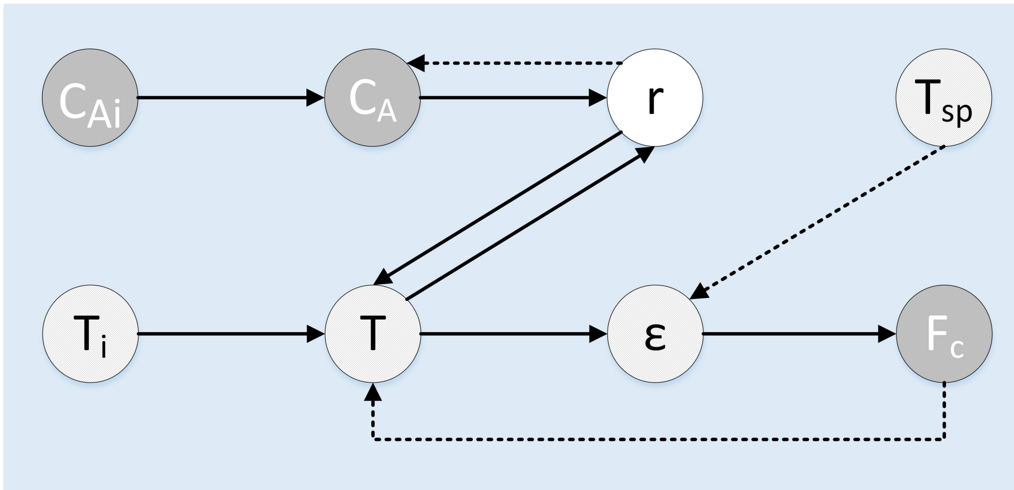


Figure 3.2: SDG for the CSTR example (exothermic reaction A→B)

be assembled from a library of unitwise SDG models, as discussed by Maurya *et al.* [Maurya *et al.*, 2003a; Maurya *et al.*, 2003b; Maurya *et al.*, 2004]. Venkatasubramanian and coworkers have also developed artificial intelligence-based systems that automate much of the cause-and-effect reasoning (both diagnostic and prognostic) using SDG models for entire flowsheets with recycle and control loops [Maurya *et al.*, 2003a; Maurya *et al.*, 2003b; Maurya *et al.*, 2004; Vaidhyanathan and Venkatasubramanian, 1996; Venkatasubramanian and Vaidhyanathan, 1994; Venkatasubramanian *et al.*, 2000; Viswanathan *et al.*, 1998a; Viswanathan *et al.*, 1998b] for process fault diagnosis and process hazards analysis applications. These methods can be adapted for developing a process systems engineering framework for modeling and analyzing risk in financial networks. We can develop automated systems that can identify the potential hazards lurking in a complex financial network by systematically examining various *what if* failure scenarios.

3.3 SDG Modeling Framework for Financial Networks

We now explain how SDG models can be used to analyze the dynamics of financial systems. A bank-dealer acts as an intermediary between buyers and sellers of securities, and between lenders and borrowers of funding. Its clients are investors, such as asset management firms, hedge funds, and pension funds, as well as other bank-dealers. There are specific business

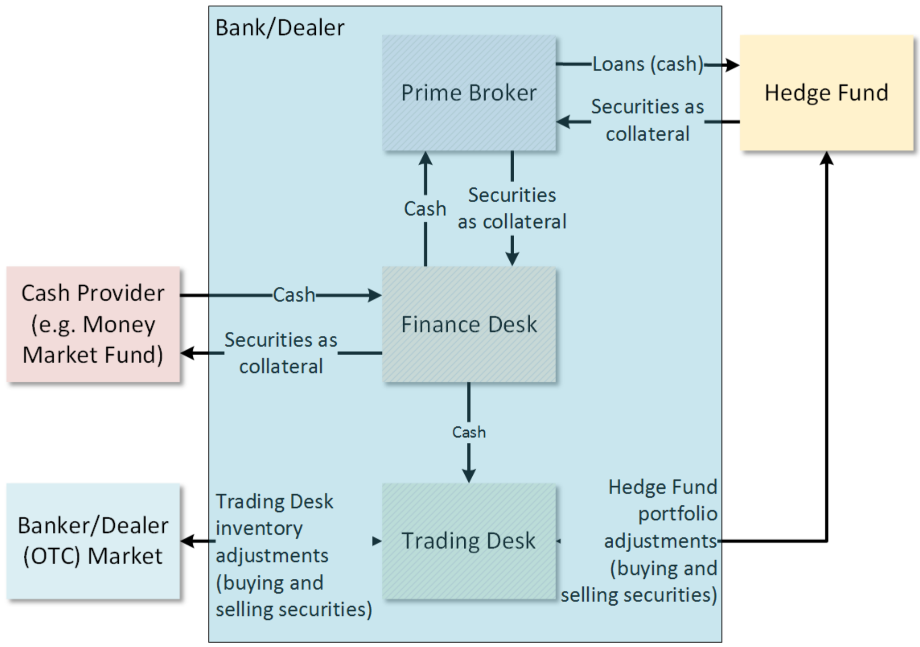


Figure 3.3: Simplified bank-dealer network

units within the bank-dealer that process funding and securities to create products for these clients. The bank-dealer's network, with its connections with other financial entities and among its business units, is complex. For the sake of simplicity, to demonstrate the process systems engineering inspired modeling framework, we now consider a simplified version of the reality and focus only on two types of bank-dealer activities shown in Figure 3.3:

1. Funding and securities lending: The bank-dealer goes to sources of funding such as money market funds through the repo market, and to security lenders, such as pension funds and asset-management firms through their custodian banks.

2. Providing liquidity as a market maker: The bank-dealer goes to the asset markets, to institutions that hold assets, and to other market makers to acquire positions in the securities that the clients demand. This function also includes securitization taking securities and restructuring them. This involves liquidity and risk transformations.

The functions we show within the bank-dealer include the prime broker, which lends cash to hedge funds in order for the hedge funds to buy securities on margin; the finance desk, which borrows cash with high-quality securities used as collateral; and the trading desk, which manages inventory in its market-making activities that it finances through the finance desk. The bank-dealer interacts with cash providers, such as money market funds, pension funds, and insurance companies; other bank-dealer through the over-the-counter market, which is the market for the bank-dealer to acquire or lay off inventory; and the hedge funds, which, as noted earlier, seek leverage and securities from prime brokers to support their long/short trading positions. The hedge funds also represent the wider swath of institutional customers that use the bank-dealer's market-making function, ranging from asset managers and hedge funds to pension funds, sovereign wealth funds, and insurance companies.

The interactions between the bank-dealer's functional areas create various financial transformations. The finance desk takes short-term loans from the cash providers and passes them through to clients that have lower credit standing, often as longer-term loans. In doing this, the bank-dealer is engaging in both a maturity and a credit transformation. The trading desk inventories securities until it can either lay them off based on the demand of another client or to the over-the-counter market. In doing this, it provides a liquidity transformation.

The network for the bank-dealer is more interconnected than that of a chemical plant, because some clients, that is, nodes that receive the output from a bank-dealer, are also sources of inputs. A hedge fund that is borrowing in order to buy securities might also be lending other securities. A pension fund that is providing funding might also be using the bank-dealer for market making. Hedge funds and related institutional investors are on both sides of the production in that they are both buyers and sellers of securities, and in that sense provide inputs as well as output in market making.

3.4 Bank-Dealer Case Study

The network depicted in Figure 3.3, though illustrative of the layout of the components of the bank-dealer and its interactions, does not represent the effect of the various flows, and therefore cannot by itself suggest conditions and areas where a disruption will create instability through positive feedback cycles. To achieve this, we need a cause-and-effect

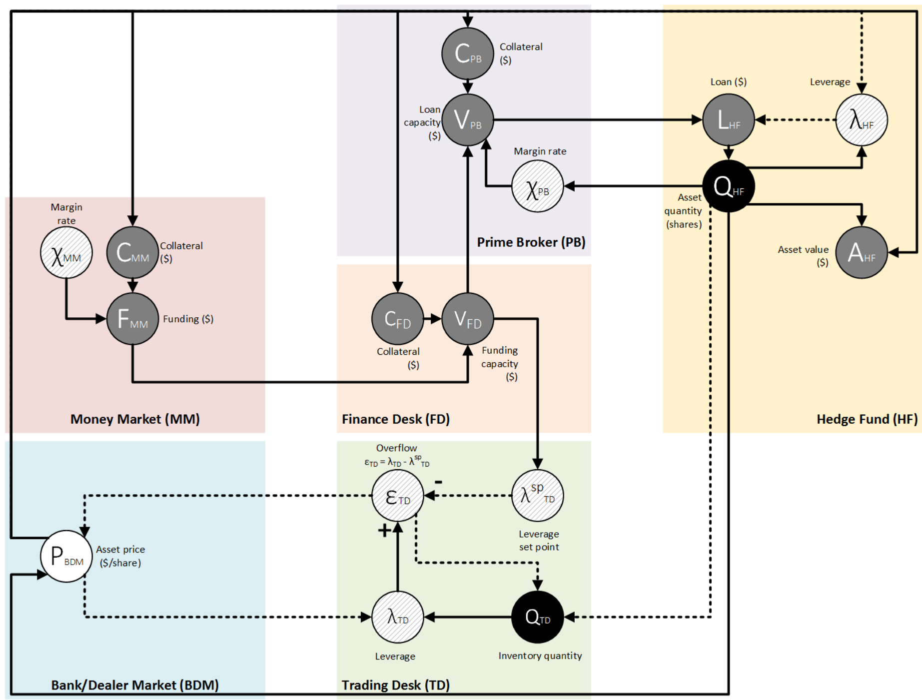


Figure 3.4: SDG model for bank-dealer example

representation of this network, as we did in the chemical processing example of the previous section. We accomplish this by creating the SDG model for this network that is displayed in Figure 3.4.

For simplicity, we consider a system with a single market asset (for example, a stock or a bond). Its price is represented by the node P_{BDM}, and this price level influences and is influenced by the rest of the system. Quantities of the asset Q_{HF} and Q_{TD} are held by the hedge fund and trading desk, respectively. These units need funding to finance their asset holdings; this funding is provided by the money market, the prime broker, and the finance desk. In each case, funding availability depends on the units collateral level, and collateral is held in the form of the market asset. Thus, changes in the market price change the value of the collateral, which in turn changes the level of funding available. A margin rate controls the ratio of funding capacity to collateral at the money market and the prime broker; a leverage target controls the level of borrowing relative to asset holdings at the hedge fund and the trading desk. More specifically, the hedge fund determines its dollar borrowing based on the availability of loans that are provided through the prime broker and a comparison of its assets to its target leverage ratio, λ_{HF}. The prime broker's lending is determined by the bank-dealer's finance desk and by the prime brokers margin rate, χ_{PB}.

The trading desk provides a market-making function; it stands ready to take on any quantity sent its way by the hedge fund. This increases its inventory of shares, and when this inventory becomes too large relative to a set point, it opens the overflow control to pass shares through to the market, dropping the price as a result. The trading desk's market-making function distinguishes its control mechanism from that of the hedge fund. As with the hedge fund, the trading desk depends on the finance desk to fund its inventory, and a drop in funding might force the trading desk to release more shares into the bank-dealer market.

The money market provides funding for both the hedge fund and the trading desk through the finance desk, and it is changes in the funding of the funding desk that lead to changes in the quantity held by the hedge fund and the trading unit, ultimately changing the price. The entire system is driven by, and feeds back into, the prices that are set in the bank-dealer market. These prices are determined by the actions of the trading desk and the hedge fund and determine the collateral value that helps drive the willingness of the various agents along the path to provide funding.

The SDG model clearly illustrates why the financial system becomes embroiled in one crisis after another: nearly all of the pathways extending from the money market through the bank-dealers to the hedge funds are positive. Thus a shock to one node may create a positive feedback, exacerbating the shock. This can be seen by applying the SDG framework and its associated process hazard analysis methodology to the two most common sources of a financial crisis: funding runs and fire sales.

Process Hazards Analysis (PHA) [Venkatasubramanian *et al.*, 2000; Venkatasubramanian, 2011; Zhao *et al.*, 2005a; Zhao *et al.*, 2005b] is a methodology for systematically identifying abnormal causes and adverse consequences that can occur anywhere in the process system. In the context of an SDG model, PHA provides the framework that can guide us in identifying methodically what can go wrong at each node and edge and how that failure would propagate through the rest of the system. Using this framework, we can identify and examine the complete list of loops in an SDG model. This list can be computed via a depth-first search of the SDG [Russell *et al.*, 1995]. Not all positive loops are necessarily significant sources of vulnerability, because the edges of the SDG record the direction of influence but not its magnitude. An individual node is typically subject to multiple competing effects, so the net effect ultimately depends on the gain associated with each feedback loop. Nevertheless, the list of loops provides a valuable tool for identifying vulnerabilities; indeed, we know of no other systematic approach to this problem.

Table 3.1 gives a complete list of loops for the SDG model of the bank-dealer network, with each row describing a loop. A positive (negative) loop is one in which the product of the signs along the edges defining the loop is positive (negative). Only the last two loops in the table are negative, and these have a simple interpretation: they are the internal risk-management processes of the hedge fund and the trading desk, respectively. Each of these units uses a leverage target as an internal control for the quantity held of the market asset. However, when we combine these stabilizing negative feedback loops with the rest of financial system, we get a range of potentially destabilizing positive feedback loops through the interactions across units. We will examine two types of positive loops in greater detail, because these represent fire sales and funding runs, two key examples of crisis dynamics. We emphasize that these dynamics are discovered automatically by the SDG analysis, which highlights the value of this approach.

3.4.1 Fire Sales

Figure 3.5 shows a segment of the SDG model of Figure 3.4 that focuses on the interaction of the hedge fund with the bank-dealer's prime broker. The fire sale occurs when there is a disruption to the system that forces a hedge fund to sell positions. As shown in Figure 3.5, this disruption can occur through three channels: a price drop and resulting drop in asset value, an increase in the margin rate that leads to a margin call from the prime broker, or a drop in the loan capacity of the prime broker. As the hedge fund reduces its assets, prices drop, again leading to a second (and subsequent) round of feedback making the situation worse in every subsequent iteration.

The fire sale is best depicted by the two loops listed in Table 3.2. Loop 8 shows a price shock increasing the leverage of the hedge fund. The hedge fund then reduces its holdings

Table 3.1: List of loops

Index	**Sign**	**Loop**
01	+	$[P_{\mathrm{BDM}}, C_{\mathrm{MM}}, F_{\mathrm{MM}}, V_{\mathrm{FD}}, V_{\mathrm{PB}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, Q_{\mathrm{TD}}, \lambda_{\mathrm{TD}}, \epsilon_{\mathrm{TD}}, P_{\mathrm{BDM}}]$
02	+	$[P_{\mathrm{BDM}}, C_{\mathrm{MM}}, F_{\mathrm{MM}}, V_{\mathrm{FD}}, V_{\mathrm{PB}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, P_{\mathrm{BDM}}]$
03	+	$[P_{\mathrm{BDM}}, C_{\mathrm{FD}}, V_{\mathrm{FD}}, V_{\mathrm{PB}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, Q_{\mathrm{TD}}, \lambda_{\mathrm{TD}}, \epsilon_{\mathrm{TD}}, P_{\mathrm{BDM}}]$
04	+	$[P_{\mathrm{BDM}}, C_{\mathrm{FD}}, V_{\mathrm{FD}}, V_{\mathrm{PB}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, P_{\mathrm{BDM}}]$
05	+	$[P_{\mathrm{BDM}}, C_{\mathrm{PB}}, V_{\mathrm{PB}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, Q_{\mathrm{TD}}, \lambda_{\mathrm{TD}}, \epsilon_{\mathrm{TD}}, P_{\mathrm{BDM}}]$
06	+	$[P_{\mathrm{BDM}}, C_{\mathrm{PB}}, V_{\mathrm{PB}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, P_{\mathrm{BDM}}]$
07	+	$[P_{\mathrm{BDM}}, \lambda_{\mathrm{HF}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, Q_{\mathrm{TD}}, \lambda_{\mathrm{TD}}, \epsilon_{\mathrm{TD}}, P_{\mathrm{BDM}}]$
08	+	$[P_{\mathrm{BDM}}, \lambda_{\mathrm{HF}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, P_{\mathrm{BDM}}]$
09	+	$[P_{\mathrm{BDM}}, C_{\mathrm{MM}}, F_{\mathrm{MM}}, V_{\mathrm{FD}}, \lambda^{sp}_{\mathrm{TD}}, \epsilon_{\mathrm{TD}}, P_{\mathrm{BDM}}]$
10	+	$[P_{\mathrm{BDM}}, C_{\mathrm{FD}}, V_{\mathrm{FD}}, \lambda^{sp}_{\mathrm{TD}}, \epsilon_{\mathrm{TD}}, P_{\mathrm{BDM}}]$
11	+	$[\chi_{\mathrm{PB}}, V_{\mathrm{PB}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, \chi_{\mathrm{PB}}]$
12	+	$[P_{\mathrm{BDM}}, \lambda_{\mathrm{TD}}, \epsilon_{\mathrm{TD}}, P_{\mathrm{BDM}}]$
13	-	$[\lambda_{\mathrm{HF}}, L_{\mathrm{HF}}, Q_{\mathrm{HF}}, \lambda_{\mathrm{HF}}]$
14	-	$[\epsilon_{\mathrm{TD}}, Q_{\mathrm{TD}}, \lambda_{\mathrm{TD}}, \epsilon_{\mathrm{TD}}]$

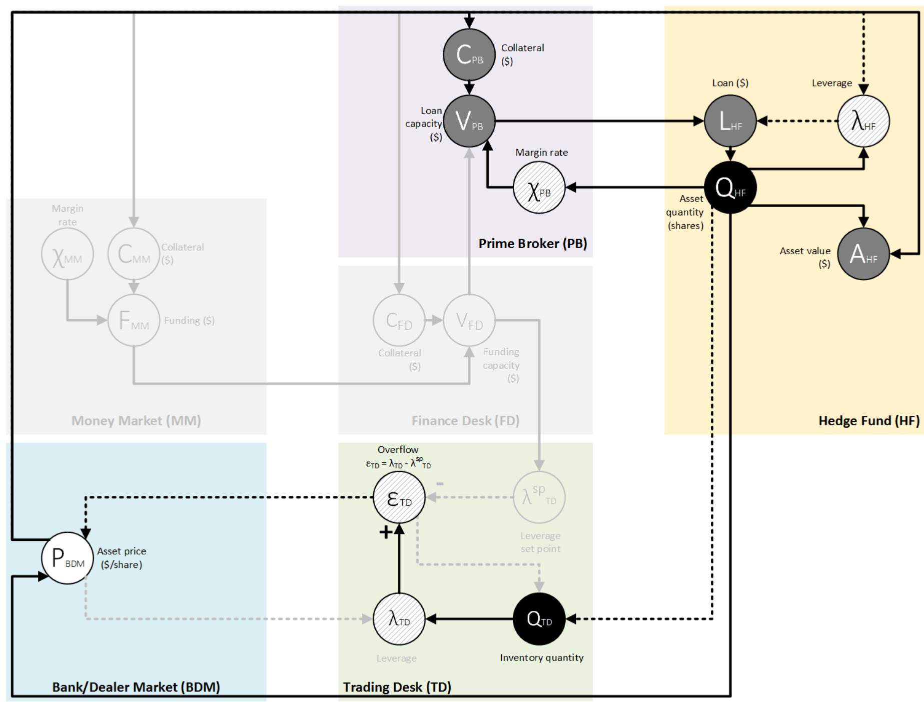


Figure 3.5: SDG model for bank-dealer fire sale example

in order to reduce its leverage, and this drops prices. Loop 7 has the same effect, a drop in prices increases leverage, which in turn leads to a drop in the quantity held by the hedge fund, but the effect in this case works its way through the trading desk. The quantity sold by the hedge fund raises the quantity held by the trading desk, increasing its λ_{TD}. This in turn leads the trading unit to sell into the market, with the end result again being a further drop in prices.

Note that each of the units is acting to maintain stability: the prime broker is keeping its loans within bounds given its collateral, the hedge fund is maintaining a target level of leverage to control its risk, and the trading desk is governing its inventory level through an outflow if its market-making activities increases its inventory above a target level. Yet the stabilizing activities at the local level still lead to instability at the global level. This underscores a central point in the functioning of the financial system, namely, that it can exhibit global instability even in the face of each unit acting to control its risk.

Table 3.2: Fire sale loops

Index	**Sign**	**Loop**
07	+	$[P_{\text{BDM}}, \lambda_{\text{HF}}, L_{\text{HF}}, Q_{\text{HF}}, Q_{\text{TD}}, \lambda_{\text{TD}}, \epsilon_{\text{TD}}, P_{\text{BDM}}]$
08	+	$[P_{\text{BDM}}, \lambda_{\text{HF}}, L_{\text{HF}}, Q_{\text{HF}}, P_{\text{BDM}}]$

3.4.2 Funding Runs

Figure 3.6 shows another segment of Figure 3.4, focusing on the interaction of the bank-dealer with the money market. A funding run can be triggered by a disruption in funding flows from the money market. This may happen if there is an increased uncertainty about the quality of the collateral, or a drop in the market value of collateral, or by a change in the money market's margin rate, which might occur due to an erosion of confidence. The drop in funding negatively affects the amount of inventory the trading desk can carry, and as a result it sells into the market. As in case with dynamics associated with fire sales, selling drops prices, which feeds back to the value of collateral, and can precipitate a further reduction in funding from the money market.

The funding run is demonstrated by the two loops in Table 3.3 that focus on the effect of a price drop on the collateral held by the money market. The price shock drops the value of the collateral being held by the money market, which reduces the funding available to the bank-dealer's finance desk. This has two effects. In Loop 2, it feeds through to ultimately reduce the funding available to the hedge fund through the prime broker, forcing a reduction in quantity held, and thereby further reducing price. In Loop 9, the reduction in funding from the money market reduces the funding available to the trading desk, and its reduction in inventory again leads to a further price drop. These are only two of the possible loops where a drop in price-induced drop in funding leads to asset sales and subsequent price drops. For example, the drop in collateral value can affect the finance desk directly.

In both fire sales and funding runs, the SDG model identifies a critical dynamic that leads to market crises: actions that dampen risk on a local level can contribute positive feedback and cascades on the global level. The proper response for the prime broker when faced with a reduction in funding is to reduce funding to the hedge funds. But this leads to

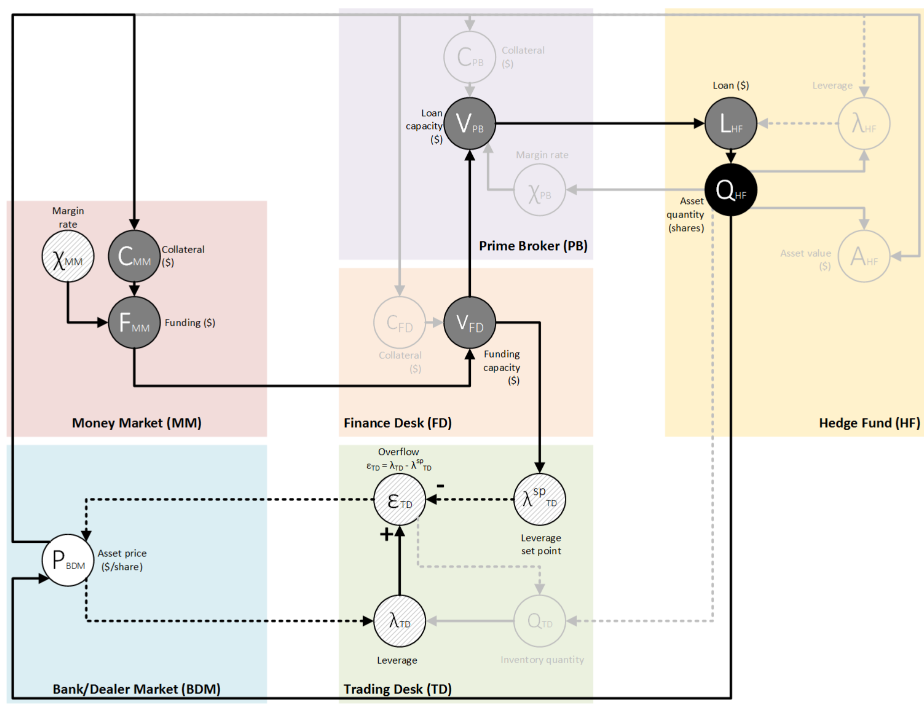


Figure 3.6: SDG model for bank-dealer funding run example

Table 3.3: Funding run loops

Index	Sign	Loop
02	+	$[P_{\text{BDM}}, C_{\text{MM}}, F_{\text{MM}}, V_{\text{FD}}, V_{\text{PB}}, L_{\text{HF}}, Q_{\text{HF}}, P_{\text{BDM}}]$
09	+	$[P_{\text{BDM}}, C_{\text{MM}}, F_{\text{MM}}, V_{\text{FD}}, \lambda^{sp}_{\text{TD}}, \epsilon_{\text{TD}}, P_{\text{BDM}}]$

actions by the hedge funds that contribute to a positive feedback cycle that reduces funding for the prime broker even further. Similarly, a locally proper response for the trading desk in the face of lower funding is to reduce inventories, but this leads to a drop in prices that feeds back to affect the value of collateral, and thereby reduces funding even further.

The unintended consequences are even more widespread than this. There are links between the segments representing fire sales and funding runs, so a funding run might precipitate a fire sale, and vice versa. From the SDG model, it is clear that a fire sale can lead to funding run, if the fire sale by the hedge fund drops prices to the point that the cash providers, seeing erosion in their collateral, begin to reduce funding. The SDG model also shows that there is pathway in the opposite direction: a drop in funding to the trading desk leads to a reduction in inventory, causing a drop in prices that reduces the value of the hedge fund portfolio, leading the prime broker to increase its margin level, thereby inducing a forced sale. The forced sale will add yet another positive feedback loop to the initial price impact that came from the trading desk. So actions that are reasonable locally can contribute to adverse global consequences.

For the simplified bank-dealer network in Figure 3.3, one can perhaps manually identify and analyze all the feedback loops listed in Table 3.1. However, for a more realistic version of this network, as shown Figure 3.7, where there are multiple hedge funds, multiple banks/dealers, multiple clients, various derivatives and structured products, it is virtually impossible to identify and analyze all such loops manually. This, again, highlights the need for the SDG framework, which can be automated to handle larger systems.

A further advantage is that the framework allows us to formulate more sophisticated models, as and when we need them, in a methodical manner. For instance, we now show how we can add numerical gains [Vaidhyanathan and Venkatasubramanian, 1996] on all the edges connecting various nodes and perform a quantitative analysis of how shocks of different magnitudes might propagate through the system. The gains used in this example are for illustrative purposes only and are not meant to reflect actual market conditions. In practice, these gains can be estimated using a combination of historical market data and the judgment of experienced market professionals.

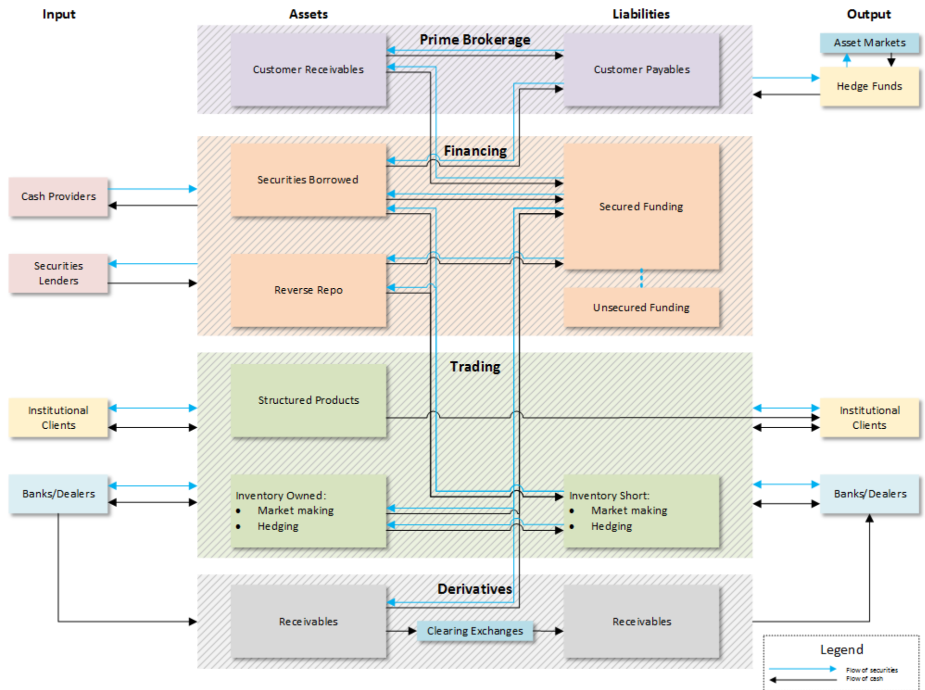


Figure 3.7: More realistic bank-dealer configuration

3.5 Semiquantitative Analysis

Consider a loop of the form $(v_1, v_2, \ldots, v_n, v_{n+1} = v_1)$ where each pair of nodes (v_i, v_{i+1}) is connected by a directed edge. Suppose the value of node v_{i+1} as a function of the value of node v_i is given by the functional relationship $v_{i+1} = f_i(v_i)$. The semi-quantitative analysis proceeds in two steps:

1. Initiate a disturbance at node v_1

2. Propagate the deviation through the nodes $v_2, v_3, \ldots, v_n$ back to $v_{n+1} = v_1$.

We are interested in quantifying whether the loop amplifies or diminishes the initial disturbance.

Let $\delta v_i = \Delta v_i / v_i$ denote the relative change in the value of node i. Then

$$\begin{aligned} \delta v_i &= \frac{\Delta v_i}{v_i} \\ &= \frac{f_{i-1}\big(v_{i-1}(1+\delta v_{i-1})\big) - f_{i-1}(v_{i-1})}{f_{i-1}(v_{i-1})} \\ &= \frac{f_{i-1}\big(v_{i-1}(1+\delta v_{i-1})\big)}{f_{i-1}(v_{i-1})} - 1 \equiv F_{i-1}(\delta v_{i-1}; v_{i-1}). \end{aligned} \tag{3.1}$$

Thus, the relative change in the value δv_i is a function of both the relative change δv_{i-1} and the current value v_{i-1}. Note that when $f_{i-1}(v_{i-1})$ is linear, i.e., $f_{i-1}(v_{i-1}) = k_{i-1} v_{i-1}$, the function $F_{i-1}(\delta v_{i-1}) = \delta v_{i-1}$. In the sequel, we will suppress the dependence on the current value v_{i-1}. We will denote δv_{n+1}, i.e., the relative disturbance in the value of node v_1 after one iteration through the loop, by $\delta v_{1,f}$. From Equation (3.1) it follows that

$$\delta v_{1,f} = F_n\Big(F_{n-1}\big(\ldots F_1(\delta v_1)\big)\Big). \tag{3.2}$$

For linear relationships, (i.e., F_i is replaced by a constant gain k_i)

$$\delta v_{i+1} = F_i(\delta v_i) = k_i \delta v_i.$$

Thus, when a loop contains only linear edges,

$$\delta v_{1,f} = k_n k_{n-1} \cdots k_1 \delta v_{1,i}.$$

We now illustrate this approach on Loop 7 displayed in Figure 3.8. Suppose the starting node $v_1 = P_{\text{BDM}}$. Our goal is to determine the relative change in the value of $v_1 = P_{\text{BDM}}$

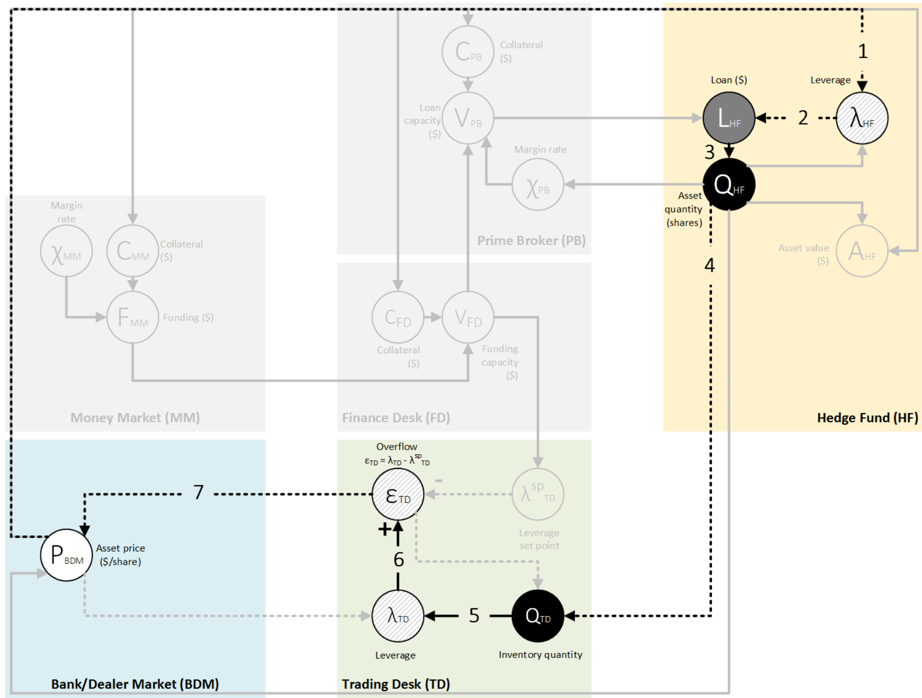


Figure 3.8: Loop 7 as an example

after one iteration. We assume that the market conditions are described as follows:

$$P_{\text{BDM}} = \$10$$

$$C_{\text{HF}} = \$1 \ \text{ billion}$$

$$C_{\text{TD}} = \$1 \ \text{ billion}$$

$$A_{\text{PB}} = \$5 \ \text{ billion}$$

$$A_{\text{HF}} = \$5 \ \text{ billion}$$

$$A_{\text{TD}} = \$15 \ \text{ billion}$$

$$A_{\text{FD}} = A_{\text{PB}} + A_{\text{TD}} = \$20 \ \text{ billion}$$

$$L_{\text{HF}} = A_{\text{HF}} - C_{\text{HF}} = \$4 \ \text{ billion}$$

$$L_{\text{TD}} = A_{\text{TD}} - C_{\text{TD}} = \$14 \ \text{ billion}$$

$$Q_{\text{HF}} = 500 \ \text{ million shares}$$

$$Q_{\text{TD}} = 1.5 \ \text{ billion shares}$$

$$\chi_{\text{MM}} = 25\%$$

$$\chi_{\text{PB}} = 25\%.$$

These values are chosen simply to illustrate the methodology; we do not claim that the values chosen are representative of true market conditions. We will first compute the functions $F_i(\delta v_i)$ for each of the nodes, and then compute the feedback effect. Economic principles give following relations.

1. $\delta\lambda_{\mathrm{HF}} = F_1(\delta P_{\mathrm{BDM}})$. The leverage

$$\begin{aligned} \lambda_{\mathrm{HF}} &= \frac{1}{1 - L_{\mathrm{HF}}/A_{\mathrm{HF}}} \\ &= \frac{1}{1 - L_{\mathrm{HF}}/\big(P_{\mathrm{BDM}} Q_{\mathrm{HF}}\big)} \equiv f_1(P_{\mathrm{BDM}}) \end{aligned}$$

   From Equation (3.1), it follows that

$$F_1(\delta P_{\mathrm{BDM}}) = \frac{-L_{\mathrm{HF}}\delta P}{P_{\mathrm{BDM}} Q_{\mathrm{HF}}(1+\delta P) - L_{\mathrm{HF}}}.$$

2. $\delta L_{\mathrm{HF}} = F_2(\delta\lambda_{\mathrm{HF}})$. The relationship between L_{HF} and λ_{HF} is as follows. The price change δP_{BDM} results in a change in the leverage λ_{HF}; this change triggers a trade since the hedge fund is targeting a fixed leverage λ_{HF}. Thus, the hedge either takes on more loan or pays down some of the loan in order to reset the leverage back to λ_{HF}. Thus, the relative change δL_{HF} can be computed from the relation

$$\lambda_{\mathrm{HF}} = \frac{A_{\mathrm{HF}}(1+\delta P_{\mathrm{BDM}}) + \delta L_{\mathrm{HF}} L_{\mathrm{HF}}}{A_{\mathrm{HF}}(1+\delta P_{\mathrm{BDM}}) - L_{\mathrm{HF}}},$$

   i.e.

$$\delta L_{\mathrm{HF}} = \frac{A_{\mathrm{HF}}(\lambda_{\mathrm{HF}} - 1)}{L_{\mathrm{HF}}}(1+\delta P_{\mathrm{BDM}}) - \lambda_{\mathrm{HF}}.$$

   Using the relationship that $\delta\lambda_{\mathrm{HF}} = F_1(\delta P_{\mathrm{BDM}})$ it follows that

$$F_2(\delta\lambda_{\mathrm{HF}}) = \frac{A_{\mathrm{HF}}(\lambda_{\mathrm{HF}} - 1)}{L_{\mathrm{HF}}}\big(1 + F_1^{-1}(\delta\lambda_{\mathrm{HF}})\big) - \lambda_{\mathrm{HF}}.$$

3. $\delta Q_{\mathrm{HF}} = F_3(\delta L_{\mathrm{HF}})$, $\delta Q_{\mathrm{TD}} = F_4(\delta Q_{\mathrm{HF}})$, and $\delta\epsilon_{\mathrm{TD}} = F_6(\delta\lambda_{\mathrm{TD}})$. The functions f_3, f_4 and f_6 are all linear; therefore, it follows that $F_3(\delta L_{\mathrm{HF}}) = \delta L_{\mathrm{HF}}$, $F_4(\delta Q_{\mathrm{HF}}) = -\delta Q_{\mathrm{HF}}$, and $F_6(\delta\lambda_{\mathrm{TD}}) = \delta\lambda_{\mathrm{TD}}$.

4. $\delta\lambda_{\mathrm{TD}} = F_5(\delta Q_{\mathrm{TD}})$. When the trading desk purchases (resp. sells) shares the capital C_{TD} of the trading desk decreases (resp. increases); moreover, the relationship is

linear. Therefore, $\delta C_{\mathrm{TD}} = -\delta Q_{\mathrm{TD}}$. The relative change in leverage δL_{TD} is given by

$$\delta\lambda_{\mathrm{TD}} = \frac{\frac{A_{\mathrm{TD}}}{(C_{\mathrm{TD}}(1+\delta C_{\mathrm{TD}}))} - \frac{A_{\mathrm{TD}}}{C_{\mathrm{TD}}}}{A_{\mathrm{TD}}/C_{\mathrm{TD}}} = \frac{-\delta C_{\mathrm{TD}}}{1+\delta C_{\mathrm{TD}}}.$$

Therefore, it follows that

$$F_5(\delta Q_{\mathrm{TD}}) = \frac{\delta Q_{\mathrm{TD}}}{1-\delta Q_{\mathrm{TD}}}.$$

5. $\delta P_{\mathrm{BDM}} = F_7(\delta\epsilon_{\mathrm{TD}})$. The relationship between P_{BDM} and ϵ_{TD} is as follows. So long as $\epsilon_{\mathrm{TD}} \leq 0$, i.e., the trading desk leverage λ_{TD} is less than or equal to the leverage set point $\lambda^{\mathrm{sp}}_{\mathrm{TD}}$, no action is taken. However, when the $\epsilon_{\mathrm{TD}} > 0$, the trading desk sells assets to reset the error $\epsilon_{\mathrm{TD}} = 0$. This trading impacts the price P_{BDM}. Thus, there is a complex non-linear relationship between $\delta\epsilon_{\mathrm{TD}}$ and δP_{BDM} that needs to calibrated from data. For the purpose of illustrating SDG approach, we assume

$$F_7(\delta\epsilon_{\mathrm{TD}}) = \begin{cases} -0.1\delta\epsilon_{\mathrm{TD}} & \text{normal market conditions} \\ -2\delta\epsilon_{\mathrm{TD}} & \text{crisis conditions} \end{cases} \quad (3.3)$$

Now we are in a position to compute the loop gain $\delta P_{\mathrm{BDM,f}}/\delta P_{\mathrm{BDM}}$ using Equation (3.2) and the nominal market condition described above. $\delta P_{\mathrm{BDM,f}}$ can be determined for a given $\delta P_{\mathrm{BDM,i}}$.

Table 3.4 reports the loop gains for all the 14 loops for both normal and crisis conditions, and for small (1%) and large (5%) initial decrease. Specifically, for Loop 7 under normal market conditions, a 1% initial decrease in P_{BDM} results in a 0.53% final decrease in P_{BDM}, i.e., the feedback through the system stabilizes the price. However, under crisis conditions, the same sale could trigger an 10.53% decrease in price. Thus, iterating over the loop several times leads to a fire sale situation.

Since the SDG approach allows one to model how the system might behave to price shocks under normal and abnormal conditions, this approach can serve as a framework for methodical stress testing and monitoring the critical nodes and edges. The next level of sophistication would be to develop differential (or difference) equations based dynamic models, which provide a more detailed analysis of the dynamic behavior of the financial system.

Table 3.4: Results for all loops

ID	Sign	Loop	Deviation	Condition	Final Value	Threshold	Remarks
1	+	[P_{BDM}, C_{MM}, F_{MM}, V_{FD}, V_{PB}, L_{HF}, Q_{HF}, Q_{TD}, λ_{TD}, ϵ_{TD}, P_{BDM}]	Low	Normal	-0.10%	-10%	safe
			Low	Abnormal	-2.02%	-10%	safe
			High	Normal	-0.53%	-10%	safe
			High	Abnormal	-10.53%	-10%	not safe
2	+	[P_{BDM}, C_{MM}, F_{MM}, V_{FD}, V_{PB}, L_{HF}, Q_{HF}, P_{BDM}]	Low	Normal	-0.10%	-10%	safe
			Low	Abnormal	-2.00%	-10%	safe
			High	Normal	-0.50%	-10%	safe
			High	Abnormal	-10.00%	-10%	not safe
3	+	[P_{BDM}, C_{FD}, V_{FD}, V_{PB}, L_{HF}, Q_{HF}, Q_{TD}, λ_{TD}, ϵ_{TD}, P_{BDM}]	Low	Normal	-0.10%	-10%	safe
			Low	Abnormal	-2.02%	-10%	safe
			High	Normal	-0.53%	-10%	safe
			High	Abnormal	-10.53%	-10%	not safe
4	+	[P_{BDM}, C_{FD}, V_{FD}, V_{PB}, L_{HF}, Q_{HF}, P_{BDM}]	Low	Normal	-0.10%	-10%	safe
			Low	Abnormal	-2.00%	10%	safe
			High	Normal	-0.50%	-10%	safe
			High	Abnormal	-10.00%	-10%	not safe
5	+	[P_{BDM}, C_{PB}, V_{PB}, L_{HF}, Q_{HF}, Q_{TD}, λ_{TD}, ϵ_{TD}, P_{BDM}]	Low	Normal	-0.10%	-10%	safe
			Low	Abnormal	-2.02%	-10%	safe
			High	Normal	-0.53%	-10%	safe
			High	Abnormal	-10.53%	-10%	not safe
6	+	[P_{BDM}, C_{PB}, V_{PB}, L_{HF}, Q_{HF}, P_{BDM}]	Low	Normal	-0.10%	-10%	safe
			Low	Abnormal	-2.00%	-10%	safe
			High	Normal	-0.50%	-10%	safe
			High	Abnormal	-10.00%	-10%	not safe
7	+	[P_{BDM}, λ_{HF}, L_{HF}, Q_{HF} Q_{TD}, λ_{TD}, ϵ_{TD}, P_{BDM}]	Low	Normal	-0.53%	-10%	safe
			Low	Abnormal	-10.53%	-10%	not safe
			High	Normal	-3.33%	-10%	safe
			High	Abnormal	-66.67%	-10%	not safe
8	+	[P_{BDM}, λ_{HF}, L_{HF} Q_{HF}, P_{BDM}]	Low	Normal	-0.50%	-10%	safe
			Low	Abnormal	-10.00%	-10%	not safe
			High	Normal	-2.50%	-10%	safe
			High	Abnormal	-50.00%	-10%	not safe
9	+	[P_{BDM}, C_{MM}, F_{MM}, V_{FD}, λ^{sp}_{TD}, ϵ_{TD}, P_{BDM}]	Low	Normal	-0.10%	-10%	safe
			Low	Abnormal	-2.00%	-10%	safe
			High	Normal	-0.50%	-10%	safe
			High	Abnormal	-10.00%	-10%	not safe
10	+	[P_{BDM}, C_{FD}, V_{FD}, λ^{sp}_{TD}, ϵ_{TD}, P_{BDM}]	Low	Normal	-0.10%	-10%	safe
			Low	Abnormal	-2.00%	-10%	safe
			High	Normal	-0.50%	-10%	safe
			High	Abnormal	-10.00%	-10%	not safe
11	+	[χ_{PB}, V_{PB}, L_{HF}, Q_{HF}, χ_{PB}]	Low	Normal	-1.00%	-10%	safe
			Low	Abnormal	-1.00%	-10%	safe
			High	Normal	-5.00%	-10%	safe
			High	Abnormal	-5.00%	-10%	safe
12	+	[P_{BDM}, λ_{TD}, ϵ_{TD}, P_{BDM}]	Low	Normal	-1.65%	-10%	safe
			Low	Abnormal	-32.94%	-10%	not safe
			Low	Normal	-28.00%	-10%	not safe
			Low	Abnormal	-560.00%	-10%	not safe
13	-	[λ_{HF}, L_{HF}, Q_{HF}, λ_{HF}]	Low	Normal	-1.23%	-10%	safe
			Low	Abnormal	-1.23%	-10%	safe
			High	Normal	-5.88%	-10%	safe
			High	Abnormal	-5.88%	-10%	safe
14	-	[ϵ_{TD}, Q_{TD}, λ_{TD}, ϵ_{TD}]	Low	Normal	-0.10%	-10%	safe
			Low	Abnormal	-1.96%	-10%	safe
			High	Normal	-0.50%	-10%	safe
			High	Abnormal	-9.09%	-10%	safe

3.6 Chapter Conclusions

The financial system does not develop as a carefully engineered system with proper consideration given to the stability and the management of its complex interactions. Because of this, it is all the more critical to understand the paths of positive and negative feedback, alternative routes for funding and securities flows in the event of a shock to one node or edge of the network, and more generally how the dynamic interactions in the system can create vulnerabilities and instabilities.

We suggest that a process systems engineering framework is the appropriate modeling paradigm for this challenge. In particular, causal knowledge represented as SDGs, and the associated process hazards analysis framework, can add the critical capabilities missing in the current network-based approaches that are emerging as the leading modeling framework for the financial system. The SDG framework adds crucial information to the context of linkages in a network in terms of the direction of various flows and whether they contribute positive or negative feedback, thereby providing a systematic framework for analyzing the potential hazards and instabilities in the system. We show that this framework can reveal hidden instabilities, and mechanisms of failure, that may not be apparent in a network-based perspective for large financial systems. It can highlight dynamics such as fire sales and funding runs, where actions that are locally stabilizing – e.g., where a financial institution takes risk management actions without an understanding of the systemic implications – might cascade to globally destabilizing consequences. Therefore, the modeling of causal knowledge help us address systemic risk at the market level of a sociotechnical system.

Chapter 4

An Ontology-Driven Knowledge Management Framework for Emerging Infectious Diseases Preparedness and Response

No knowledge obtained without risk.

Stephen King

Systemic risk associated with the market layer of a sociotechnical system can be studied via modeling causal knowledge. However, moving up along the hierarchy of sociotechnical system to the regulatory and government layers, where human decision making plays the dominant role, DAE and SDG models become difficult to apply. At these layers, the heuristic knowledge of decision makers determines system's behavior. To manage systemic risk at these layers, we need to model heuristic knowledge, which is usually documented in manuals, guidelines, etc.

In this chapter, we study a public health system, which is a typical complex sociotechnical system consisting of humans, organizations, technology, resources, and information. Systemic risk management in public health system emphasizes the management of public health document knowledge. We develop a document ontology to store and model public health knowledge so that regulators can respond to public health systemic risk more effectively.

4.1 Systemic Risk Management for Public Health

Public health experts constantly mitigate the risk of Emerging Infectious Diseases (EIDs) to keep millions of people safe. However, the recent Ebola outbreak in West Africa reminds us the weaknesses in preparing for and responding to EIDs. The Ebola epidemic directly affected the health and economies of multiple countries in West Africa over a period of two years, and resulted in 11,299 deaths among 28,599 suspected infections [Organization, 2015]. The initial international response was regarded as slow and uncoordinated by many experts [Tomori, 2015], an indication of the poor application of the lessons learned from prior global pandemics.

Effective coordination and communication of information among different stakeholders are necessary components of a strong response to an EID outbreak [Stoto *et al.*, 2013]. Public health coordination and communication requires not only sharing resources and specialties, but also sharing, managing, and using knowledge effectively. This is a recognized challenge in practice [Oshitani *et al.*, 2008; Bloom, 2002; Revere *et al.*, 2007; LaPelle *et al.*, 2006; Ho and Participants, 2014]. Knowledge sharing and management is not a single government task. It needs the collaboration of multiple groups across several sectors. Such effort, however, is usually hindered by geographical, temporal, and political constraints. A lack of a strong public health infrastructure in many countries and the persistent problems in our global health governance structure could exacerbate the crisis and complicate the collaboration [Oshitani *et al.*, 2008]. The spatial-temporal dynamics of outbreaks further complicate the real-time preparedness and response processes [Li and Mackaness, 2015; Ostfeld *et al.*, 2005; Mao and Bian, 2010]. Moreover, how to use the knowledge from prior pandemics to make a prompt decision under current condition perplexes the public health community.

Different approaches have been employed to address this challenge. Recent progress includes influenza information management [Keselman *et al.*, 2010], meta-knowledge analysis [Trinquart and Galea, 2015], and public health surveillance [Neill, 2012]. Semantic reasoning has been used to address the spatial-temporal difficulties of epidemic management [Li and Mackaness, 2015]. However, advances in the knowledge management of public health have been limited. This chapter demonstrates how to apply systems engineering concepts to develop a knowledge management framework facilitated by ontology and semantic reasoning and to support decision making in EIDs preparedness and response.

The public health system is a complex adaptive system [Bloom, 2002]. We tackle its complexity using a systems engineering-based approach [Trochim *et al.*, 2006]. The problem of EIDs preparedness and response resembles risk management in many engineering disciplines. Recently, systems engineering concepts have gained considerable attention in the public health community. National Academy of Engineering and Institute of Medicine have advocated the widespread application of systems engineering tools [Kopach-Konrad *et al.*, 2007]. Systems engineering methods such as Markov models are used to enhance public health preparedness [Yaylali *et al.*, 2014].

As a result, we propose a novel systems engineering-inspired, ontology-driven knowledge management approach. This approach utilizes knowledge from public health documents to support decision making, for both global and local levels. In this chapter, we demonstrate how to develop the ontology and semantic rules to manage knowledge and support decision making. This ontology could also serve as a part of other applications, such as a public health training or practice tool. Its flexibility enables the integration with other ontologies.

4.2 Ontology-driven Knowledge Management Framework

Public health knowledge management aims to systematically manage tasks and support decision making, which view implicit and explicit knowledge as a key strategic resource [Staab and Studer, 2013]. It needs storage, retrieval, and utilization of public health knowledge. We propose the ontology-driven knowledge management approach, which decomposes public health documents to elements of knowledge, and stores them in an ontology, namely, the Public Health Ontology (OntoPH). An inference engine accesses knowledge models, assembles and manipulates elements of knowledge in the ontology to draw conclusions about EIDs preparedness and response.

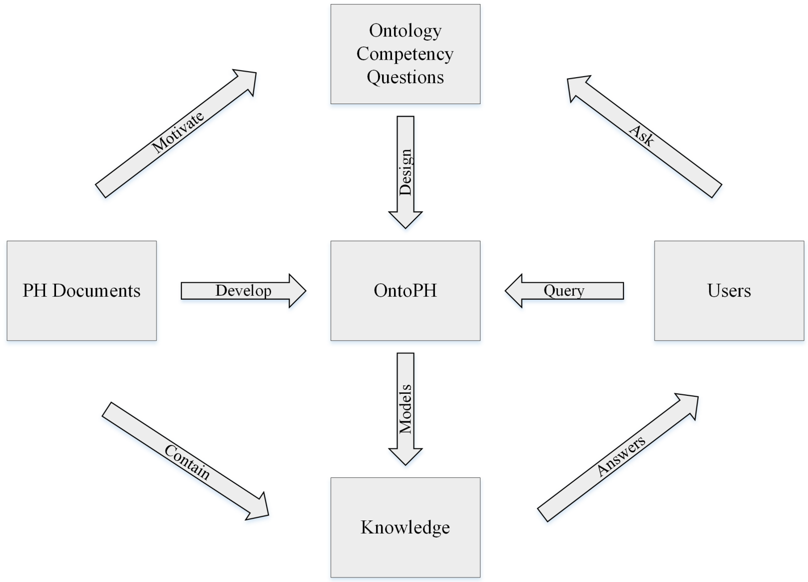


Figure 4.1: Systems engineering inspired ontology-driven knowledge management approach

4.2.1 Overall Architecture

Public health knowledge is mainly preserved in public health documents, which include guidelines, procedures, and academic publications. They are the most important media to share, store, and manage knowledge because they are vetted, high quality, generated by authoritative content source, verifiable by a trusted source and up to date and regularly updated [Revere *et al.*, 2007]. In order to support decision making, OntoPH's corpus should meet at least two requirements: breadth and depth. "Breadth" means the corpus should cover many, if not all, fields that are involved in public health decision making. "Depth" means the corpus should contain not only global-level guidelines but also local-level procedures. Our ontology-driven approach works with public health documents as depicted in Figure 4.1.

OntoPH is developed using concepts and relations decomposed from public health documents as building blocks and ontology competency questions as guidance. Grüninger and Fox state that an ontology should answer competency questions proposed based on the motivation of the ontology [Grüninger and Fox, 1995]. Competency questions define the terminology and specify the definitions and constraints of the terminology. Knowledge is modeled using the terminology. An inference engine retrieves knowledge from OntoPH via

Semantic Web Rule Language (SWRL) rules to answer users' queries.

4.2.2 Function-based Knowledge Representation

The first task is to represent knowledge preserved in public health documents. Effective knowledge storage and retrieval requires a knowledge representation, which addresses both the hierarchical complexity and the semantic heterogeneity. The hierarchical complexity of public health knowledge is rooted in the multiple layers of public health activities. Practitioners need different chunks of knowledge in various contexts to prepare for and respond to EIDs. Health workers in the clinic, for example, demand knowledge about disease diagnosis, whereas the Department of Health wants to know how to manage and coordinate. Knowledge always serves some purposes. The health workers' knowledge leads to accurate diagnoses. The Department of Health's knowledge achieves effective emergency response. Multiple layers of public health activities are linked via their purposes. To better respond to emergencies, Department of Health requires the health workers to diagnose the disease effectively.

Semantic heterogeneity, on the other hand, is the result of the cross reference of public health knowledge, which is a mixture of various fields such as medical science, epidemiology, biology, and engineering [Ho and Participants, 2014]. For instance, the knowledge of physician training lies in the intersection of medical science (i.e., what skills to train) and management science (i.e., how to train). Nonetheless, the two aspects share the same purpose, i.e., training physicians for better EIDs preparedness. In Chapter 2.2, we summarize that complex system activities usually have common purposes: communication, decision making, processing, and sensing.

One can resolve both hierarchical complexity and semantic heterogeneity by identifying the purpose of knowledge. For a piece of knowledge could serve different purposes under different conditions. Chapter 2.2 identifies the importance of means-end relation in complex system risk management and propose a systems engineering framework to explicate the relation. Adopting this idea, our approach models elements of knowledge based on their mean-end relations. We use teleological functions to represent the purposes of knowledge elements. Unlike mathematical functions that map a set of inputs onto a set of permissible outputs, teleological functions emphasize the means to realize a goal by indicating the common purpose between two connected entities. The four common purposes aforementioned induce four types of teleological functions. A function-based knowledge representation has been used in many fields including engineering [Heussen and Lind, 2009; Lind, 1994; Chittaro, 1995; Chittaro *et al.*, 1993] and data science [Kopena and Regli, 2003].

To develop such a function-based knowledge representation, we first classify public health documents into two categories, general documents that contain general public health principles and specific documents that store evidence-based procedures. There exists a gap between these two types of documents: general documents are usually too general to implement, whereas specific documents are mostly event-specific thereby limiting their usefulness for new events. We organize knowledge of general documents as a teleological function of that of specific documents:

$$\text{knowledge}_{\text{general doc}} = f\left(\text{knowledge}_{\text{specific doc1}}, \text{knowledge}_{\text{specific doc2}}, \dots\right) \tag{4.1}$$

where f is a teleological function. Specific activities expand a general guideline with specific recommendations. For example, after the 2009 Influenza A H1N1 Pandemic, many specific documents have discussed vaccination preparedness and distribution [Union, 2010; UKDOH, 2010]. World Health Organization (WHO) also has issued general guidelines for vaccination preparation during the pandemic [Organization, 2009a]. The function vaccination describes activities related to vaccination preparedness and distribution. Therefore, Equation (4.1) can be re-written as

$$\text{knowledge}_{\text{[Organization, 2009a]}} = \textit{vaccination}\left(\text{knowledge}_{\text{[Union, 2010]}}, \text{knowledge}_{\text{[UKDOH, 2010]}}, \dots\right). \tag{4.2}$$

meaning that WHO guidelines about vaccination can be expanded with specific activities, hence, bridge the gap. The function-based knowledge representation is depicted as a tree structure shown in Figure 4.2. Root of the tree is a public health document. Leaves are the event-based procedures. A *general document* (e.g., g1) contains general knowledge expressions (e.g., ge1.1 and ge1.2). A *general knowledge expression* specifies a *teleological function.* For instance, WHO guideline [Organization, 2009a] points out roles of the health and non-health sectors in vaccination sharing and distribution activities. We can label this knowledge expression with a function vaccination (i.e., f2). *Specific guidelines* (e.g., s2) elaborate the teleological functions and define many specific knowledge expressions (e.g., se1.2). *Specific knowledge expressions* can further indicate *sub-functions* (e.g., sf1.2), which include detailed procedures and instructions. Unlike specific procedures, teleological functions are event independent. Same functions can apply to different events with similar fundamental lessons. The tree structure demonstrates how general documents and specific documents are linked via teleological functions. The function-based knowledge representation handles the hierarchical complexity through the tree structure of documents, and manages the semantic heterogeneity by grouping distinct activities under the same function. Teleological functions define the scope and intention of the specific documents. They let a specific document elaborate a general document by adding actionable items.

4.2.3 Ontology Development

An ontology is a formal description of entities and their properties, relationships, and constraints [Grüninger and Fox, 1995]. It is widely used for the information system and knowledge management. An ontology consists of classes, individuals, and properties. Classes are a collection of concepts in the domain of discourse. Individuals are instances of each class. Properties are relations between classes, values restrictions, or instance descriptions in the domain of discourse. An ontology models knowledge by axiomatizing concepts as well as the relationships between them [Cimiano, 2006]. Knowledge is defined and organized in a layer style (Appendix B.1). Terms with similar meaning are classified as synonyms. A list of synonyms is defined as a concept. Concepts form a hierarchy and are connected by relations. Concepts and relations constitute general axioms that represent the knowledge of discourse. Figure 4.3 shows the ontology development process, which consists of three steps. (1) Concept Extraction: extracting knowledge from the corpus; (2) Ontology Assembly: decomposing knowledge into terms, relations, constraints, and descriptions; integrating these components to form an ontology; (3) Reasoning: creating semantic rules to enable knowledge retrieval.

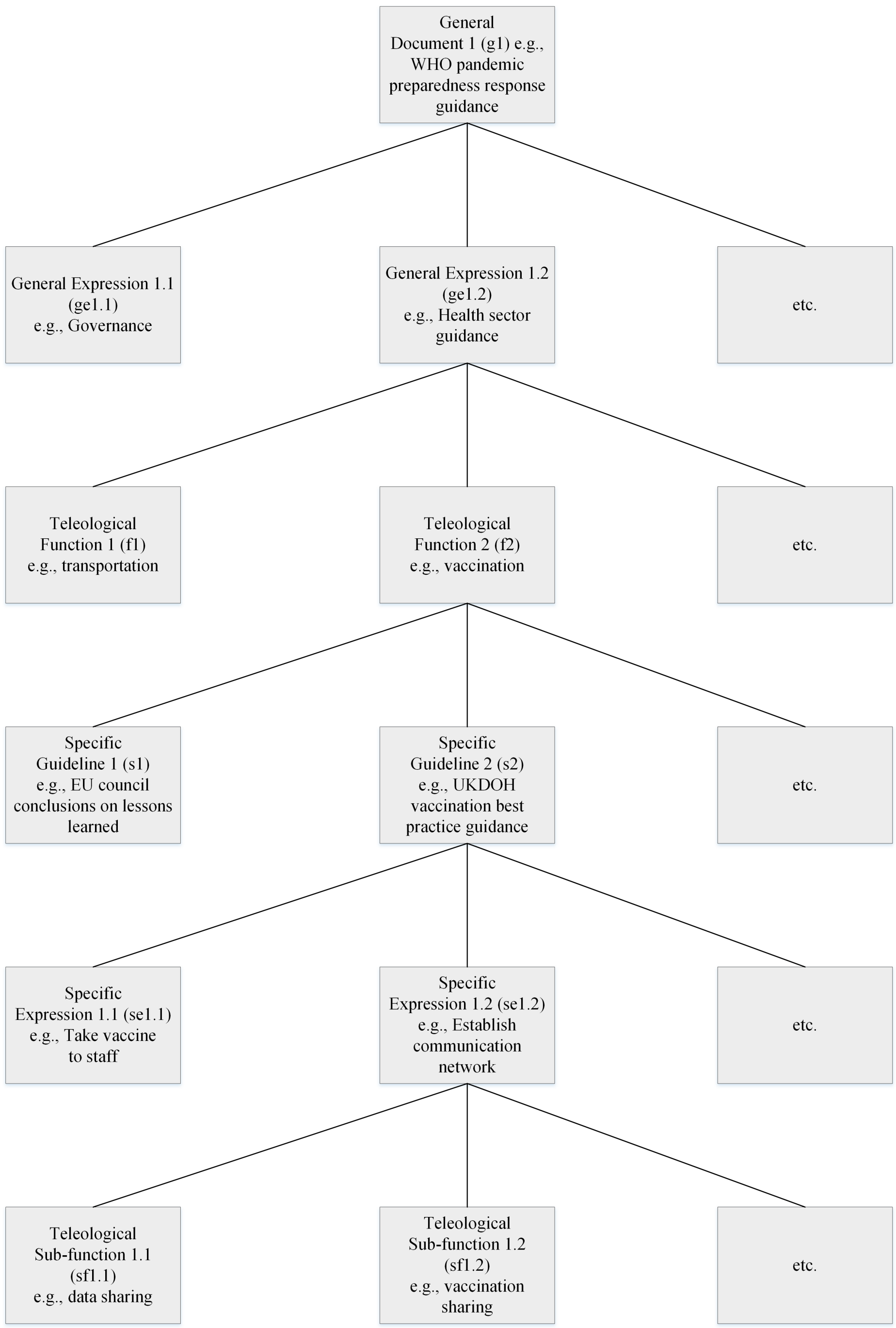


Figure 4.2: The tree structure of function-based knowledge representation

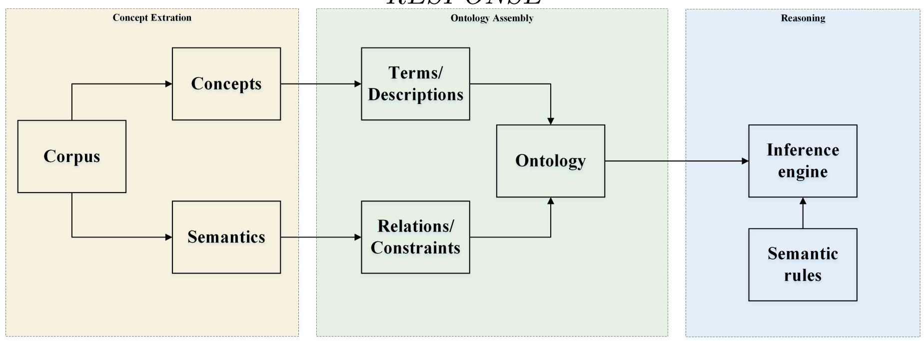


Figure 4.3: Ontology knowledge management

4.2.3.1 Concept Extraction

Our corpus, with 135,946 words in total, consists of the U.S. Code [Government, 2011], federal level regulations [Union, 2010; UKDOH, 2010; Services and Human, 2013; Services and Human, 2010], international health regulations [Organization, 2009a; Organization, 2005; Organization, 2010; Organization, 2009b], and pandemic evaluations of outbreak responses [Fineberg, 2014; Asnis *et al.*, 2000]. They cover all types of public health documents aforementioned. U.S. Code is the generic legal document, which ensures that the ontology aligns with laws. The federal regulations and the international health regulations are guidelines regarding surveillance, transportation, and preparedness. The evaluations are chosen per disease. Influenza A (H1N1) virus (H1N1) and West Nile Virus (WNV) are two specific diseases chosen for illustration. These two cases are selected because they are well studied recent emerging diseases with an impact on health resources both locally and globally. In addition, their impact on health and geographical coverage are both significant. We want to evaluate case examples where the primary infection risk is associated with different infection transmission routes in order to evaluate the potential for having a unified framework for EIDs. There are two knowledge extraction methods available: manual annotation and Natural Language Processing (NLP) annotation. Manual annotation requires domain experts to review and annotate every term in the corpus per predefined criteria. Manual annotation provides high accuracy but requires tremendous human effort. On the other hand, NLP annotation automatically recognizes and classifies terms into predefined categories [Carley *et al.*, 2012]. NLP annotation is much more efficient than manual annotation but at the cost of accuracy. Usually, a NLP based information retrieval performs clustering or classification to identify key concepts. The performance is usually measured by precision or recall [Riloff and Wiebe, 2003].

In this work, we implement a hybrid approach. NLP methods are used mainly for pre-processing the corpus. By removing stop words and tagging the parts of speech, one can extract meaningful and most frequent terms and relations using text mining tools like KHCoder [Higuchi, 2001]. The classification work is done manually. Two domain experts (our collaborators from Columbia Mailman School of Public Health) review every term and relation, and decide their descriptions and constraints. OntoPH is built upon these terms and relations. Domain experts and ontology engineers work collaboratively to select and annotate documents. Such a team-based method has been used extensively in many scientific studies and applications, such as the HAZOP analysis in chemical engineering [Venkatasubramanian and Rengaswamy, 2003]. Such a team should be as small as possible while maintain sufficient expertise. In a series of meetings, team members work together to select documents. Conflicts must be resolved before the list of documents is finalized. Each domain expert annotates a part of the corpus and reviews others' annotations. This practice, therefore, keeps the corpus and annotation as objective as possible.

4.2.3.2 Ontology Assembly

OntoPH includes 199 classes, 78 properties, and 1234 axioms (Appendix B.2-B.8). We develop the general structure of OntoPH based on the Legal Knowledge Interchange Format (LKIF) Core Ontology. LKIF Core Ontology is developed by the European project for Standardized Transparent Representations to extend Legal Accessibility Consortium to cater for a continuing need for a standard vocabulary of basic legal terms [Hoekstra *et al.*, 2007]. We expand this legal term vocabulary to include public health vocabulary.

OntoPH is structured in a modularized nature. Modularization improves the reusability, scalability, and maintenance of an ontology [dAquin *et al.*, 2007; Grau *et al.*, 2007]. OntoPH has seven modules: space-time module, agent module, action module, role module, process module, document module, and event module. Inheriting all modules, OntoPH core module has nine main classes (Table 4.1). The *Space* class defines spatial concepts such as region and nation. The *Time* class describes temporal concepts such as time point or period. The *Resource* class specifies resources used for public health preparation and response. The *Action* class defines potential actions for an EID event. Actions are categorized regarding the four basic teleological functions: communication, control, implementation, and monitoring. Sub-classes of the *Action* class represent specific functions under the four basic functions. The *Process* class describes both continuous and discrete event flows. The *Agent* class lists all the intelligent and non-intelligent agents involved in a process or an action. The *Description* class describes the state and the role of any agent or action or process. The *Medium* class summarizes different types of public health documents, such as legal documents or non-binding documents. Lastly, the *Expression* class represents the knowledge expressions of the documents.

OntoPH properties (Appendix B.6-B.7) define the relationships between classes and subclasses. For instance, *participate* (Figure 4.4) has a domain of *Role* and a range of *Action*, indicating that a role participates in some actions. This property has an inverse of *participate_by*. OntoPH contains individuals extracted from public health documents. For example, *Legal_role*, a subclass of *Role*, has individuals of "emergency committee" and "PH authority" (Figure 4.5).

4.2.3.3 Semantic Rules and Reasoning

OntoPH is developed using Web Ontology Language (OWL) under Protégé environment [Musen, 2015]. Logic-based semantic rules allow OWL to "exploit the considerable existing body of logical reasoning fulfill important logical requirements" [Wang *et al.*, 2004]. They imply answers to the competency questions. OntoPH answers three types of questions: (1) the relation between actions and roles; (2) the relation between roles and the outbreak conditions; and (3) the relation between actions and the outbreak conditions. OntoPH uses *Time*, *Space*, *Resource*, and *Process* classes to describe the conditions of an EID outbreak. Hence, we can construct the following informal competency questions:

1. What action must a role perform?

2. What are the roles specified by an action?

Table 4.1: Ontology classes

Class	Sub-class
Action	Communication Control Implementation Monitoring
Agent	Animal Human Organization Other agent Pathogen
Description	Attribute Role
Expression	Argument Assertion Assumption Comment Declaration Evaluative proposition Evidence Expectation Fact Feedback Intention Knowledge Observation Qualification
Medium	Document Sample
Process	Continuous process Discrete process
Resource	Equipment material Financial Human resource Intellectual tool
Space	Area Space point
Time	Period Time point

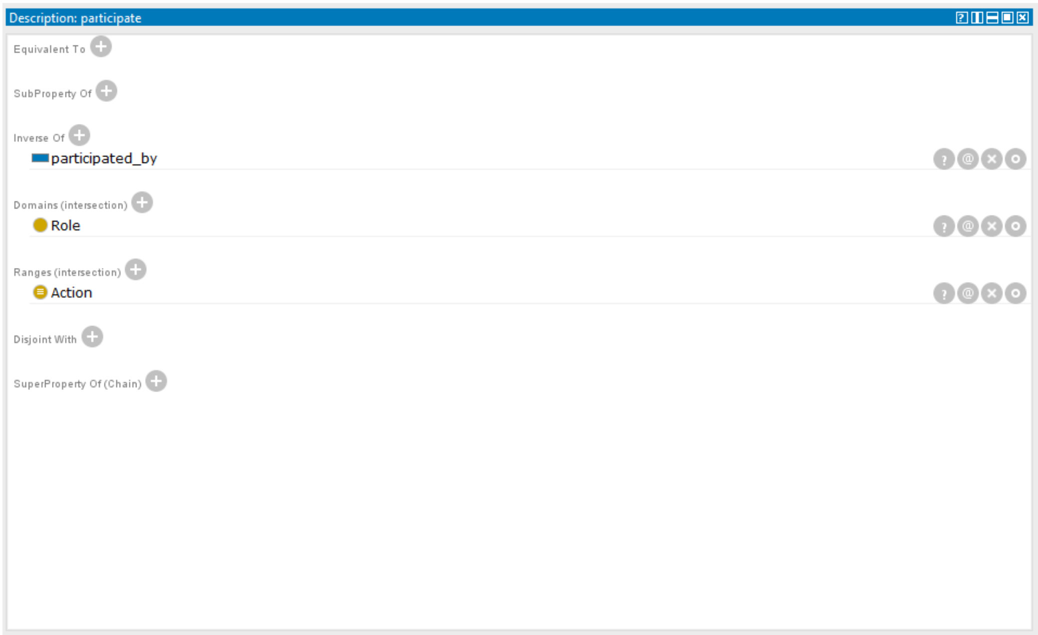


Figure 4.4: Protégé screenshot for Property "participate"

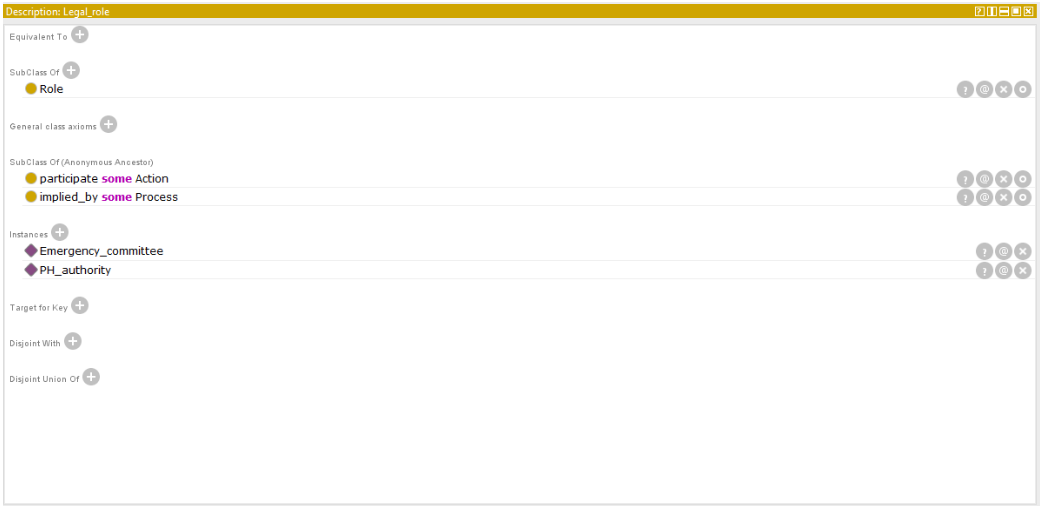


Figure 4.5: Protégé screenshot for Individual "Legal_role"

3. What are the actions required under an outbreak condition?

4. What are the roles specified under an outbreak condition?

Informal competency questions should be translated to a formal format, so that an ontology can retrieve the elements of knowledge to answer them [Grüninger and Fox, 1995]. We denote T_{ontology} as a set of axioms in the ontology, G_{ground} as a set of ground instances, and Q as a first-order sentence using only predicates in the language of T_{ontology}. We can formulate the formal translations for the four informal competency questions.

(1) Let $Q(\text{action})$ denote a sentence that describes some actions. Given a ground formula G_{role} defining instances of role, determine

$$T_{\text{condition}} \cup T_{\text{action}} \cup G_{\text{role}} \vDash Q(\text{action}) \tag{4.3}$$

(2) Let $Q(\text{role})$ denote a sentence that describes some roles. Given a ground formula G_{action} defining instances of action, determine

$$T_{\text{condition}} \cup T_{\text{role}} \cup G_{\text{action}} \vDash Q(\text{role}) \tag{4.4}$$

(3) Let $Q(\text{action})$ denote a sentence that describes some actions. Given a ground formula $G_{\text{condition}}$ defining instances of a condition, determine

$$T_{\text{role}} \cup T_{\text{action}} \cup G_{\text{condition}} \vDash Q(\text{action}) \tag{4.5}$$

(4) Let $Q(\text{role})$ denote a sentence that describes some roles. Given a ground formula $G_{\text{condition}}$ defining instances of a condition, determine

$$T_{\text{action}} \cup T_{\text{role}} \cup G_{\text{condition}} \vDash Q(\text{role}) \tag{4.6}$$

Semantic rules will link axioms T with instances G, and entail a first-order sentence Q, which is the answer to the competency question.

Semantic rules are created using Semantic Web Rule Language (SWRL), a rule language for the semantic web. SWRL rules apply unary predicates for describing classes and data types, binary predicates for properties, and some special built-in n-ary predicates [Kuba, 2012]. An example SWRL rule is as

Listing 4.1: SWRL rule for married parents

```
(Person(?x), hasParent(?x, ?y), hasParent(?x, ?z),
hasSpouse(?y, ?z) -> ChildOfMarriedParents(?x))
```

This rule describes the assertion that someone is a child of married parents. Letters with question mark (e.g., $?x$) denote variables. Person($?x$) indicates that a variable x is a *Person*. The binary relation hasParent($?x$, $?y$) indicates that person x has a parent y. The formal formula is shown in Equation (4.7), which reads: there exists persons x, y, and z if x has parent y, and x has parent z, and y and z are a spouse, then x is a child of married parents. SWRL rules translate natural language assertions into computable forms.

$$\begin{aligned}&(\exists x, y, z : \text{Person})[\text{hasParent}(x, y) \wedge \text{hasParent}(x, z) \wedge \text{hasSpouse}(y, z)]\\&=> \text{childOfMarriedParents}(x).\end{aligned} \tag{4.7}$$

We create SWRL rules in three steps (rules are listed in Appendix C.1 and C.2). (1) Public health experts review documents and identify knowledge expressions. For example, the "WHO Technical Advice for Case Management of Influenza A(H1N1) in Air Transport" [Organization, 2009a] ("WHO Advice Air Transport") is a WHO issued guideline for air transportation case management. It specifies the procedures that the pilot in command should follow when a suspicious case is identified. We identify a knowledge expression "pilot_in_command_action" under the *Expression* class. (2) Public health experts create logic expressions for knowledge expressions. This intermediate step translates a procedure into a formal representation. For example, the "pilot_in_command_action" can be written as logic expressions,

$$\begin{aligned}&(\exists \text{ Pilot action})(\exists \text{ Pilot})(\forall r : \text{Reporting})\\&[\textit{contains}(\text{Case mgt, Pilot action}] \vDash \textit{participate}(\text{Pilot}, r).\end{aligned} \tag{4.8}$$

$$\begin{aligned}&(\exists \text{ PH authority})(\exists \text{ Comm between agencies})\\&[\textit{contains}(\text{Case mgt, Comm between agencies})]\\&\vDash \textit{participate}(\text{PH authority, Comm between agencies}).\end{aligned} \tag{4.9}$$

Logic expressions and natural language are interchangeable. Equation (4.8) says "WHO Advice Air Transport" contains specifications about pilot actions. The pilot in command should report any suspicious activities on the flight. Equation (4.9) says that "WHO Advice Air Transport" requires communication between agencies. Public health authority should communicate with other agencies. (3) Public health experts work with ontology engineers to develop the SWRL rules based on the logic expressions from step 2. Listing (4.2) shows the SWRL rule created for the same example. The rule first states the knowledge expression and its parent document. Then, it specifies the roles ("Pilot" and "PH_authority") and the expected actions.

Listing 4.2: SWRL rule for pilot

```
Guideline(Case_management_H1N1_AirTransport_guidance),
Knowledge(Pilot_in_command_actions)
-> contains(Case_management_H1N1_AirTransport_guidance,
Pilot_in_command_actions)

Non-health_sector(Pilot), Reporting(?reporting),
contains(Case_management_H1N1_AirTransport_guidance,
Pilot_in_command_actions) -> participate(Pilot, ?reporting)

Legal_role(PH_authority),
Interactive_network(Communication_between_agencies),
contains(Case_management_H1N1_AirTransport_guidance,
Pilot_in_command_actions) -> participate(PH_authority,
Communication_between_agencies)
```

Logical inference connects documents with knowledge expressions. An inference process is depicted in Figure 4.6. "WHO Advice Air Transport" carries many knowledge expressions. One of them informs the chief pilot's actions for an EID emergency during a flight mission. This piece of knowledge then implies that pilots and public health authority should

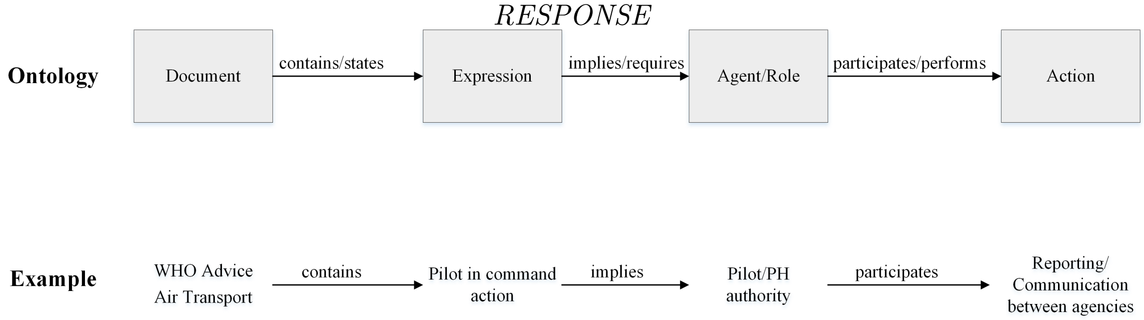


Figure 4.6: An inference process

report suspicious cases and communicate with each other in time.

Reasoning results are presented per individual. Figure 4.7 shows the reasoning results of “Mayor’s Office of Emergency Management” under the class *Department*. Given an individual, we obtain a list of sentences, such as “Mayor’s Office of Emergency Management performs delivery strategy.” These sentences in fact are the elements of knowledge.

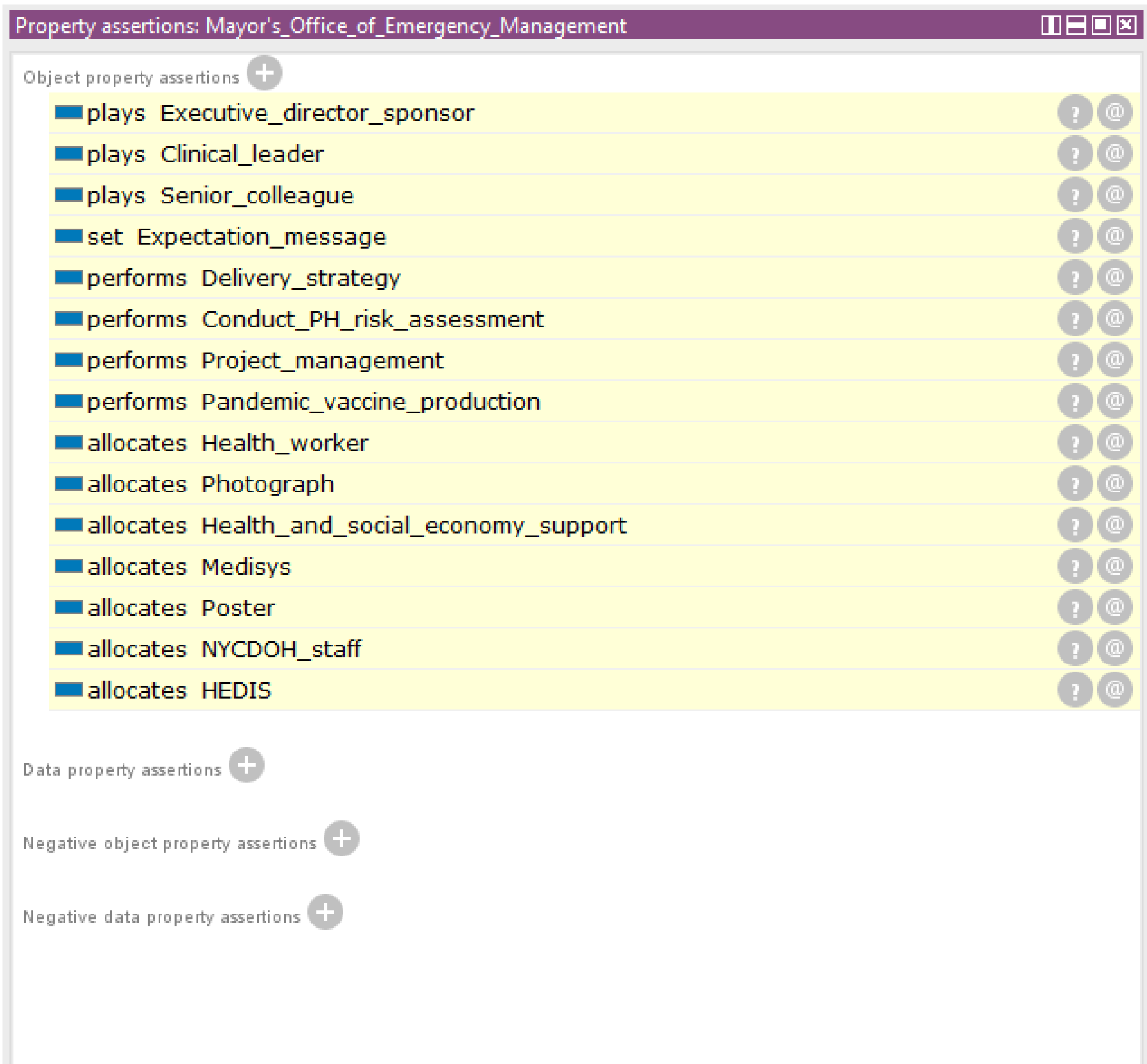


Figure 4.7: Reasoning results

4.3 Results

We use OntoPH in two different ways. First, OntoPH answers general questions regarding EIDs preparedness and response. Second, it provides recommendations with respect to an outbreak. OntoPH achieves both via semantic reasoning. Before applying OntoPH, we need to evaluate its quality.

4.3.1 Ontology Evaluation

The quality of ontology is critical. It affects not only the quality of reasoning results but also the effectiveness of the application. Ontology can be evaluated on many aspects, namely, vocabulary, syntax, structure, semantics, representation, and context [Staab and Studer, 2013]. Extensive research has been conducted to formally evaluate the quality of ontologies [Staab and Studer, 2013; Burton-Jones *et al.*, 2005; Duque-Ramos *et al.*, 2014; Brank *et al.*, 2005; Maedche and Staab, 2002]. Among these methods, we follow OQuaRE approach [Duque-Ramos *et al.*, 2014], which adapts the software engineering ISO standards SQuaRE. OQuaRE assesses 6 characteristics, 39 sub-characteristics of an ontology using quality metrics. Quality metrics are composed of primitive and derived measurements. Primitive measurements are metrics that can be measured directly on the ontology, such as number of classes, number of relations, etc. Derived measurements are combinations of some primitive ones [Duque-Ramos *et al.*, 2014]. With a scale 1 to 5 (1 means "not acceptable" and 5 means "exceeds the requirement"), it rates every aspect of an ontology. Final score is the arithmetic average of individual scores of all characteristics. The details of this method can be found on Duque-Ramos *et al.* [Duque-Ramos *et al.*, 2014]. We include 30 out of the 39 sub-characteristics in our evaluation. The other 9 sub-characteristics that require experts' subjective assessment are excluded. The evaluation results of OntoPH core ontology is presented in Table 4.2. The evaluation indicates that the core ontology is satisfactory with an average score of 4. Problems have been found on redundancy and controlled vocabulary, mainly due to the relatively small corpus size.

Table 4.2: Ontology evaluation results

Characteristics	**Sub-characteristics**	**OQuaRE Score**
Structural	Formalization	5
	Formal relations support	4
	Redundancy	2
	Consistency	5
	Tangledness	4
	Cycles	5
	Cohesion	4
	Domain coverage	4
Functional adequacy	Controlled vocabulary	2
	Schema and value reconciliation	4.67
	Consistent search and query	4
	Knowledge acquisition representation	3.67
	Clustering	2
	Similarity	4
	Indexing and linking	4.5
	Results representation	5
	Text analysis	5
	Guidance	5
	Decision trees	4.5
	Knowledge reuse	4.28
	Inference	4.67
Compatibility	Replacebility	3.5
Transferability	Adaptability	3.5
Operability	Learnability	4.17
Maintainability	Modularity	3
	Reusability	4
	Analyzability	3.8
	Changeability	4
	Modification stability	4.2
	Testability	3.8

4.3.2 Answering Queries

OntoPH answers general queries based on the competency questions. By substituting the axioms with classes and the ground instances with individuals, we obtain specific questions. For illustration purpose, we list four simple queries as following:

1. What actions should the clinical leader perform in workplaces regarding vaccination issues?
2. What are the roles involved in vaccine sharing during an outbreak?
3. What are the health sector communication activities that involve the Healthcare Effectiveness Data and Information Set (HEDIS)?
4. Who are emphasized with respect to the financial resources during the preparedness process?

We rephrase query 1 as: Given clinical leader, regarding vaccination issues in workplaces, what are the implied actions? Applying the formal form of competency question 1 (Equation (4.3)), we substitute G_{role} with "clinical leader," $T_{\text{condition}}$ with *Workplace*, and T_{action} with *Vaccination*. Figure 4.8 displays the reasoning

- Boxes: OntoPH classes;
- Nodes: OntoPH instances (blue nodes are implied instances);
- Arcs: relations implied by OntoPH inference;

Then the answer to query 1 is a formal formula:

$$\begin{aligned}&(\exists\ \text{Clinical leader})(\forall i \in \text{Vaccination})(\forall j \in \text{Workplace})\\&\vDash participate(\text{Clinical leader}, i) \wedge in(i, j).\end{aligned} \tag{4.10}$$

It reads: Clinical leader participates vaccination activities such as vaccine sharing, the p2p vaccination campaign, and vaccination distribution in the office or in the ward.

Following the same logic, we restate query 2: Given vaccine sharing, what do health sector and non-health sector staff imply? Competency question 2 (Equation (4.4)) is applied

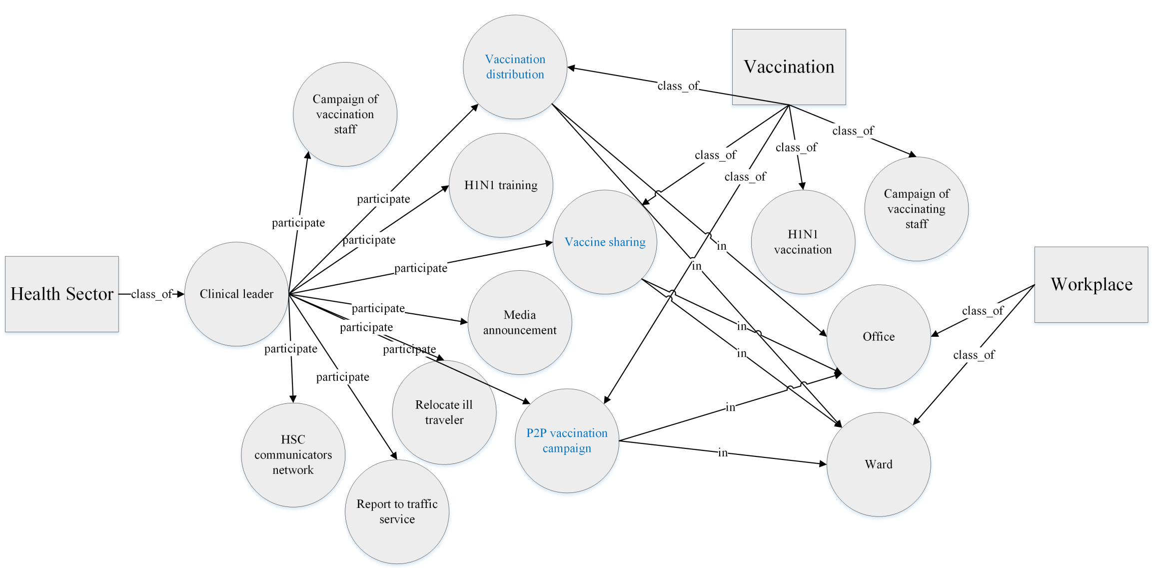


Figure 4.8: Query 1 reasoning process

by substituting G_{action} with "vaccine sharing," and T_{role} with *Health sector* and *Non-health sector* and $T_{\text{condition}}$ with *Staff*. Similarly, query 3 is rephrased: Given the intellectual tool (e.g., HEDIS) we are interested in, for an interactive network, what are the implied activities of health sector? Competency question 3 is applied with $G_{\text{condition}}$ as the "intellectual tool," T_{role} as the *Health sector*, and T_{action} as the *Interactive network communication*. Query 4 is translated: Who is important with respect to health and social economy support considering surveillance? By replacing $G_{\text{condition}}$ with "health and social economy support," T_{action} with *Surveillance*, and T_{role} with *Non-health sector*, OntoPH gives an answer to query 4. Figure 4.9-4.11 depict the reasoning results respectively. The formal formulas of the reasoning results are:

$$(\exists \text{ Vaccine sharing})(\forall i \in \text{Health sector})(\forall j \in \text{Non-health sector})(\forall k \in \text{Staff}) \models \mathit{involves}(\text{Vaccine sharing}, i) \wedge \mathit{involves}(\text{Vaccine sharing}, j) \wedge \mathit{involves}(\text{Vaccine sharing}, k). \quad (4.11)$$

$$(\exists \text{HEDIS})(\forall i \in \text{Interactive network})(\forall j \in \text{Health sector}) \models \mathit{participate}(j, i) \wedge \mathit{involved}(\text{HEDIS}, i). \quad (4.12)$$

$$\begin{aligned}&(\exists\text{Health and social economy support})(\forall i \in \text{Surveillance})(\forall j \in \text{Nonhealth sector})\\&\vDash involves(i, j) \wedge involved(\text{Health and social economy support}, i)\\&\wedge allocates(j, \text{Health and social economy support}).\end{aligned} \tag{4.13}$$

and their natural language translations are:

- Vaccine sharing requires the input of health workers and the New York Department of Health (NYCDOH) staff.
- HEDIS can be used by the Mayor's Office of Emergency Management for Health Security Committee (HSC) communicators network and the human and animal health authority communication.
- The NYCDOH staff are the important non-health roles with respect to health and social economy support for surveillance.

Next, we want to verify whether the reasoning results can provide meaningful suggestions to real outbreaks. We create a test scenario - a hypothetical WNV outbreak – that is similar to the one happened in 1999 in New York City (NYC). We intentionally modify some details, such as outbreak locations, responding agents, etc., of 1999 WNV outbreak to evaluate OntoPH's reasoning capacity. The goal is to verify whether the ontology is able to provide meaningful outbreak preparedness and response suggestions.

4.3.3 West Nile Virus Outbreak Case Study

We assume that a hypothetical WNV outbreak occurs in Europe. WNV is a mosquito-borne virus known in Africa, the Middle East, and southwestern Asia [Asnis *et al.*, 2000]. On August 23, 1999, two cases were reported to the NYCDOH. By the end of that week, six additional cases had been identified. An intensive effort has been made to discover 62 NYC residents infected, marked the first documented appearance of WNV in the Western Hemisphere and the first arboviral outbreak in NYC since the yellow fever epidemics [Fine and Layton, 2001]. WNV outbreak is a relatively small scale outbreak. Its simplicity makes

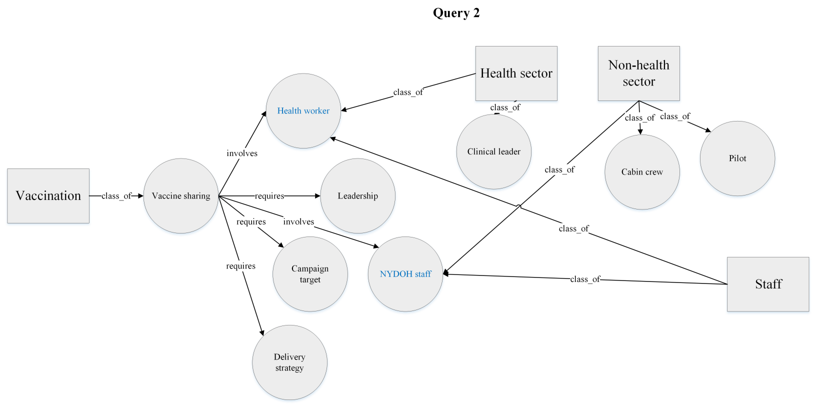


Figure 4.9: Query 2 reasoning process

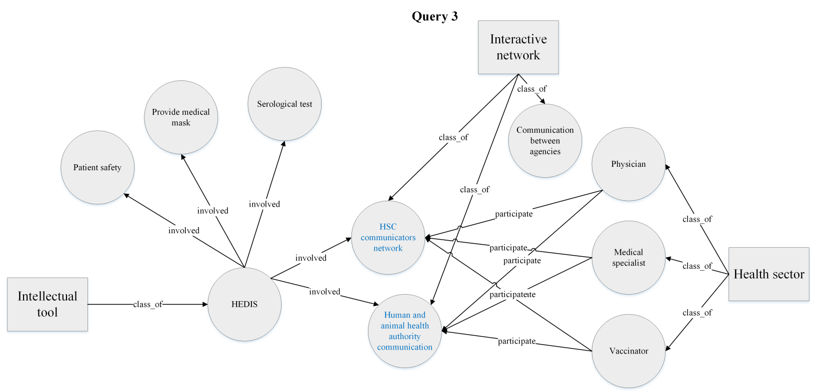


Figure 4.10: Query 3 reasoning process

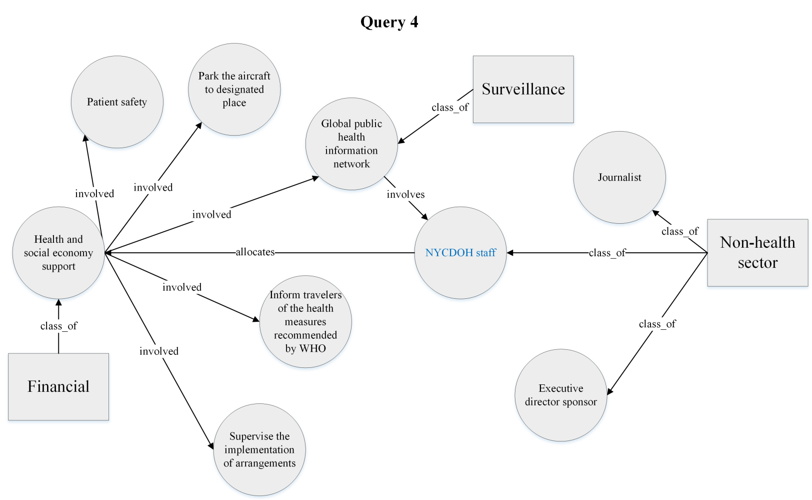


Figure 4.11: Query 4 reasoning process

it suitable for demonstration. We wonder what advice OntoPH will generate to prepare for and respond to this epidemic.

WNV information includes descriptions about the disease, relevant agents, locations, etc. OntoPH classifies the input information by their classes. Semantic reasoning connects these classes with other relevant classes and instances. Therefore, an instance-to-instance relationship is established. This relationship is described by a logical expression. Users feed a piece of WNV query information to OntoPH, and it will return corresponding logical assertions as results. Hence, users can directly find useful information from the ontology rather than digging out the documents.

OntoPH's response to this hypothetical scenario is a list of recommendations. The recommendations emphasize activities of government agencies and public health community. OntoPH recommends that the Emergency Office (Figure 4.7) should conduct risk assessment, issue vaccine delivery strategy, and prepare vaccines. EU member states should allocate resources such as health workers, financial support, and staff members. On the other hand, reporting suspicious cases and communicating with animal health authority are critical communication actions during the outbreak. Communication requires the participation of different roles such as journalist, health workers, and physicians. Specifically, physicians are recommended to engage in the communication with animal health authority. Vaccination, as a control action, is another important aspect. Vaccination distribution requires the collaboration of staff from Department of Health, health workers, and disease experts. OntoPH not only asks for an authority communication program for vaccination distribution but also suggests a way of doing so (e.g., using an HSC communication network). OntoPH advocates educational programs, such as physician training program. It suggests that both physicians and animal health experts should be properly trained. Reasoning details of above recommendations are presented in the Appendix B.9-B.14.

We compare the recommendations with those made by Fine and Layton [Fine and Layton, 2001] for the 1999 WNV outbreak in NYC. They recommend to (1) enhance awareness and train clinicians; (2) improve communication between human and animal health authorities; (3) strengthen laboratory capacity; and (4) prepare public education. OntoPH recommendations are able to cover most of these aspects; moreover, it gives similar guidance in a more systematic manner. OntoPH scans through its knowledge base and lists all the possible relations between individuals. The reasoning results form pieces of knowledge consistent with the outbreak condition.

4.4 Discussion

The possibility of using ontology and semantic reasoning in public health decision making has been recognized in literature [Bure *et al.*, 2012]. In this work, we adapt this idea and our previous experience of knowledge management in pharmaceutical industry [Venkatasubramanian *et al.*, 2006] to derive a detailed methodology on how to develop such a tool. We introduce the systems engineering inspired ontology-driven framework for public health knowledge management. We demonstrate how complex and heterogeneous public health knowledge can be modeled and stored in an ontology. Previous work has focused on local activities, such as activities within a healthcare network [Rao *et al.*, 2014]. OntoPH extends the scope from local level to global/national level by focusing on general documents.

OntoPH's strength is threefold. First, it stores public health documents knowledge as classes, relations, and instances. Public health documents, including guidelines, procedures, and academic publications, are important sources of knowledge. Even though medical records, GIS data, and disease information have been studied and stored in the ontologies [Schriml *et al.*, 2012; Rao *et al.*, 2014], to our knowledge, there is no ontology for public health documents. OntoPH provides this missing piece of public health knowledge management. Second, we present a flexible knowledge management framework. OntoPH implements a modularized structure, which ensures its extensibility. For example, the space-time module can be extended using time ontologies [Hobbs and Pan, 2004; Rao *et al.*, 2014] and W3C spatial ontologies [Lieberman *et al.*, 2007]. It is also possible to add new modules. If disease information is needed, we can create a new disease module, which inherits the Disease Ontology [Schriml *et al.*, 2012]. This modularized structure makes OntoPH a potential generic public health knowledge center. Third, OntoPH can manage the hierarchical complexity and heterogeneity of public health knowledge. Elements of knowledge are effectively organized by the teleological functions that highlight the means-end relations.

This framework is most useful in the Low- and Middle-Income Countries (LMICs). A lack of resources and public health experts in LMICs usually makes knowledge management system difficult to implement. Nonetheless, OntoPH's general knowledge is widely applicable. By Expanding the data sources to include LMICs specific knowledge [Nolen *et al.*, 2005] and connecting with other ontologies [Tao *et al.*, 2010; Hobbs and Pan, 2004; Lieberman *et al.*, 2007; Schriml *et al.*, 2012], OntoPH would become a useful tool to help LMICs respond to an outbreak quickly, both at the national and the local levels.

OntoPH can support decision making by answering users' queries. For example, given an outbreak scenario, a user could list questions regarding disease identification, transmission prevention, disease control, and risk mitigation. With enough pre-stored knowledge, OntoPH could answer the list of questions by producing logical assertions with respect to each question. However, at this stage, there still exist some limitations.

4.4.1 Limitations

First, the training document corpus is relatively small. Only five general documents and seven specific documents are pre-stored due to the manual annotation constraint. It requires a more concerted effort to annotate and develop a more extensive public health knowledge base for widespread application. Nonetheless, the current corpus is comprehensive enough for proof of concept. Second, the selection of documents is subjective. When the corpus size is small, the accuracy of reasoning results is dependent on the document selection rather than the knowledge base. Increasing the size of the corpus and precise query statement will improve reasoning accuracy in general. In addition, rule-based reasoning has its intrinsic limitations – semantic rules are subjective. SWRL rules rarely allow ternary relations and that limits the power of the SWRL representation. Third, the current framework is restricted to public health documents, which lack information from various data sources, such as GIS data, news articles, social media feeds, etc. This limits OntoPH's real-time usage. Moreover, current knowledge representation would not be able to capture knowledge in research articles that do not fit in the knowledge model. However, the basic and domain ontologies, such as space-time module, resource module, role module, and agent module, contain fundamental public health knowledge, therefore, make the knowledge framework extendable to cover research articles. It of course requires further study of new knowledge representation. Potentially, a research article knowledge expression module could be developed and incorporated into OntoPH.

4.4.2 Future Work

Future work aims to address the limitations and evaluate OntoPH's reasoning capacity. Adopting artificial intelligence techniques would significantly reduce the human effort, thus, get rid of many of the limitations. Specifically, a term extraction module implementing NLP techniques such as topic modeling would enable automated concept classification of public health documents, reducing the amount of work required for annotation. Enriching data sources will improve OntoPH's ability of real-time response. We plan to expand the corpus incorporating experts' opinions. A survey for eliciting expert feedback on what to include in the corpus will be conducted. A systematic literature review on effectiveness of policy and interventions could help us determine what documents to include. To further evaluate this method, we will conduct a survey to collect a list of general queries from public health practitioners. Moreover, we will test OntoPH's reasoning capacity on realistic outbreaks. The full-scale case studies will provide us valuable information on how to improve the usage and accuracy of OntoPH decision support.

4.5 Chapter Conclusion

In recent decades, many EID outbreaks and epidemics have resulted in considerable human disability and mortality in part due to ineffective coordination or slow response at the start of the outbreak. Responding to EID outbreaks is intrinsically challenging due to the uncertainties associated EID, specifically level of risk and potential the impact of its spread in a population. During an outbreak, evidence-based public health policies developed by public health authorities, legislators, and other government officials facilitate the implementation of a strong public health response. However, there are structural and political forces that prevent decision makers from making evidence-based policies in response to outbreaks.

Therefore, it is necessary to have in place a mechanism to easily identify evidence in order to evaluate the consequences of public health or policy actions recommended to address these public health emergencies. An ontology framework for public health outbreak response will cut the time spent aggregating expert opinions during the initial stages of an outbreak. It would also assist public health administrators and government officials on next steps based on individual- and systems-level factors associated with the outbreak.

This approach manages document knowledge for the regulatory and government layers of a public health system. It introduces a systematic way of storing, retrieving, and using public health knowledge. Accuracy and comprehensiveness of decision making can be improved as more knowledge is stored in the ontology. It is a potentially effective methodology for EIDs preparedness and response.

Chapter 5

Modeling Emergent Phenomena of Dynamical Sociotechnical Systems

Nothing endures but change.

Heraclitus

In previous chapters, we discussed how to model system knowledge, cause-and-effect knowledge, and heuristic knowledge for a sociotechnical system. Systemic risk management requires the understanding of system's emergent behaviors. In this chapter, we model system's teleodynamics, i.e., the goal-driven dynamics, to study emergent behaviors to answer the question, "*how do simple individual components of a system interact to result in a system behavior that cannot be explained by the components alone?*" This has been a long standing open question, especially from a control-theoretic perspective.

We investigate simple systems to understand how interactions of parts lead to unexpected behavior of the whole. People may wonder how simple systems could help explain emergence in complex systems. However, science and engineering are full of examples of simple models that give useful insights about complex phenomena even though they may miss some of the details.

5.1 Emergent Behaviors in Dynamical Sociotechnical Systems

A chemical plant is a multi-layer hierarchical structure where information or materials flow within each layer or through different layers via goal-driven processes. This hierarchical structure can be modeled as a seven-layer input-output framework, depicted in Figure 2.1. At each layer, elements achieve their goals via their functions. For example, a level controller of a tank system has the goal to maintain the level at its set-point. The controller achieves this goal by tuning the electronic signal of valve pressure. When elements (e.g., controller) have realized their goals, the system (e.g., level control tank system) achieves its desired status. This is a goal-driven process. A chemical plant is a hierarchy of such networked processes. One level is an aggregation of processes of the adjacent level below it. When low-level processes execute their goals, the aggregate effect makes the system at the high-level evolve a new state. Ideally, this new state is the goal of the high-level system. However, as the system becomes more complex, it might evolve towards a state that is not a desirable one. For example, BP Texas City refinery and Deepwater Horizon oil rig are at the plant level while BP as a company is at the company level. The flawed activities at the BP plants can lead to unexpected state of BP, i.e., a vast monetary loss and reputation crisis. The whole event is a systemic failure. The goal-driven activities in multi-layered hierarchy lead to emergent behaviors, some of which are undesirable.

To ensure safe operations over the life cycles of chemical plants, we need to design, analyze, and model their behaviors, and manage the potential for increasing systemic instability and fragility [Centeno *et al.*, 2015; Fouque and Langsam, 2013]. This requires the representation of system behavior focusing on the mechanisms generating behavior in the actual, dynamic work context [Rasmussen, 1997]. Along these lines, some researchers try to understand the system's self-organizing behavior [Bialek *et al.*, 2012; Feistel, 2016; Hemelrijk and Hildenbrandt, 2011; Polani, 2013; Reynolds, 1987]. Others study the complex dynamics of engineered systems using chaos theory [Hirsch *et al.*, 2012] and control theory [Leveson and Stephanopoulos, 2014; Ogunnaike and Ray, 1994; Seborg *et al.*, 2011]. These studies focus on explaining what is emergent behavior. However, the question how simple individual components interact to result in a system behavior that cannot be explained by the behavior of individual components alone has not been explicitly answered in a control-theoretic setting.

In this chapter, we try to answer this well-known question in complexity science from a control-theoretic perspective. We explain how goal-driven behaviors propagate and aggregate in a hierarchical sociotechnical system. This chapter unfolds as follows. First, we review both the philosophical and the scientific definitions of emergence. Next, we argue that the study of emergence needs to investigate goal-driven dynamics. We introduce a formal representation to illustrate emergent behaviors of different systems. We also compare our approach with Qualitative Simulation (QSIM).

5.2 Define Emergence: A Journey from Philosophy to Science

Let us start the discussion by reviewing the definition of emergence. English philosopher G. H. Lewes coined the term "emergence" [Lewes, 1877] in 1875. Emergent phenomena are widely recognized in biological, physical, chemical, and social systems. Emergence has been extensively discussed in both philosophy and science. Now people tend to agree that emergent phenomena represent the behaviors that "the whole is more than the sum of its parts." An emergent behavior is usually novel and not previously observed by any parts. The emergent behavior appears as integrated whole at the system level. Moreover, it is not pre-given but evolves over time [Goldstein, 1999].

Philosophers are interested in the fundamental question – "what is emergence?" Tremendous efforts have been devoted to an answer [Bar-Yam, 2004; Bedau, 1997; Bedau, 2008; Bonabeau and Dessalles, 1997; O'Connor, 1994; Prokopenko, 2008; Steels, 1991]. All have emphasized the concept "level," i.e., the *part-whole relationship* [Deguet *et al.*, 2006]. Among these works, two famous perspectives have established: *strong emergence* and *weak emergence*. Strong emergence is defined by O'Conner [O'Connor, 1994] as:

> Property P is an emergent property of a (mereologically-complex) object O iff P supervenes on properties of the parts of O, P is not had by any of the

> object's parts, P is distinct from any structural property of O, and P has a direct ("downward") determinative influence on the pattern of behavior involving O's parts.

Strong emergence emphasizes supervenience of systems, which leads to a downward causation. However, Bedau argues that this downward causation raises from nothing, which makes strong emergence scientifically irrelevant [Bedau, 1997]. In contrast, Bedau defines *weak emergence* as: macro-state P of system S with micro-dynamic D is weakly emergent if and only if P can be derived from D and S's external conditions but only by simulation [Bedau, 1997]. Weak emergence emphasizes the interactions between system and the "external" environment, as well as the claim that emergence can be shown only via simulation, which is more scientifically relevant. Chalmers well summarized both perspectives [Chalmers, 2008]:

> A high-level phenomenon is strongly emergent with respect to a low-level domain when the high-level phenomenon arises from the low-level domain, but truths concerning that phenomenon are not deducible even in principle from truths in the low-level domain. A high-level phenomenon is weakly emergent with respect to a low-level domain when the high-level phenomenon arises from the low-level domain, but truths concerning that phenomenon are unexpected given the principles governing the low-level domain.

These two definitions successfully describe the characteristics of emergence, however, are difficult to apply. Many concepts in the definitions are ambiguous and confusing. For example, novel behaviors such as birds flocking are based on visual inspection and have no quantitative meaning.

Scientists want to examine the role of emergence in natural and social phenomena. Emergence has been defined from a self-organization perspective [Deacon, 2011; Goldstein, 1999]. Mathematical models and simulations are developed to model emergent behaviors of a bird flock and a biological system [Cucker and Smale, 2007; Marsh, 2009]. From a complexity science perspective, emergence is defined as the attraction of a strange attractor [Newman, 1996]. Both formal representation and system dynamics are used to investigate emergence [Hollnagel, 2012; Newman, 1996]. Parunak *et al.* demonstrate the emergent behavior of a power grid is the stabilizing behavior without centralized control [Parunak and VanderBok, 1997]. The simulation shows the system converges to a fixed/stable point. Recent years, game theory, information theory, and systems science have been used to explain emergent phenomena. A game-theoretic model by Paravantis *et al.* [Paravantis, 2016], for example, is developed for world politics and diplomacy. It treats international relations as complex sociotechnical systems and studies how political relations emerge. Information loss principle is used to explain the unintended computational properties that emerge in computational processes [Licata and Minati, 2016]. Others study system's structural and symbolic information to explain how a system evolves over time [Feistel, 2016].

5.3 Teleodynamics: the Dynamics of Sociotechnical Systems

We investigate what contribute to the part-whole relationship of a sociotechnical system. Corning explains emergence as "a subset of the vast (and still expanding) universe of cooperative interactions that produce synergistic effects of various kinds, both in nature and in human societies" [Corning, 2002]. "Cooperative interactions" underscore the goal-driven activities, whereas "synergistic effects" emphasize the aggregate effect of these activities. Recall that sociotechnical systems are multi-layered hierarchy. The aggregation is not happening just at one layer, but at different layers. The inter-layer "synergistic effects" conduce an emergent behavior.

Therefore, sociotechnical system behaviors can be understood through the study of goal-driven behaviors propagating through the hierarchical structure, namely, *teleodynamics*. As the name suggested, teleodynamics is the dynamics of goal-driven agents, who act to achieve their individual goals and collectively drive the system to a new state [Venkatasubramanian, 2017b]. Teleodynamics was originally proposed by Venkatasubramanian [Venkatasubramanian, 2007] to state how part-level properties are related to the system-level properties in a self-organizing network. He further developed statistical teleodynamics [Venkatasubramanian, 2017a; Venkatasubramanian, 2017b], the mathematical framework for analyzing goal-driven agents' emergent behavior in the context of economics. Activities in a sociotechnical system are driven by goals. Even if the system is not statistical, teleodynamics is applicable in the understanding of its part-whole relationship.

Teleodynamics emphasizes the relationship between *teleology* and *dynamics*. Teleology means the study of things in terms of their purposes, principles, and goals. It emphasizes the *means-ends* relation of entities, which essentially captures the input-output process of the system. "End" is the system goal imposed by the system modeler. "Means", on the other hand, represents the process to achieve the goal. For example, the "end" of a tank is to maintain the liquid level to the set-point, whereas the "means" of a tank is to contain liquid. Kant emphasizes the importance of teleology as a way of understanding nature in the "Critique of Teleological Judgment" in 1790 [Kant and Pluhar, 1987]. Teleology is the end or purpose in Kant's view (The terms "end" and "purpose" in translations of the Critique of Judgment both correspond to the German term Zweck [Ginsborg, 2014]). However, the usefulness of teleology was not well recognized by the scientific community until recent years. Bertalanffy underscores the importance of teleology in analyzing complex sociotechnical systems. He emphasizes teleology as one of the keys to understanding the "wholeness" of systems [Von Bertalanffy, 1968]. Along these lines, Chittaro explains the usefulness of using both teleological and functional knowledge to model physical systems. He uses teleological knowledge to abstract a system and functional knowledge to bridge the gap between abstract purposes and the actual structure and behavior of the system [Chittaro *et al.*, 1993]. Venkatasubramanian highlights the teleological multi-perspective modeling framework for managing risk in sociotechnical systems [Venkatasubramanian, 2007; Venkatasubramanian and Zhang, 2016]. On the other hand, dynamics studies how a physical system changes over time. Mathematical models are used to represent the evolution of a system. Classical system dynamics handles systems with a flat structure and goal-free agents. Nonetheless, dynamics of sociotechnical systems consisting of goal-driven agents requires an adaption of classical dynamical theory. Teleodynamics, therefore, is an extension. It demonstrates the propagation of dynamical behaviors across levels via goals. The aggregate effect of low-level activities becomes a function at the high-level. Teleodynamics captures the common theme among various definitions of emergence – the concept "level." It describes the dynamics resulting from the goal-driven activities propagating through the hierarchy of sociotechnical systems, thus, induces emergent behaviors.

Therefore, the question aforementioned really reduces to the investigation on how teleodynamics explains the part-whole relationship.

5.4 A Formal Representation for Sociotechnical Systems

To model emergent behaviors of a sociotechnical system, we need a unified representation that captures system's teleodynamics. This representation should satisfy several criteria. First, it should be simple, i.e., capturing only the essential elements of a sociotechnical system, so that a complex sociotechnical system (e.g., the financial system) can be properly represented. Second, it needs to have a structure that mimics the part-whole nature of sociotechnical systems. Third, this representation should reveal means-end relations.

A sociotechnical system consists of agents and their interactions. It can be viewed as a collection of agents, which are described by some characteristics. The interactions are functions that enable the system moving from one state to another. System behavior, therefore, is the path of state transitions. In this spirit, we propose a formal representation, which abstracts system components as classes and sets, and adopts the formal definition of functions to describe means-end relations.

5.4.1 Object

A sociotechnical system consists of many agents, both autonomous and non-autonomous. Informally speaking, an agent is an *object* that is *something perceived by the sense or presented to the mind (a physical or mental entity)*. For example, a bird in a flock is an object. A controller in a level control tank system is an object as well. Therefore, a *system* is defined as *an intended organization of a collection of objects*, formally a class, denoted as SY,

Definition 5.4.1.

$$SY = \{x_1,\ x_2,\ \ldots,\ x_n : x_1,\ x_2,\ \ldots,\ x_n \text{ are objects}\}$$

Members of SY are denoted as,

$o \in SY$ abbreviates "*o is an object of system SY.*"

A sociotechnical system is represented as a class of objects. It simplifies the representation of systems by focusing on the collection of objects rather than the nature of objects.

5.4.2 Attribute

However, objects themselves cannot fully describe the status of a system. People use objects' characteristics to illustrate system's state. For example, a liquid tank can be characterized by its volume, height, material, etc. We call them attributes. An *attribute* is *a characteristic, a feature, or a factor that can help in defining a particular object or system.*

Definition 5.4.2. Attributes of object i form a class

$$A_i = \{\varrho : \varrho \text{ is an attribute of an object } i\}.$$

Attributes of a system form a class

$$A = \{A_i : \forall i \in SY\}.$$

Attributes are also known as state variables, which have values.

5.4.3 Value

The value space of an attribute numerically characterizes the collective activity of physics. *Values* are *mathematical entities that represent magnitudes of attributes of objects or systems, denoted as* $\mathbb{V}$. Mathematical entities are well constructed in *ZFC* axiomatic system [Kunen, 2009]. Values precisely describe attributes, hence, the corresponding objects and system. v_ϱ denotes the value of any attribute ϱ of an object. For instance, a tank has an attribute of height h, which has a value space ranging from 0 to infinity, denoted as $\{v_h : v_h \geq 0\}$. An object's attributes with values represent the status of the object, namely, state.

5.4.4 State

A system has a state space $\mathbb{S}$ that *describes all the possible statuses of a system.* $\mathbb{S}$ consists of system state S, which is a set of objects' state s.

Definition 5.4.3. States of an object i form a set

$$s_i = \{v_\varrho : \forall \varrho \in A_i\}.$$

So the jth state of the system SY is

$$S_j = \{s_i : \forall i \in SY\}.$$

The state space $\mathbb{S}$ is a union of all states,

$$\mathbb{S} = \bigcup S_j \forall j.$$

System's dynamical behavior can be described by state transition. The three types of states (s, S, and $\mathbb{S}$) capture the hierarchy of a sociotechnical system.

5.4.5 Function

State transition is enabled by functions, which is formally defined as follows [Kunen, 2009]:

Definition 5.4.4. f is a function *if and only if* f is a relation and for every $x \in \text{dom}(f)$, there is a unique y such that $(x, y) \in f$. In this case, $f(x)$ denotes that unique y ($!y$).

$$\forall x \in S_k \exists ! y \in S_l \text{ such that } (x, y) \in f[u = (x, y)].$$

A *function* is specified regarding *an object or a system in relation to some rules or principles describing an intended state-change* [Heussen and Lind, 2010b]. In other words, functions are mappings between input states and output states. That is, functions have $\text{dom}(f) \subset S_k$ and $\text{ran}(f) \subset S_l$. The formal definition allows a function to be quantitative or qualitative. The quantitative form is usually seen at low-levels of a sociotechnical system, whereas qualitative form is more applicable for high-levels. Functions and states together represent the means-end relation.

5.4.6 Phase Space

Visualizing system behaviors requires delineating state transitions. In fact, state transition has been widely used to study dynamical behavior of automata, which is also a famous example of emergence [Wolfram, 1984]. In our representation, we capture three types of states, i.e., object state s, system state S, and a set $\mathbb{S}$ consisting of all the possible system instances. One may find it similar to the ensemble theory that describes system's micro- and macro-states. For a microcanonical ensemble, a micro-state describes a snapshot of the system, where all the parameters of constituents are specified. A macro-state, on the other hand, is defined by the specifications of macro-level physical quantities such as number N, temperature T, energy E. It is a collection of micro-states. In our representation, a system state S is similar to a micro-state, which depicts the system at a particular moment. The set $\mathbb{S}$ is similar to an ensemble of a system, hence, can be seen as the phase space, which is a $k \times n$ dimensional space if each of n objects has k attributes. A subset of $\mathbb{S}$ possibly forms a macro-state. Therefore, micro-states and macro-states have the same meaning even though the language is different.

The notion of phase space naturally underscores the part-whole relationship by distinguishing micro- and macro-states. The means-end relation is represented by state transition, which forms phase space trajectories. Such trajectories delineate the goal-driven dynamical behaviors of the system. Therefore, phase space is an ideal tool to visualize system's teleodynamics.

The dynamical view of the world through the phase space is not new. In fact, there is a long history of studying complex dynamics in the phase space [Strogatz, 2014]. In 19th century, Poincaré invented this geometric tool to visualize complex nonlinear dynamics so that one can study the dynamics without actually solving it. Since then, it has been used in modelings of both self-organizing systems [Pathria and Beale, 2011] and dynamical systems [Nolte, 2010; Strogatz, 2014]. The phase space is used to demonstrate complex dynamical behaviors, such as the three-body problem [Szebehely, 2012]. Quantum physics uses it to study molecule behaviors, which is the foundation of statistical thermodynamics.

We extend the usage of phase space to teleodynamics by emphasizing the part-whole and the means-end relationships. *A system behavior can be seen as a phase space trajectory*, which consists of states and functions. The system moves from one micro-state to another along the trajectory, consequently, develops a behavior. *A single point on the trajectory cannot induce the entire state transition.* It means that one cannot predict the system's behavior by only knowing objects' states. It is objects' functions and their causal relationships that facilitate the state transitions.

5.5 Modeling Emergent Behaviors – Control Examples

In this section, we show the emergent behaviors of different dynamical systems by studying their teleodynamics. Examples include a linear level control tank and a nonlinear level control tank, which are parts of a complex sociotechnical system, and a financial system at the market view layer, which mainly consists of humans.

5.5.1 A Level Control Tank

A level control tank, depicted in Figure 5.1, consists of three main objects: a tank, a controller, and a valve. They are characterized by three attributes: liquid level h, valve pressure p, and flowrate q. Using the formal representation, we can reveal its means-end relations, hence, understand its teleodynamics.

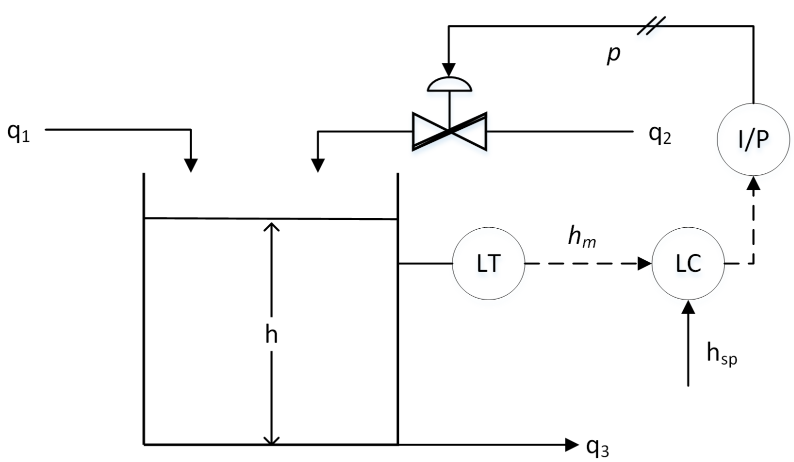


Figure 5.1: The level control tank system (adapted from [Seborg *et al.*, 2011])

This system can be written as a collection of objects:

$$SY = \{\text{valve}, \text{ controller}, \text{ tank}, \text{ liquid}\}.$$

Attributes of each mechanical/electronic object (obviously liquid is not) form a class,

$$A_{\text{tank}} = \{h\}$$
$$A_{\text{controller}} = \{p\}$$
$$A_{\text{valve}} = \{q_2\}$$

where h is the tank level, p is the valve pressure, q_2 is the liquid flowrate. They are elements of the system attribute class A,

$$A = \{A_{\text{controller}},\ A_{\text{valve}},\ A_{\text{tank}}\}.$$

Attributes have quantitative values in $\mathbb{R}$. Therefore, the object states are

$$s_{\text{tank}} = \{v_h\}$$
$$s_{\text{controller}} = \{v_p\}$$
$$s_{\text{valve}} = \{v_{q_2}\}.$$

The jth system state or a micro-state is

$$S_j = \{s_{\text{controller}},\ s_{\text{valve}},\ s_{\text{tank}}\}.$$

Then, the phase space can be expressed as

$$\mathbb{S} = \bigcup S_j, \forall j,$$

depicted in Figure 5.2. The phase space contains all the possible micro-states of the system. If the system is *unconnected*, i.e., *no causal relationship* exists among the three objects, we need all three attributes to fully describe the system. The attributes can take any values in $\mathbb{R}$. Being axes of the phase space, these attributes form a three-dimensional space, where every point is a three-tuple (h, p, q_2). The *continuum of phase volume* shown in Figure 5.2 represents the sum of parts, i.e., all possible states of the system.

If the system is *connected*, functions of the objects are stated mathematically as follows [Seborg *et al.*, 2011]:

$$e = k_m(h'_{\text{sp}} - h')$$
$$p' = k_c \cdot e$$
$$q'_2 = k_v \cdot p',$$

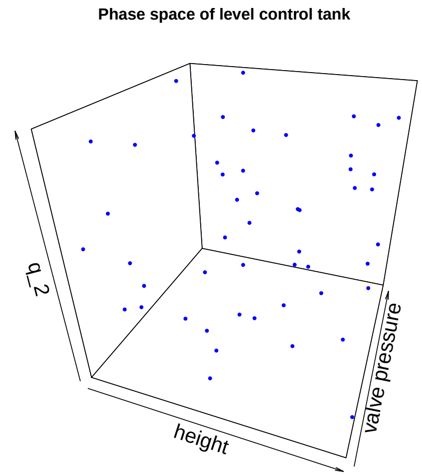


Figure 5.2: The phase space of unconnected linear level control tank system

where primed variables stand for the deviation variables and e is the error (i.e., difference) between actual tank level and set-point level. The system has a goal of controlling the liquid level in the tank. It is realized by the controller which tunes the valve pressure through the I/P transducer; the valve opens up and let liquid flow into the tank; and the tank constantly measures the liquid level, compares with the set-point, and sends the signal to the controller. The teleodynamics can be described by the following differential equations,

$$\begin{aligned} A\frac{dh'}{dt} &= q_1' + q_2' - q_3' \\ &= q_1' + q_2' - \frac{h'}{R} \\ &= q_1' + k_v k_c k_m (h'_{\text{sp}} - h') - \frac{h'}{R} \\ &= q_1' + k_c k_v k_m h'_{\text{sp}} - (k_v k_c k_m + \frac{1}{R})h', \end{aligned}$$

where q_1 is a constant inflow to the tank, $k_m = 0.5$, $k_c = 4$, $k_v = 1.03 \times 10^{-2}$, $A = 0.785$, $h_{sp} = 1$, and $R = 6.37$ (values taken from Example 11.2 of Seborg *et al.* [Seborg *et al.*, 2011]) are process constants.

This system has linear dynamics and one state variable is enough to describe the system state as shown in Figure 5.3. The dynamics describes the control behavior, whereas the teleodynamics indicates how goals and functions determine that behavior. The corresponding phase line on the right not only shows the linear dynamics, but also reveals how a system behavior emerges. Tank level $h(t)$ can be viewed as a particle moving along the line. At equilibrium, the particle remains at rest. Figure 5.4 shows that the tank level h stays close to the set-point with an offset, due to proportional control action on a first-order process. The cause of the offset has been discussed in detail elsewhere [Seborg *et al.*, 2011] and is not important here. The solid dot represents a *stable fixed point*. Obviously, the system eventually moves to the fixed point in the phase space.

When the system is *unconnected*, any object's function and goal do not interact with those of the others. Therefore, their states are independent of each other's. So the "system" can be at any one of the random dots shown in the phase space figure (Figure 5.2), at any given time. In fact, when unconnected, this collection of objects has not become a *system* yet. That happens only when they are all *connected* in a *particular* manner.

When the system is *connected* in the appropriate manner, a *causal* relationship is *imposed* among the objects. Now, the *output* of one object *determines* the *input* of another object it is connected to. Their states are *not* independent anymore, but are now limited to a few admissible ones, instead of the entire phase space continuum they had in the unconnected case. The connectivity *imposes* certain *constraints* on the possible states of the objects. Thus, the teleodynamics results in a *phase line*, instead of a *phase volume*, with a *stable fixed point* embedded in it. By connecting all these objects in an appropriate manner, we have *qualitatively* changed the nature of the allowed phase space. In the unconnected version, all points in the phase space are *equally likely* to be occupied by the objects collection at any time. There is no preferred region or preferred point. But in the connected version, we have imposed certain constraints on the phase space, making a certain region (in fact, a certain point) more preferred than others at steady state. And the system eventually gets attracted to the preferred region, in this case a preferred point, namely, the fixed point, and settles there at steady state. For this to happen, all the objects need to be connected in the correct manner. Further more, all the parameters have to be in the correct ranges. For example, for the controller to work properly, its proportional gain parameter has to have the correct value. If, for example, it is extremely low, then it will not be effective in providing feedback control action and the system will not reach this fixed point.

In the unconnected version, the phase space is merely the "sum of its parts," metaphorically speaking. To be more precise, it is actually the "product of its parts." If the valve pressure ranges from $0 - 100$, tank level also $0 - 100$, and controller set point also $0 - 100$, then the total phase space volume is simply $100 \times 100 \times 100$ – the product of its parts! The unconnected collection of these objects can be *anywhere* in this volume - for example, the controller set point at 81, the valve at 25, and the tank level sensor at 60, giving the state $(81, 25, 60)$. The other such combinations are all also equally likely. There is no preferred point or region.

But, when connected, the fixed point, determined by the controller set point, emerges as the preferred point. This is where the system will now settle at, at steady state. The system's phase space is no longer the entire $100 \times 100 \times 100$ phase volume, but it is constrained to a phase line, and even that is restricted to a fixed point. So, the system's phase space is no longer the "product of its parts," but something *qualitatively* different. In this case, the "whole" is *not* more than the "sum of its parts," but *less*, as far as phase space region is concerned. But whether it is more or less is *not* the point. The point is that the "whole" is *very different* from the "sum of the parts," *qualitatively.*

But where is this information contained? It is not obvious from the individual properties of the components. It seems to emerge from their dynamic interactions. The phase line is a system-level information, not known by any individual component. As a result, we say that *the level control behavior is an emergent behavior.* It is not previously known by any individual components, and thus is novel from the components' perspective.

5.5.2 Nonlinear Level Control Tank

Next, let us consider a more complicated example – a nonlinear level control tank [Ogunnaike and Ray, 1994], depicted in Figure 5.5. Similarly, this system consists of four objects: a tank, a valve, a controller, and liquid. The formal representation is similar to the one in preceding example, except the function of the tank is no longer linear. The system SY can be written as

$$SY = \{\text{valve, controller, tank, liquid}\}.$$

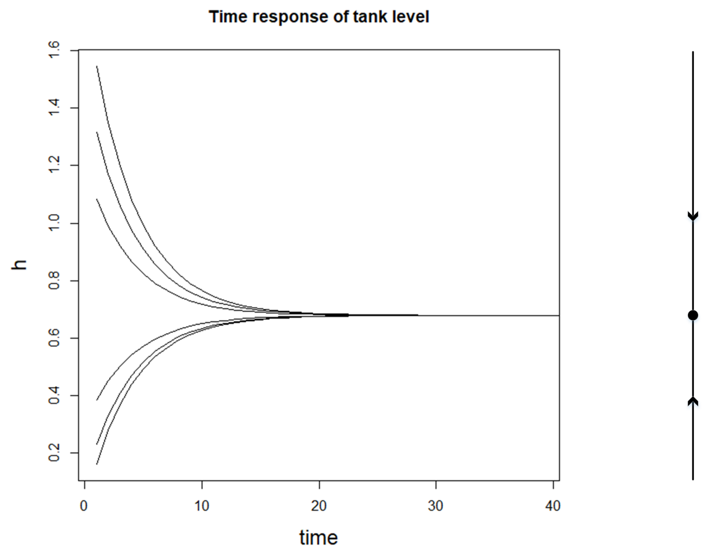


Figure 5.3: The time response of the linear level control tank system

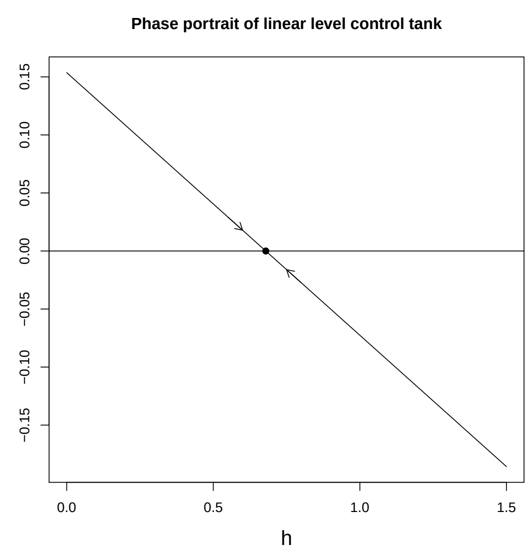


Figure 5.4: The phase portrait of the linear level control tank system

Objects are characterized by attributes,

$$A_{\text{tank}} = \{h\}$$

$$A_{\text{controller}} = \{p\}$$

$$A_{\text{valve}} = \{F_o\}$$

where h is the tank level, p is the valve pressure, F_o is the liquid outflow rate. So the system attribute class

$$A = \{A_{\text{controller}},\ A_{\text{valve}},\ A_{\text{tank}}\}.$$

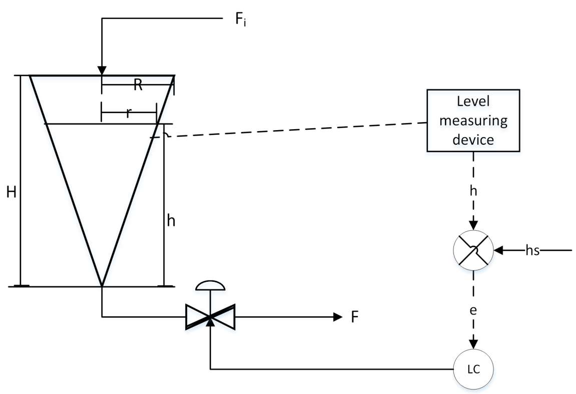


Figure 5.5: The nonlinear level control tank system (adapted from [Ogunnaike and Ray, 1994])

These attributes have values in $\mathbb{R}$. Therefore, object states can be written as

$$s_{\text{tank}} = \{v_h\}$$

$$s_{\text{controller}} = \{v_p\}$$

$$s_{\text{valve}} = \{v_{Fo}\}.$$

The jth system state is

$$S_j = \{s_{\text{controller}},\ s_{\text{valve}},\ s_{\text{tank}}\}.$$

The phase space is

$$\mathbb{S} = \bigcup S_j, \forall j.$$

The three attributes become the axes of the phase space, as shown in Figure 5.2. The functions of objects are described by the following equations

$$e = k_m(h' - h'_s)$$

$$p' = k_c \cdot e$$

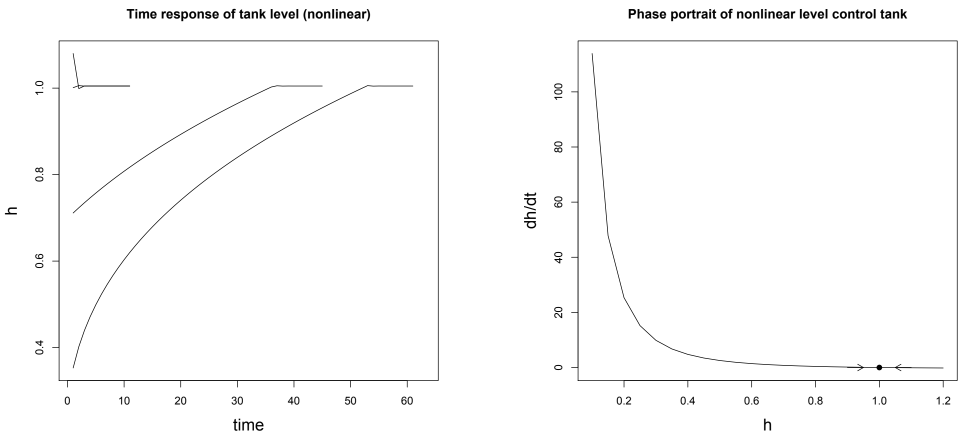
$$F_o = k_v \cdot p'$$

The system's dynamical model [Ogunnaike and Ray, 1994] is

$$\begin{aligned} A &= \pi\left(\frac{Rh}{H}\right)^2 \\ \frac{dh}{dt} &= \frac{F_i - F_o}{A} \\ &= \frac{F_i - k_v k_c k_m (h - h_s)}{A} \\ &= \frac{\alpha}{h^2}(F_i + k_v k_c k_m h_s) - \frac{k_v k_c k_m \alpha}{h}, \end{aligned}$$

where $\alpha = \frac{H^2}{\pi R^2}$, $k_m = 0.5$, $k_c = 4$, $k_v = 1.03$, $H = 1.2$, $h_s = 1$ and $R = 0.866$ (constants are chosen to match the linear level control tank example). The time response of h is shown in Figure 5.6(a). 4 sets of different initial conditions all settle down at the set-point level, as expected. The phase portrait $\dot{h}$ versus h, depicted in Figure 5.6(b), shows the change of height reaches zero while actual height is at the set-point. Apparently, the phase portrait shows a nonlinear behavior. The fixed point can be easily identified. The emergence of the level control behavior is the behavior where a continuum of phase volume reduces to a curve and a point. Individual components do not have full knowledge about this outcome, but contribute towards it.

Classical dynamics explains what emergent behavior is. As we have seen, both linear and nonlinear dynamics lead to emergent behaviors, but the dynamics itself does not explain how the emergent behavior emerges. Answering this question requires the understanding of teleodynamics. Therefore, it is important to clarify which question regarding emergence we are trying to answer. Even though the emergent behaviors in the first two examples seem trivial and are usually taken for granted, these systems, however, give us insights about emergence in simple dynamical systems which can be used as fundamental building blocks towards the understanding of more complex systems. In the next example, we will examine a system at higher levels in the hierarchy.



(a) (b)

Figure 5.6: The behavior of the nonlinear level control tank system

5.5.3 The Bank-Dealer System

So far, we have discussed simple engineered systems that are building blocks of a sociotechnical system. Now, let us consider the bank-dealer system, depicted in Figure 3.3. It is a complex system consisting of the financial market, a bank-dealer, a hedge fund as market participants. The bank-dealer system has been well explained Chapter 3.4. This system is a typical example of the market view layer shown in Figure 2.1.

The teleodynamics of this system is hardly modeled quantitatively, rather, it is easier to describe the teleodynamics using the SDG causal model. Two loops in the graph identify the fire sale scenario, shown in Table 3.2. The fire sale occurs when there is a disruption to the system that forces a hedge fund to sell positions. As depicted in Figure 3.5, this disruption can occur through three channels: a price drop and resulting drop in asset value, an increase in the margin rate that leads to a margin call from the prime broker, or a drop in the loan capacity of the prime broker. As the hedge fund reduces its assets, prices drop, again, leading to a second (and subsequent) round of feedback making the situation worse in every subsequent iteration. The first loop shows a price shock increasing the leverage of the hedge fund. The hedge fund then reduces its holdings in order to reduce its leverage, and this drops prices. The second loop has the same effect, drop in prices increases leverage, which in turn leads to a drop in the quantity held by the hedge fund, but the effect, in this case, works its way through the trading desk. The quantity sold by the hedge fund raises the quantity held by the trading desk, increasing its leverage. This, in turn, leads the trading desk to sell into the market, with the result again being a further drop in prices.

A bank-dealer system consists of following objects,

$$\begin{aligned} SY = \{&\text{money market (MM)},\ \text{bank-dealer market (BDM)},\\ &\text{trading desk (TD)},\ \text{finance desk (FD)},\ \text{prime broker (PB)},\ \text{hedge fund (HF)}\}. \end{aligned}$$

The attributes of each object are listed:

$$\begin{aligned} A_{\text{MM}} &= \{\chi, c, F\} \\ A_{\text{BDM}} &= \{p\} \\ A_{\text{TD}} &= \{\lambda, \lambda_{sp}, \epsilon, q\} \\ A_{\text{FD}} &= \{c, V\} \\ A_{\text{PB}} &= \{c, V, \chi\} \\ A_{\text{HF}} &= \{l, q, \lambda\} \end{aligned}$$

where χ is margin rate, c is collateral in dollar, F is funding in dollar, V is funding capacity in dollar, λ is leverage ratio, q represents quantity of shares, l is loan in dollar, and ϵ is the difference between real leverage and target leverage. They form the attribute class A,

$$A = \{A_{\text{MM}}, A_{\text{BDM}}, A_{\text{TD}}, A_{\text{FD}}, A_{\text{PB}}, A_{\text{HF}}\}.$$

These attributes can be quantitatively characterized by values in $\mathbb{R}$. The object states, therefore, are

$$s_{\text{MM}} = \{v_\chi, v_c, v_F\}$$
$$s_{\text{BDM}} = \{v_p\}$$
$$s_{\text{TD}} = \{v_\lambda, v_{\lambda,sp}, v_\epsilon, v_q\}$$
$$s_{\text{FD}} = \{v_c, v_V\}$$
$$s_{\text{PB}} = \{v_\chi, v_c, v_V\}$$
$$s_{\text{HF}} = \{v_l, v_q, v_\lambda\}$$

The jth system state is

$$S_j = \{s_{\text{MM}},\ s_{\text{BDM}},\ s_{\text{TD}},\ s_{\text{FD}},\ s_{\text{PB}},\ s_{\text{HF}}\}.$$

Hence, the phase space of the bank-dealer system is

$$\mathbb{S} = \bigcup S_j, \forall j.$$

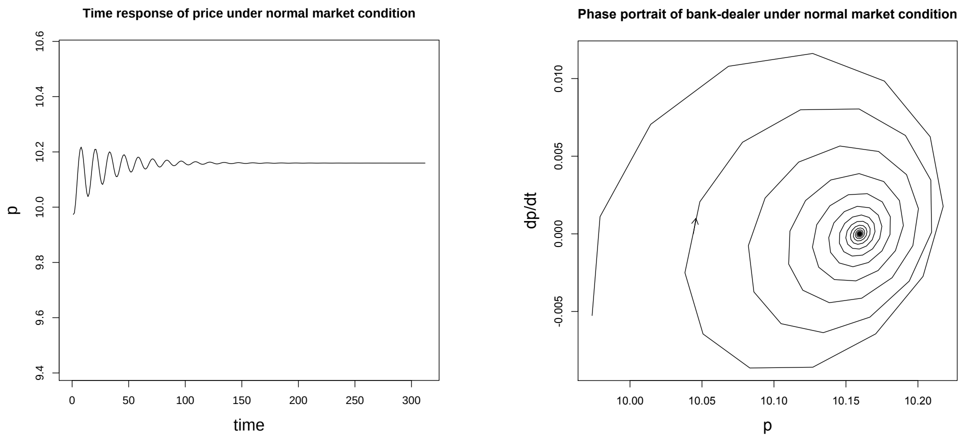
In this case, it is a high-dimensional space, where every attribute is an axis.

The teleodynamics can be further explained by the semi-quantitative analysis presented in Chapter 3.5, where the equations demonstrate the functions of objects.

5.5.3.1 Normal Market Condition

In this example, we demonstrate that it is really goals that affect system dynamics, hence, result different emergent behaviors.

Under the normal market condition, market participants have a goal to make profit. Price stabilizes after several trading iterations, as shown in Figure 5.7(a), because market participants are confident about the market, hence, will buy at low and sell at high. As a consequence, the price is eventually stabilized. Price stabilization is a system-level behavior. One cannot predict when and at what price the market will stabilize. It reflects the stochastic nature of the financial market. So the market behavior, depicted in Figure 5.7(b), is emergent. However, price is not always stabilized. Different market prospects could lead to very different teleodynamics, thus, change the market behavior dramatically.



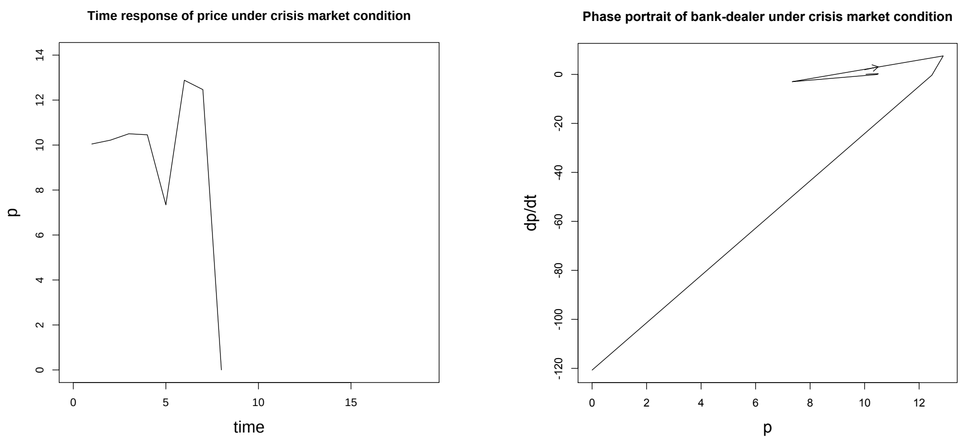
(a) (b)

Figure 5.7: The behavior of the bank-dealer system under normal condition

5.5.3.2 Crisis Condition

When most market participants are pessimistic about the market, they lose confidence, therefore, are willing to sell rather than to buy. The crisis teleodynamics could result in a price drop depicted in Figure 5.8(a). In this situation, a new phase space pattern, depicted in Figure 5.8(b), appears. It shows an opposite direction compared with the behavior shown in Figure 5.7(b). Individual market participants, such as the prime broker and the hedge fund, assess market information and make their decisions independently. Their actions would further impact to the market prospects. When the market prospects change, teleodynamics changes as indicated by the different "weight" terms in Equation (3.3) (0.1 in normal market condition and 2 in crisis condition).

Each of the units acts to maintain their stability. The prime broker is keeping its loans within bounds given its collateral; the hedge fund is maintaining a target level of leverage to control its risk, and the trading desk is governing its inventory level through an outflow if its market making activities increases its inventory above a target level. Their functions are the same. Yet the stabilizing activities at the local level still lead to instability at the global level. This underscores a central point in the functioning of the financial system, namely that it can exhibit global instability even in the face of each unit acting to control its risk.



(a) (b)

Figure 5.8: The behavior of the bank-dealer system under crisis condition

Different market prospects are the reason why *the stabilizing activities of objects still lead to the instability of the entire system.* When market participants change their goals, from adventurous to conservative, the market's teleodynamics changes consequently. It leads to different behaviors of the market.

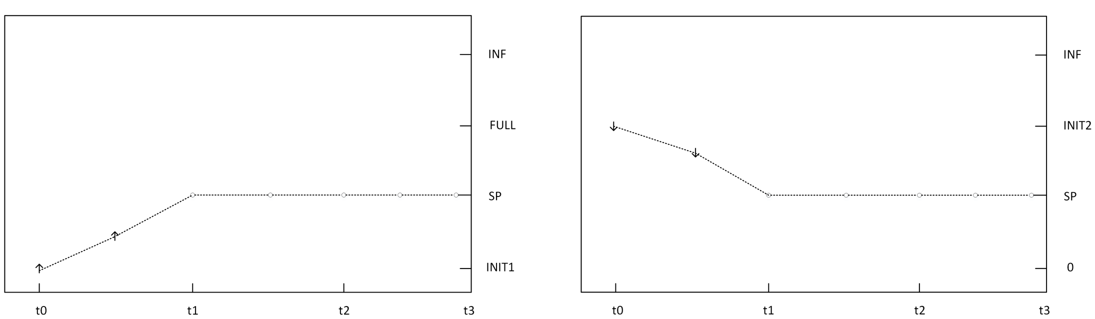
Market behaviors are unpredictable and emergent. Even though one may know the dynamical mechanisms of the market (i.e., the functions of every entity in the market), one cannot predict the behavior because the aggregate effect of the market prospects (i.e., the weight terms in Equation (3.3)) is unknown to individual market participant. Classical dynamics cannot capture the the importance of the market prospects, whereas teleodynamics emphasizes the critical role of goals in the dynamical behavior, therefore, is suitable to study emergence.

5.6 QSIM Comparison

QSIM is a qualitative reasoning algorithm developed by Kuipers [Dalle Molle *et al.*, 1988; Kuipers, 1986]. The purpose of QSIM is to explain system behavior from the physical descriptions, even if the description is incomplete. It starts from a set of constraints and produces all the possible future states that are consistent with the description. The qualitative states are represented as landmark values and direction of change. Then possible behaviors can be visualized as graphs. QSIM models a system behavior as a sequence of states constituting a path from the initial state to the final state [Dalle Molle *et al.*, 1988]. Moreover, QSIM is able to construct qualitative phase space to depict dynamical behaviors [Lee and Kuipers, 1993].

Our work is similar to QSIM in several aspects. Both works focus on system dynamics. Phase space plays an important role in explaining system behaviors. A path of states is used to delineate a behavior. QSIM aims to qualitatively reason a system's behavior given only partial information. The essence of QSIM is to construct Qualitative Differential Equations (QDEs) and solve them to get system's qualitative behavior. However, our study is not interested in how to obtain the dynamics. Instead, we focus on explaining emergent phenomena via teleodynamics. The examples presented in Section 5.5 have dynamics as differential equations or casual relationships. System's teleodynamics can also be given as QDEs.

If we construct QDEs for the level control tank system (Section 5.5) and plot the qualitative behaviors of both the "starting low" and the "starting high" scenarios (details about QSIM model construction can be found in Appendix D), as shown in Figure 5.9(a) and Figure 5.9(b), we find the two scenarios reach the same final state, i.e., the set point, as expected.



(a) (b)

Figure 5.9: Qualitative behavior of the linear level control tank system

We can also plot the qualitative phase portrait (Figure 5.10) to show that the system settles down at the set point. It confirms the behavior we obtained in Section 5.5.

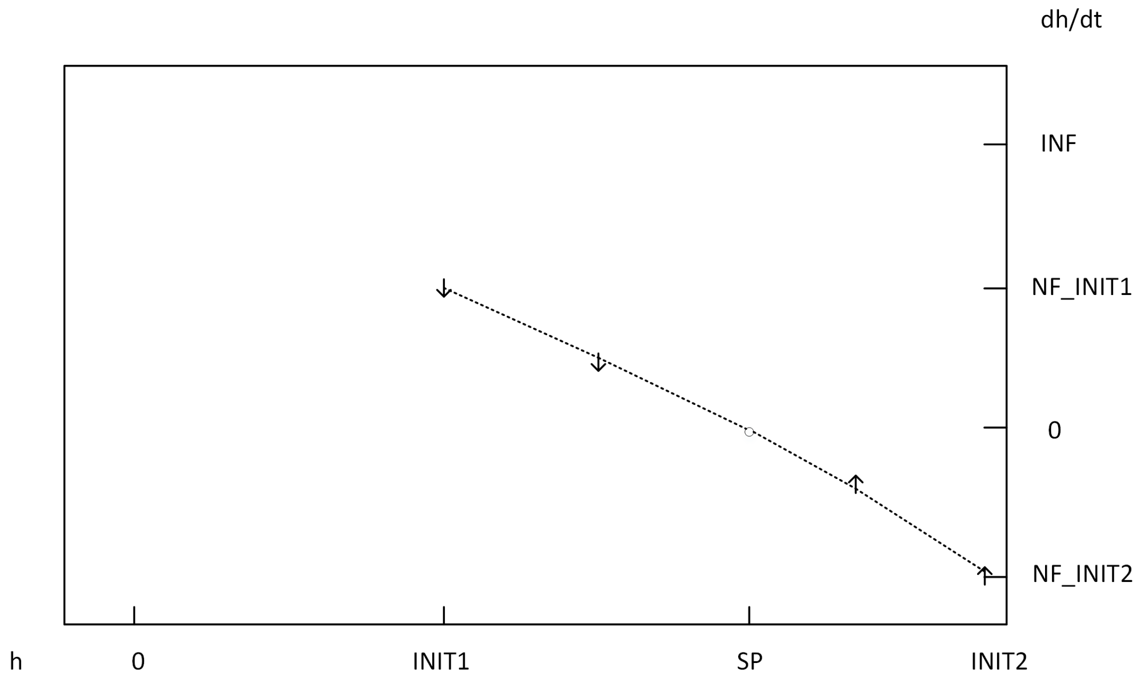


Figure 5.10: Qualitative phase portrait

5.7 Chapter Conclusion

In this chapter, we illustrate emergent behaviors of sociotechnical systems by studying teleodynamics. A formal representation is developed to model the teleodynamics of sociotechnical systems at any level. It describes a sociotechnical system in terms of classes and sets, and system behaviors in terms of functions and states. Examples show systems' control behaviors in the phase space as "the whole more than the sum of parts." Phase space trajectory illustrates the transition of system states, thus, delineates the evolution of a system. Every point in the phase space represents a micro-state. The trajectory cannot be induced from an individual micro-state. As a result, we answer the question "how simple individual components of a system interact to result in a system behavior that cannot be explained by any components alone."

It is important to recognize the difference between teleodynamics and classical dynamics.

Classical dynamics studies the evolution of a system. It does not care about the part-whole relationship. As a result, classical dynamics is able to explain what emergent behavior is, however, unable to answer how the behavior emerges. In contrast, teleodynamics concerns both teleology and dynamics. It demonstrates system's part-whole relationship using teleology and complex behaviors using dynamics, hence, uncovers the mystery of emergence.

Chemical engineers study the complex dynamics of chemical processes using control theory, but rarely think about its complexity science implications. We demonstrate that a control behavior is in fact an emergent behavior, hence, bridge the knowledge gaps between chemical engineering and complexity science.

Chapter 6

Conclusion Remarks

> The road ahead will be long, I shall search.
>
> Qu Yuan

To ensure the safe operation and production of complex sociotechnical systems, we need to model and analyze systemic risk. Traditional emphasis of chemical engineering risk analysis is on equipment and processes. However, systemic risk management studies not only equipment and processes but also human activities. This means classical quantitative approaches are no longer satisfactory. It is critical to model different kinds of knowledge of a sociotechnical system.

In this thesis, we develop a new knowledge modeling paradigm that goes beyond traditional risk modeling in chemical plants. Specifically, we develop the TeCSMART framework to model system knowledge, We use SDG to model cause-and-effect knowledge and ontology to model heuristic knowledge. We study system's teleodynamics to answer the question "how simple individual components interact to result in a system behavior that cannot be explained by the behavior of just the individual components alone."

6.1 The Roles of Teleology, Feedback, and Emergence

Our study emphasizes the roles of teleology, feedback, and emergence in modeling systemic risk. A teleological framework is established to model sociotechnical system as a whole by integrating both social elements and technical elements via the goal-driven activities. The framework models system knowledge to systematically analyze risk associated with different levels of sociotechnical systems. Teleology also helps develop an ontological document knowledge model, which supports public health decision making during EID emergencies.

Feedback is widely observed in complex dynamical systems. A positive feedback loop usually indicates a run-away situation. By modeling system's cause-and-effect knowledge, we can identify positive feedback loops in a complex financial network. These feedback loops explain the hidden instability of a sociotechnical system.

Moreover, emergent behavior is a result of the aggregate effect of sociotechnical system's dynamic, goal-driven activities in the multi-layered hierarchy. The underlying part-whole relationship can be illustrated in the phase space. Teleodynamics integrates teleology with system dynamics, therefore, explains how systemic risk emerges in complex sociotechnical systems.

6.2 Significance of the Work

Our work extends traditional risk modeling in chemical engineering by introducing various knowledge modeling paradigms for different levels of a sociotechnical system.

By carrying out a comparative analysis of 13 major systemic events, we systematically classify failures into five categories and develop a teleological modeling framework to capture system knowledge. Even though every systemic failure happens in a unique manner, and is not an exact replica of a past event, we show that the underlying failure mechanism can be traced back to similar patterns associated with other events through the teleological framework.

We identify that a cause-and-effect knowledge model can add the critical capabilities missing in the current network-based approaches. It reveals the hidden instability and failure mechanisms via feedback loops in SDGs. It can highlight, and help us monitor, dynamics such as fire sales and funding runs, of a financial system where actions that are locally stabilizing – e.g., where a financial institution takes risk management actions without an understanding of the systemic implications – might cascade to globally destabilizing consequences.

The public health document ontology is the first attempt to store and model knowledge from public health documents in an ontology. It supports the reuse and management of public health knowledge for risk mitigation. It is useful for LMICs to make quick response during a public health emergency.

Our work connects complexity science with control theory by showing a control behavior as the whole that is more than the sum of parts. The control behaviors of individual financial entities are shown as the emergent behaviors of a complex financial system. This observation answers the question that "how simple individual components interact to result in a system behavior that cannot be explained by any components alone."

6.3 Future Directions

At this stage, there are some known limitations. First of all, the failure comparative analysis needs to be carried out manually, requiring tremendous human effort. The size of the ontology corpus is small because of the time consuming manual annotation process. Second, the financial network described in Chapter 3 is relatively simple. It does not take into account the contagion effect of multiple assets. Third, teleodynamics is demonstrated using simple examples, which only contain a small number of components. It is important to study how teleology affects the dynamics of a system, which has a very large number of components?

Future research should focus on improving the methods by addressing these existing issues. Automation is a necessary step. NLP based concept extraction, such as topic modeling, can reduce manual effort, hence, improve the scalability. A large scale SDG model needs to be built for a financial system with multiple classes of assets. The teleodynamics of systems with a large number of goal-driven agents needs to be studied.

6.4 Final Remarks

This thesis have studied systemic risk in complex sociotechnical systems via the role of teleology, feedback, and emergence. It extends the scope of complex system modeling from differential equations to system knowledge, cause-and-effect knowledge, heuristic knowledge, and teleodynamical knowledge. As we have argued in Chapter 1, systemic risk modeling should go beyond modeling mechanical activities. Instead, it is critical to model different types of knowledge in sociotechnical systems.

Bibliography

[Acemoglu *et al.*, 2015] Daron Acemoglu, Asuman Ozdaglar, and Alireza Tahbaz-Salehi. Systemic risk and stability in financial networks. *The American Economic Review*, 105(2):564–608, 2015.

[Adrian and Shin, 2014] Tobias Adrian and Hyun Song Shin. Procyclical leverage and value-at-risk. *Review of Financial Studies*, 27(2):373–403, 2014.

[Amaral and Ottino, 2004] Luis AN Amaral and Julio M Ottino. Complex networks. *The European Physical Journal B-Condensed Matter and Complex Systems*, 38(2):147–162, 2004.

[Apostolakis, 2004] George E Apostolakis. How useful is quantitative risk assessment? *Risk analysis*, 24(3):515–520, 2004.

[Ashburner *et al.*, 2000] Michael Ashburner, Catherine A Ball, Judith A Blake, David Botstein, Heather Butler, J Michael Cherry, Allan P Davis, Kara Dolinski, and Selina S Dwight. Gene ontology: tool for the unification of biology. *Nature genetics*, 25(1):25–29, 2000.

[Asnis *et al.*, 2000] Deborah S Asnis, Rick Conetta, Alex A Teixeira, Glenn Waldman, and Barbara A Sampson. The west nile virus outbreak of 1999 in new york: the flushing hospital experience. *Clinical Infectious Diseases*, 30(3):413–418, 2000.

[Baker *et al.*, 2007] J. Baker, N. Leveson, F. Bowman, and S. Priest. The report of the bp us refineries independent safety review panel. Report, The B.P. U.S. Refineries Independent Safety Review Panel, 2007.

[Bar-Yam, 2004] Yaneer Bar-Yam. A mathematical theory of strong emergence using multiscale variety. *Complexity*, 9(6):15–24, 2004.

[Battiston *et al.*, 2013] S. Battiston, G. Caldarelli, C. P. Georg, R. May, and J. Stiglitz. Complex derivatives. *Nature Physics*, 9(3):123–125, 2013.

[Battiston *et al.*, 2016] Stefano Battiston, J Doyne Farmer, Andreas Flache, Diego Garlaschelli, Andrew G Haldane, Hans Heesterbeek, Cars Hommes, Carlo Jaeger, Robert May, and Marten Scheffer. Complexity theory and financial regulation. *Science*, 351(6275):818–819, 2016.

[Bedau, 1997] Mark A Bedau. Weak emergence. *Noûs*, 31(s11):375–399, 1997.

[Bedau, 2008] Mark A Bedau. Is weak emergence just in the mind? *Minds and Machines*, 18(4):443–459, 2008.

[Bequette and Bequette, 1998] B Wayne Bequette and Wayne B Bequette. *Process dynamics: modeling, analysis, and simulation.* Prentice Hall PTR Upper Saddle River, NJ, 1998.

[Bialek *et al.*, 2012] William Bialek, Andrea Cavagna, Irene Giardina, Thierry Mora, Edmondo Silvestri, Massimiliano Viale, and Aleksandra M Walczak. Statistical mechanics for natural flocks of birds. *Proceedings of the National Academy of Sciences*, 109(13):4786–4791, 2012.

[Blackburn, 2008] Robin Blackburn. The subprime crisis, March 2008.

[Blinder, 2016] Alan Blinder. Donald blankenship sentenced to a year in prison in mine safety case, April 6 2016.

[Bloom, 2002] Bernard S Bloom. Crossing the quality chasm: a new health system for the 21st century. *JAMA: The Journal of the American Medical Association*, 287(5):646–647, 2002.

[Board, 2003] CAI Board. Columbia accident investigation board report. *Vol. 1*, I(August), 2003.

[Bonabeau and Dessalles, 1997] Eric Bonabeau and Jean-Louis Dessalles. Detection and emergence. *Intellectica*, 25(2):85–94, 1997.

[Brank *et al.*, 2005] Janez Brank, Marko Grobelnik, and Dunja Mladeni. A survey of ontology evaluation techniques. In *In In Proceedings of the Conference on Data Mining and Data Warehouses (SiKDD 2005)*, 2005.

[Browning, 1993] J. B. Browning. Union carbide: Disaster at bhopal. *on Managing under Siege. Detroit (MI):* , pages 1–15, 1993.

[Brunnermeier and Pedersen, 2009] Markus K Brunnermeier and Lasse Heje Pedersen. Market liquidity and funding liquidity. *Review of Financial studies*, 22(6):2201–2238, 2009.

[Bure *et al.*, 2012] Vladimr Bure, Tereza Otenkov, Pavel ech, and Karel Anto. A proposal for a computer-based framework of support for public health in the management of biological incidents: the czech republic experience. *Perspectives in Public Health*, 132(6):292–298, 2012.

[Burton-Jones *et al.*, 2005] Andrew Burton-Jones, Veda C Storey, Vijayan Sugumaran, and Punit Ahluwalia. A semiotic metrics suite for assessing the quality of ontologies. *Data & Knowledge Engineering*, 55(1):84–102, 2005.

[Caldarelli *et al.*, 2013] G. Caldarelli, A. Chessa, A. Gabrielli, F. Pammolli, and M. Puliga. Reconstructing a credit network. *Nature Physics*, 9(3):125–126, 2013.

[Carley *et al.*, 2012] Kathleen M Carley, Dave Columbus, and Ariel Azoulay. Automap user's guide 2012. Report, CARNEGIE-MELLON UNIV PITTSBURGH PA INST OF SOFTWARE RESEARCH INTERNAT, 2012.

[Catanzaro and Buchanan, 2013] M. Catanzaro and M. Buchanan. Network opportunity. *Nature Physics*, 9(3):121–123, 2013.

[CCPS, 2005] CCPS. Building process safety culture: Tools to enhance process safety performance. Report, Center for Chemical Process Safety of the American Institute of Chemical Engineers, 2005.

[Centeno *et al.*, 2015] Miguel A Centeno, Manish Nag, Thayer S Patterson, Andrew Shaver, and A Jason Windawi. The emergence of global systemic risk. *Annual Review of Sociology*, 41:65–85, 2015.

[CERC, 2012] CERC. Report on the grid disturbance on 30th july 2012 and grid disturbance on 31st july 2012. Report, India Ministry of Power, 2012.

[Chalmers, 2008] David J Chalmers. *Varieties of emergence*, book section 11. Oxford University Press, 2008.

[Chittaro *et al.*, 1993] Luca Chittaro, Giovanni Guida, Carlo Tasso, and Elio Toppano. Functional and teleological knowledge in the multimodeling approach for reasoning about physical systems: a case study in diagnosis. *IEEE Transactions on Systems, Man, and Cybernetics*, 23(6):1718–1751, 1993.

[Chittaro, 1995] L Chittaro. Functional diagnosis and prescription of measurements using effort and flow variables. *IEE Proceedings-Control Theory and Applications*, 142(5):420–432, 1995.

[Cimiano, 2006] Philipp Cimiano. *Ontology Learning and Population from Text*. Springer US, 2006.

[Commission, 2011] Financial Crisis Inquiry Commission. The financial crisis inquiry report. *US Government Printing Office*, 2011.

[Corning, 2002] Peter A. Corning. The re-emergence of "emergence": A venerable concept in search of a theory. *Complexity*, 7(6):18–30, 2002.

[CSB, 2005] CSB. Investigation report refinery explosion and fire. Report, U.S. Chemical Safety and Hazard Investigation Board, 2005.

[Cucker and Smale, 2007] Felipe Cucker and Steve Smale. On the mathematics of emergence. *Japanese Journal of Mathematics*, 2(1):197–227, 2007.

[Cullen, 1993] W Douglas Cullen. The public inquiry into the piper alpha disaster. Report 0046-0702, U.K. Department of Energy, 1993.

[Dalle Molle *et al.*, 1988] DT Dalle Molle, BJ Kuipers, and TF Edgar. Qualitative modeling and simulation of dynamic systems. *Computers & Chemical Engineering*, 12(9-10):853–866, 1988.

[dAquin *et al.*, 2007] Mathieu dAquin, Anne Schlicht, Heiner Stuckenschmidt, and Marta Sabou. Ontology modularization for knowledge selection: Experiments and evaluations. In *International Conference on Database and Expert Systems Applications*, pages 874–883. Springer, 2007.

[De Bandt and Hartmann, 2000] Olivier De Bandt and Philipp Hartmann. Systemic risk: a survey. *European Central Bank Working Paper Series*, 2000.

[Deacon, 2011] Terrence W Deacon. *Incomplete nature: How mind emerged from matter*. WW Norton & Company, 2011.

[Deguet *et al.*, 2006] Joris Deguet, Yves Demazeau, and Laurent Magnin. Elements about the emergence issue: A survey of emergence definitions. *ComPlexUs*, 3(1-3):24–31, 2006.

[Diamond and Dybvig, 1983] Douglas W Diamond and Philip H Dybvig. Bank runs, deposit insurance, and liquidity. *Journal of political economy*, 91(3):401–419, 1983.

[Drilling, 2011] National Commission on the B. P. Deepwater Horizon Oil Spill Offshore Drilling. Deep water: The gulf oil disaster and the future of offshore drilling: Report to the president. Report 9780160873713, National Commission on the B. P. Deepwater Horizon Oil Spill Offshore Drilling, 2011.

[Duque-Ramos *et al.*, 2014] Astrid Duque-Ramos, Martin Boeker, Ludger Jansen, Stefan Schulz, Miguela Iniesta, and Jesualdo Toms Fernndez-Breis. Evaluating the good ontology design guideline (goodod) with the ontology quality requirements and evaluation method and metrics (oquare). *PloS one*, 9(8):e104463, 2014.

[Eilperin and Higham, 2010] Juliet Eilperin and Scott Higham. How the minerals management services partnership with industry led to failure, August 24, 2010 2010.

[Feistel, 2016] Rainer Feistel. Self-organisation of symbolic information. *Eur. Phys. J. Special Topics*, 226(2):207–228, 2016.

[Fine and Layton, 2001] Annie Fine and Marcelle Layton. Lessons from the west nile viral encephalitis outbreak in new york city, 1999: Implications for bioterrorism preparedness. *Infectious Diseases in Clinical Practice*, 10(4):229, 2001.

[Fineberg, 2014] Harvey V Fineberg. Pandemic preparedness and responselessons from the h1n1 influenza of 2009. *New England Journal of Medicine*, 370(14):1335–1342, 2014.

[Force, 2004] US-Canada Power System Outage Task Force. Final report on the august 14, 2003 blackout in the united states and canada. Report, US-Canada Power System Outage Task Force, 2004.

[Fostel and Geanakoplos, 2008] Ana Fostel and John Geanakoplos. Leverage cycles and the anxious economy. *The American Economic Review*, 98(4):1211–1244, 2008.

[Fouque and Langsam, 2013] Jean-Pierre Fouque and Joseph A Langsam. *Handbook on systemic risk*. Cambridge University Press, 2013.

[Freixas *et al.*, 2000] Xavier Freixas, Bruno M Parigi, and Jean-Charles Rochet. Systemic risk, interbank relations, and liquidity provision by the central bank. *Journal of money, credit and banking*, pages 611–638, 2000.

[Gai and Kapadia, 2010] Prasanna Gai and Sujit Kapadia. Contagion in financial networks. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, page rspa20090410. The Royal Society, 2010.

[Garvey, 2008] Paul R Garvey. *Analytical methods for risk management: A systems engineering perspective*. CRC Press, 2008.

[Gertler, 1991] Janos Gertler. Analytical redundancy methods in fault detection and isolation. In *Preprints of IFAC/IMACS Symposium on Fault Detection, Supervision and Safety for Technical Processes SAFEPROCESS91*, pages 9–21, 1991.

[Gertler, 1993] Janos J Gertler. Residual generation in model-based fault detection and isolation. *Control theory and advanced technology*, 9:259–285, 1993.

[Ginsborg, 2014] Hannah Ginsborg. *Oughts Without Intentions: A Kantian Perspective on Biological Teleology.* Kant's Theory of Biology. Walter De Gruyter, Berlin/New York, 2014.

[Goldstein, 1999] Jeffrey Goldstein. Emergence as a construct: History and issues. *Emergence*, 1(1):49–72, 1999.

[Gorton, 2010] Gary B Gorton. *Slapped in the Face by the Invisible Hand: Banking and the Panic of 2007.* Oxford University Press, New York, 2010.

[Government, 2011] U.S. Government. Public health service, 2011.

[Grau *et al.*, 2007] Bernardo Cuenca Grau, Ian Horrocks, Yevgeny Kazakov, and Ulrike Sattler. A logical framework for modularity of ontologies. In *IJCAI*, pages 298–303, 2007.

[Grüninger and Fox, 1995] Michael Grüninger and Mark S Fox. Methodology for the design and evaluation of ontologies. In *Workshop on Basic Ontological Issues in Knowledge Sharing, IJCAI-95*, 1995.

[Hemelrijk and Hildenbrandt, 2011] Charlotte K Hemelrijk and Hanno Hildenbrandt. Some causes of the variable shape of flocks of birds. *PloS one*, 6(8):e22479, 2011.

[Heussen and Lind, 2009] Kai Heussen and Morten Lind. Decomposing objectives and functions in power system operation and control. In *Sustainable Alternative Energy (SAE), 2009 IEEE PES/IAS Conference on*, pages 1–8. IEEE, 2009.

[Heussen and Lind, 2010a] Kai Heussen and Morten Lind. *Functional modeling of perspectives on the example of electric energy systems*, pages 254–260. Springer, 2010.

[Heussen and Lind, 2010b] Kai Heussen and Morten Lind. Representing causality and reasoning about controllability of multi-level flow-systems. In *Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on*, pages 1896–1903. IEEE, 2010.

[Higuchi, 2001] Koichi Higuchi. Kh coder, 2001.

[Hirsch *et al.*, 2012] Morris W Hirsch, Stephen Smale, and Robert L Devaney. *Differential equations, dynamical systems, and an introduction to chaos*. Academic press, 2012.

[Ho and Participants, 2014] Kendall Ho and Peter Wall Workshop Participants. Harnessing the social web for health and wellness: issues for research and knowledge translation. *Journal of medical Internet research*, 16(2), 2014.

[Hobbs and Pan, 2004] Jerry R Hobbs and Feng Pan. An ontology of time for the semantic web. *ACM Transactions on Asian Language Information Processing (TALIP)*, 3(1):66–85, 2004.

[Hoekstra *et al.*, 2007] Rinke Hoekstra, Joost Breuker, Marcello Di Bello, and Alexander Boer. The lkif core ontology of basic legal concepts. *LOAIT*, 321:43–63, 2007.

[Hollnagel, 2012] Erik Hollnagel. *FRAM, the functional resonance analysis method: modelling complex socio-technical systems*. Ashgate Publishing, Ltd., 2012.

[Hopkins, 2008] Andrew Hopkins. *Failure to learn: the BP Texas City refinery disaster*. CCH Australia Ltd, 2008.

[Jasanoff, 1994] Sheila Jasanoff. *Learning from disaster: risk management after Bhopal*. University of Pennsylvania Press, 1994.

[Jefferson, 1776] Thomas et al. Jefferson. United states declaration of independence, 1776.

[Jickling, 2011] Mark Jickling. Containing financial crisis. Report, Congressional Research Service, 2011.

[Johnson and Neave, 2007] Lewis D Johnson and Edwin H Neave. The subprime mortgage market: familiar lessons in a new context. *Management Research News*, 31(1):12–26, 2007.

[Kant and Pluhar, 1987] Immanuel Kant and Werner S Pluhar. *Critique of judgment*. Hackett Publishing, 1987.

[Kaplan and Garrick, 1981] Stanley Kaplan and B John Garrick. On the quantitative definition of risk. *Risk analysis*, 1(1):11–27, 1981.

[Keselman *et al.*, 2010] Alla Keselman, Graciela Rosemblat, Halil Kilicoglu, Marcelo Fiszman, Honglan Jin, Dongwook Shin, and Thomas C Rindflesch. Adapting semantic natural language processing technology to address information overload in influenza epidemic management. *Journal of the American Society for Information Science and Technology*, 61(12):2531–2543, 2010.

[Kleindorfer and Wind, 2009] Paul R Kleindorfer and Yoram Wind. *The network challenge: strategy, profit, and risk in an interlinked world*. Pearson Prentice Hall, 2009.

[Kopach-Konrad *et al.*, 2007] Renata Kopach-Konrad, Mark Lawley, Mike Criswell, Imran Hasan, Santanu Chakraborty, Joseph Pekny, and Bradley N Doebbeling. Applying systems engineering principles in improving health care delivery. *Journal of general internal medicine*, 22(3):431–437, 2007.

[Kopena and Regli, 2003] Joseph Kopena and William C Regli. Functional modeling of engineering designs for the semantic web. *IEEE Data Engineering Bulletin*, 26(4):55–61, 2003.

[Krugman, 2010] Paul Krugman. Berating the raters, April 25, 2010 2010.

[Kuba, 2012] M. Kuba. Owl 2 and swrl tutorial, 2012.

[Kuipers, 1986] Benjamin Kuipers. Qualitative simulation. *Artificial intelligence*, 29(3):289–338, 1986.

[Kunen, 2009] Kenneth Kunen. *The foundations of mathematics*. College Publications London, 2009.

[Kurokawa *et al.*, 2012] Kyoshi Kurokawa, K Ishibashi, K Oshima, H Sakiyama, M Sakurai, K Tanaka, M Tanaka, S Nomura, R Hachisuka, and Y Yokoyama. The official report of the fukushima nuclear accident independent investigation commission. Report, The Fukushima Nuclear Accident Independent Investigation Commission, 2012.

[LaPelle *et al.*, 2006] Nancy R LaPelle, Roger Luckmann, E Hatheway Simpson, and Elaine R Martin. Identifying strategies to improve access to credible and relevant information for public health professionals: a qualitative study. *BMC public health*, 6(1):1, 2006.

[Lapp and Powers, 1977] Steven A Lapp and Gary J Powers. Computer-aided synthesis of fault-trees. *IEEE Transactions on Reliability*, 1:2–13, 1977.

[Lee and Kuipers, 1993] Wood W Lee and Benjamin Kuipers. A qualitative method to construct phase portraits. In *AAAI*, pages 614–619, 1993.

[Lehar, 2005] Alfred Lehar. Measuring systemic risk: A risk management approach. *Journal of Banking & Finance*, 29(10):2577–2603, 2005.

[Leveson and Stephanopoulos, 2014] N. G. Leveson and G. Stephanopoulos. A system-theoretic, control-inspired view and approach to process safety. *Aiche Journal*, 60(1):2–14, 2014. 265CI Times Cited:2 Cited References Count:33.

[Leveson, 2004] N. Leveson. A new accident model for engineering safer systems. *Safety Science*, 42(4):237–270, 2004.

[Leveson, 2015] Nancy Leveson. A systems approach to risk management through leading safety indicators. *Reliability Engineering & System Safety*, 136:17–34, 2015.

[Lewes, 1877] George Henry Lewes. *Problems of life and mind.* Trübner & Company, 1877.

[Lewis, 2011] M. Lewis. *The Big Short: Inside the Doomsday Machine.* W. W. Norton, 2011.

[Li and Mackaness, 2015] Sen Li and William A Mackaness. A multi-agent-based, semantic-driven system for decision support in epidemic management. *Health informatics journal*, 21(3):195–208, 2015.

[Licata and Minati, 2016] Ignazio Licata and Gianfranco Minati. Emergence, computation and the freedom degree loss information principle in complex systems. *Foundations of Science*, pages 1–19, 2016.

[Lieberman *et al.*, 2007] Joshua Lieberman, Raj Singh, and Chris Goad. W3c geospatial ontologies, 2007.

[Lind, 1994] Morten Lind. Modeling goals and functions of complex industrial plants. *Applied Artificial Intelligence*, 8(2):259–283, 1994.

[Lind, 2005] Morten Lind. *Modeling Goals and Functions of Control and Safety Systems -theoretical Foundations and Extensions of MFM.* NKS Secretariat, 2005.

[Luo *et al.*, 2016] Yu Luo, Garud Iyengar, and Venkat Venkatasubramanian. Soft regulation with crowd recommendation: coordinating self-interested agents in sociotechnical systems under imperfect information. *PloS one*, 11(3):e0150343, 2016.

[MacGregor and Kourti, 1995] John F MacGregor and Theodora Kourti. Statistical process control of multivariate processes. *Control Engineering Practice*, 3(3):403–414, 1995.

[MacGregor *et al.*, 1991] John F MacGregor, Thomas E Marlin, James Kresta, and Bert Skagerberg. Multivariate statistical methods in process analysis and control. In *Proc. of Fourth Intl. Conf. On Chemical Process Control*, pages 665–672, 1991.

[MacGregor *et al.*, 1994] John F MacGregor, Christiane Jaeckle, Costas Kiparissides, and M Koutoudi. Process monitoring and diagnosis by multiblock pls methods. *AIChE Journal*, 40(5):826–838, 1994.

[Maedche and Staab, 2002] Alexander Maedche and Steffen Staab. Measuring similarity between ontologies. In *International Conference on Knowledge Engineering and Knowledge Management*, pages 251–263. Springer, 2002.

[Manson, 2001] Steven M Manson. Simplifying complexity: a review of complexity theory. *Geoforum*, 32(3):405–414, 2001.

[Mao and Bian, 2010] Liang Mao and Ling Bian. Spatialtemporal transmission of influenza and its health risks in an urbanized area. *Computers, Environment and Urban Systems*, 34(3):204–215, 2010.

[Marsh, 2009] Gerald E Marsh. The demystification of emergent behavior. *arXiv preprint arXiv:0907.1117*, 2009.

[Maurya *et al.*, 2003a] M. R. Maurya, R. Rengaswamy, and V. Venkatasubramanian. A systematic framework for the development and analysis of signed digraphs for chemical processes. 1. algorithms and analysis. *Industrial & Engineering Chemistry Research*, 42(20):4789–4810, 2003.

[Maurya *et al.*, 2003b] M. R. Maurya, R. Rengaswamy, and V. Venkatasubramanian. A systematic framework for the development and analysis of signed digraphs for chemical processes. 2. control loops and flowsheet analysis. *Industrial & Engineering Chemistry Research*, 42(20):4811–4827, 2003.

[Maurya *et al.*, 2004] Mano Ram Maurya, Raghunathan Rengaswamy, and Venkat Venkatasubramanian. Application of signed digraphs-based analysis for fault diagnosis of chemical process flowsheets. *Engineering Applications of Artificial Intelligence*, 17(5):501–518, 2004.

[McAteer *et al.*, 2011] J Davitt McAteer, K. Beall, J. Beck, and P. McGinley. Upper big branch: The april 5, 2010, explosion: a failure of basic coal mine safety practices: Report to the governor. Report, Governors Independent Investigation Panel, 2011.

[Millot, 2014] Patrick Millot. *Risk Management in Life Critical Systems*. John Wiley & Sons, 2014.

[MSNBC, 2010] MSNBC. Mine owner ran up serious violations, April 6, 2010 2010.

[Musen, 2015] Mark A Musen. The protg project: A look back and a look forward. *AI matters*, 1(4):4–12, 2015.

[Natarajan and Srinivasan, 2014] S. Natarajan and R. Srinivasan. Implementation of multi agents based system for process supervision in large-scale chemical plants. *Computers & Chemical Engineering*, 60:182–196, 2014.

[Neill, 2012] Daniel B Neill. New directions in artificial intelligence for public health surveillance. *IEEE Intelligent Systems*, 27(1):56–59, 2012.

[Newman, 1996] David V Newman. Emergence and strange attractors. *Philosophy of Science*, pages 245–261, 1996.

[Nolen *et al.*, 2005] Lexi Bambas Nolen, Paula Braveman, J Norberto W Dachs, Iris Delgado, Emmanuela Gakidou, Kath Moser, Liz Rolfe, Jeanette Vega, and Christina Zarowsky. Strengthening health information systems to address health equity challenges. *Bulletin of the World Health Organization*, 83(8):597–603, 2005.

[Nolte, 2010] David D Nolte. The tangled tale of phase space. *Physics today*, 63(4):33–38, 2010.

[O'Connor, 1994] Timothy O'Connor. Emergent properties. *American Philosophical Quarterly*, 31(2):91–104, 1994.

[Ogunnaike and Ray, 1994] Babatunde Ayodeji Ogunnaike and Willis Harmon Ray. *Process dynamics, modeling, and control*, volume 1. Oxford University Press New York, 1994.

[Olive *et al.*, 2006] Claire Olive, T Michael OConnor, and M Sam Mannan. Relationship of safety culture and process safety. *Journal of Hazardous Materials*, 130(1):133–140, 2006.

[Organization, 2005] World Health Organization. *International Health Regulations*. World Health Organization, 2005.

[Organization, 2006] World Health Organization. Sars: How a global epidemic was stopped. Report, World Health Organization, 2006.

[Organization, 2009a] World Health Organization. *Pandemic Influenza Preparedness and Response Guide*. World Health Organization, 2009.

[Organization, 2009b] World Health Organization. Who technical advice for case management of influenza a (h1n1) in air transport. Report, World Health Organization, 2009.

[Organization, 2010] World Health Organization. Protocol for assessing national surveillance and response capacities for the international health regulations, 2010.

[Organization, 2015] World Health Organization. Situation summary data published on 12 november 2015, 2015.

[Oshitani *et al.*, 2008] Hitoshi Oshitani, Taro Kamigaki, and Akira Suzuki. Major issues and challenges of influenza pandemic preparedness in developing countries. *Emerging infectious diseases*, 14(6):875, 2008.

[Ostfeld *et al.*, 2005] Richard S Ostfeld, Gregory E Glass, and Felicia Keesing. Spatial epidemiology: an emerging (or re-emerging) discipline. *Trends in ecology & evolution*, 20(6):328–336, 2005.

[Ottino, 2004] Julio M Ottino. Engineering complex systems. *Nature*, 427(6973):399–399, 2004.

[Paravantis, 2016] John A Paravantis. *From Game Theory to Complexity, Emergence and Agent-Based Modeling in World Politics*, pages 39–85. Springer, 2016.

[Parunak and VanderBok, 1997] H Van Dyke Parunak and Raymond S VanderBok. Managing emergent behavior in distributed control systems. *Ann Arbor*, 1001:48106, 1997.

[Pathria and Beale, 2011] R. K. Pathria and Paul D. Beale. *Statistical Mechanics*. Elsevier Science & Technology, 3 edition, 2011.

[Plotz, 2002] David Plotz. Play the enron blame game!, 2002.

[Polani, 2013] Daniel Polani. *Foundations and formalizations of self-organization*, pages 23–42. Springer, 2013.

[Prokopenko, 2008] Mikhail Prokopenko. *Advances in applied self-organizing systems*. Springer, 2008.

[Rakoff, 2014] Jed S Rakoff. The financial crisis: why have no high-level executives been prosecuted?, January 9, 2014 2014.

[Rao *et al.*, 2014] Rohini R Rao, Krishnamoorthi Makkithaya, and Neha Gupta. Ontology based semantic representation for public health data integration. In *Contemporary Computing and Informatics (IC3I), 2014 International Conference on*, pages 357–362. IEEE, 2014.

[Rasmussen, 1997] Jens Rasmussen. Risk management in a dynamic society: a modelling problem. *Safety Science*, 27(23):183–213, 1997.

[Representative and of, 1986] Committee on Science Representative and Technology House of. Investigation of the challenger accident. Report, U.S. Congress, October 29, 1986 1986.

[Revere *et al.*, 2007] Debra Revere, Anne M. Turner, Ann Madhavan, Neil Rambo, Paul F. Bugni, AnnMarie Kimball, and Sherrilynne S. Fuller. Understanding the information needs of public health practitioners: A literature review to inform design of an interactive digital knowledge management system. *Journal of Biomedical Informatics*, 40(4):410–421, 2007.

[Reynolds, 1987] Craig W Reynolds. Flocks, herds and schools: A distributed behavioral model. *ACM SIGGRAPH computer graphics*, 21(4):25–34, 1987.

[Riloff and Wiebe, 2003] Ellen Riloff and Janyce Wiebe. Learning extraction patterns for subjective expressions. In *Proceedings of the 2003 conference on Empirical methods in natural language processing*, pages 105–112. Association for Computational Linguistics, 2003.

[Russell *et al.*, 1995] Stuart Russell, Peter Norvig, and Artificial Intelligence. A modern approach. *Artificial Intelligence. Prentice-Hall, Egnlewood Cliffs*, 25:27, 1995.

[Saleh *et al.*, 2014] Joseph H. Saleh, Karen B. Marais, and Francesca M. Favar. System safety principles: A multidisciplinary engineering perspective. *Journal of Loss Prevention in the Process Industries*, 29:283–294, 2014.

[Schriml *et al.*, 2012] Lynn Marie Schriml, Cesar Arze, Suvarna Nadendla, Yu-Wei Wayne Chang, Mark Mazaitis, Victor Felix, Gang Feng, and Warren Alden Kibbe. Disease ontology: a backbone for disease semantic integration. *Nucleic acids research*, 40(D1):D940–D946, 2012.

[Schumer and Maloney, 2007] Charles E. Schumer and Carolyn B. Maloney. The subprime lending crisis: The economic impact on wealth, property values and tax revenues, and how we got here. Report, Joint Economic Committee, January 15 2007.

[Seborg *et al.*, 2011] Dale Seborg, Thomas F Edgar, and Duncan Mellichamp. *Process dynamics & control*. John Wiley & Sons, 2011.

[Seider *et al.*, 2009] Warren D Seider, Junior D Seader, and Daniel R Lewin. *Product & Process Design Principles: Synthesis, Analysis and Evaluation*. John Wiley & Sons, 2009.

[Services and Human, 2010] Department of Health Services and Human. Foreign quarantines: Etiological agents, hosts, and vectors, 2010.

[Services and Human, 2013] Department of Health Services and Human. Code of federal regulations, 2013.

[Shleifer and Vishny, 2011] Andrei Shleifer and Robert Vishny. Fire sales in finance and macroeconomics. *The Journal of Economic Perspectives*, 25(1):29–48, 2011.

[Srinivasan and Venkatasubramanian, 1996] R. Srinivasan and V. Venkatasubramanian. Petri net-digraph models for automating hazop analysis of batch process plants. *Computers & Chemical Engineering*, 20(96):S719–S725, 1996.

[Srinivasan and Venkatasubramanian, 1998a] R. Srinivasan and V. Venkatasubramanian. Automating hazop analysis of batch chemical plants: Part i. the knowledge representation framework. *Computers & Chemical Engineering*, 22(9):1345–1355, 1998.

[Srinivasan and Venkatasubramanian, 1998b] R. Srinivasan and V. Venkatasubramanian. Automating hazop analysis of batch chemical plants: Part ii. algorithms and application. *Computers & Chemical Engineering*, 22(9):1357–1370, 1998.

[Srinivasan and Venkatasubramanian, 1998c] R. Srinivasan and V. Venkatasubramanian. Multi-perspective models for process hazards analysis of large scale chemical processes. *Computers & Chemical Engineering*, 22(98):S961–S964, 1998.

[Staab and Studer, 2013] Steffen Staab and Rudi Studer. *Handbook on ontologies*. Springer Science & Business Media, 2013.

[Steels, 1991] Luc Steels. Towards a theory of emergent functionality. In *The first international conference on simulation of adaptive behavior on From animals to animats*, pages 451–461. MIT Press, 1991.

[Steinzor, 2014] Rena Steinzor. *Why Not Jail?: Industrial Catastrophes, Corporate Malfeasance, and Government Inaction*. Cambridge University Press, 2014.

[Stephanopoulos, 1984] George Stephanopoulos. *Chemical process control: an introduction to theory and practice*. Prentice Hall, Inc., 1984.

[Stoto *et al.*, 2013] Michael A Stoto, Christopher Nelson, Melissa A Higdon, John Kraemer, Lisle Hites, and Christa-Marie Singleton. Lessons about the state and local public health system response to the 2009 h1n1 pandemic: a workshop summary. *Journal of Public Health Management and Practice*, 19(5):428–435, 2013.

[Strogatz, 2014] Steven H Strogatz. *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. Westview press, 2014.

[Szebehely, 2012] Victory Szebehely. *Theory of orbit: The restricted problem of three Bodies*. Elsevier, 2012.

[Tao *et al.*, 2010] Cui Tao, Wei-Qi Wei, Harold R Solbrig, Guergana Savova, and Christopher G Chute. Cntro: a semantic web ontology for temporal relation inferencing in clinical narratives. In *AMIA annual symposium proceedings*, page 787. American Medical Informatics Association, 2010.

[ThinkReliability, 2008] ThinkReliability. The cause map of northeast blackout 0f 2003, 2008 2008.

[Thomas *et al.*, 2010] Pierre Thomas, Jack Jones, Lisa A. Cloherty, and Jason Ryan. Bp's dismal safety record, May 27, 2010 2010.

[Tomori, 2015] Oyewale Tomori. Will africas future epidemic ride on forgotten lessons from the ebola epidemic? *BMC medicine*, 13(1):116, 2015.

[Trinquart and Galea, 2015] Ludovic Trinquart and Sandro Galea. Mapping epidemiology's past to inform its future: Metaknowledge analysis of epidemiologic topics in leading journals, 19742013. *American journal of epidemiology*, 182(2):93–104, 2015.

[Trochim *et al.*, 2006] W. M. Trochim, D. A. Cabrera, B. Milstein, R. S. Gallagher, and S. J. Leischow. Practical challenges of systems thinking and modeling in public health. *Am J Public Health*, 96(3):538–46, 2006. Trochim, William M Cabrera, Derek A Milstein, Bobby Gallagher, Richard S Leischow, Scott J eng 2006/02/02 09:00 Am J Public Health. 2006 Mar;96(3):538-46. Epub 2006 Jan 31.

[UKDOH, 2010] UKDOH. Learning the lessons from the h1n1 vaccination campaign for health care workers. Report, U.K. Department of Health, 2010.

[Union, 2010] Council of the European Union. Council conclusions on lessons learned from the a/h1n1 pandemic - health security in the european union. Report, Council of the European Union, 2010.

[Urbina, 2010] Ian Urbina. Inspector general's inquiry faults regulators, May 24 2010.

[Vaidhyanathan and Venkatasubramanian, 1995] R. Vaidhyanathan and V. Venkatasubramanian. Digraph-based models for automated hazop analysis. *Reliability Engineering & System Safety*, 50(1):33–49, 1995.

[Vaidhyanathan and Venkatasubramanian, 1996] R. Vaidhyanathan and V. Venkatasubramanian. A semi-quantitative reasoning methodology for filtering and ranking hazop results in hazopexpert. *Reliability Engineering & System Safety*, 53(2):185–203, 1996.

[Venkatasubramanian and Chan, 1989] Venkat Venkatasubramanian and King Chan. A neural network methodology for process fault diagnosis. *AIChE Journal*, 35(12):1993–2002, 1989.

[Venkatasubramanian and Rengaswamy, 2003] Venkat Venkatasubramanian and Raghunathan Rengaswamy. A review of process fault detection and diagnosis: Part i: Quantitative model-based methods. *Computers & chemical* , 27:293–311, 2003.

[Venkatasubramanian and Vaidhyanathan, 1994] V. Venkatasubramanian and R. Vaidhyanathan. A knowledge-based framework for automating hazop analysis. *Aiche Journal*, 40(3):496–505, 1994.

[Venkatasubramanian and Zhang, 2016] Venkat Venkatasubramanian and Zhizun Zhang. Tecsmart: A hierarchical framework for modeling and analyzing systemic risk in sociotechnical systems. *AIChE Journal*, 2016.

[Venkatasubramanian *et al.*, 2000] V. Venkatasubramanian, J. S. Zhao, and S. Viswanathan. Intelligent systems for hazop analysis of complex process plants. *Computers & Chemical Engineering*, 24(9-10):2291–2302, 2000.

[Venkatasubramanian *et al.*, 2003a] V. Venkatasubramanian, R. Rengaswamy, S. N. Kavuri, and K. Yin. A review of process fault detection and diagnosis part iii: Process history based methods. *Computers & Chemical Engineering*, 27(3):327–346, 2003.

[Venkatasubramanian *et al.*, 2003b] Venkat Venkatasubramanian, Raghunathan Rengaswamy, Surya N Kavuri, and Kewen Yin. A review of process fault detection and diagnosis: Part iii: Process history based methods. *Computers & chemical engineering*, 27(3):327–346, 2003.

[Venkatasubramanian *et al.*, 2006] Venkat Venkatasubramanian, Chunhua Zhao, Girish Joglekar, Ankur Jain, Leaelaf Hailemariam, Pradeep Suresh, Pavankumar Akkisetty, Ken Morris, and Gintaras V Reklaitis. Ontological informatics infrastructure for pharmaceutical product development and manufacturing. *Computers & chemical engineering*, 30(10):1482–1496, 2006.

[Venkatasubramanian, 2007] V. Venkatasubramanian. A theory of design of complex teleological systems: Unifying the darwinian and boltzmannian perspectives. *Complexity*, 12(3):14–21, 2007.

[Venkatasubramanian, 2009] Venkat Venkatasubramanian. Drowning in data: Informatics and modeling challenges in a data-rich networked world. *AIChE Journal*, 55(1):2–8, 2009.

[Venkatasubramanian, 2011] V. Venkatasubramanian. Systemic failures: Challenges and opportunities in risk management in complex systems. *Aiche Journal*, 57(1):2–9, 2011.

[Venkatasubramanian, 2017a] Venkat Venkatasubramanian. *How Much Inequality Is Fair?: Mathematical Principles of a Moral, Optimal, and Stable Capitalist Society*. Columbia University Press, 2017.

[Venkatasubramanian, 2017b] Venkat Venkatasubramanian. Statistical teleodynamics: Toward a theory of emergence. *Langmuir*, 2017.

[Viswanathan *et al.*, 1998a] S. Viswanathan, C. Johnsson, R. Srinivasan, V. Venkatasubramanian, and K. E. Arzen. Automating operating procedure synthesis for batch processes: Part i. knowledge representation and planning framework. *Computers & Chemical Engineering*, 22(11):1673–1685, 1998.

[Viswanathan *et al.*, 1998b] S. Viswanathan, C. Johnsson, R. Srinivasan, V. Venkatasubramanian, and K. E. Arzen. Automating operating procedure synthesis for batch processes: Part ii. implementation and application. *Computers & Chemical Engineering*, 22(11):1687–1698, 1998.

[Von Bertalanffy, 1968] Ludwig Von Bertalanffy. General systems theory. *New York*, 41973:40, 1968.

[Wang *et al.*, 2004] Xiao Hang Wang, D Qing Zhang, Tao Gu, and Hung Keng Pung. Ontology based context modeling and reasoning using owl. In *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, pages 18–22. Ieee, 2004.

[Watanabe *et al.*, 1989] Kajiro Watanabe, Ichiro Matsuura, Masahiro Abe, Makoto Kubota, and DM Himmelblau. Incipient fault diagnosis of chemical processes via artificial neural networks. *AIChE journal*, 35(11):1803–1812, 1989.

[Watanabe *et al.*, 1994] Kajiro Watanabe, Seiichi Hirota, Liya Hou, and DM Himmelblau. Diagnosis of multiple simultaneous fault via hierarchical artificial neural networks. *AIChE Journal*, 40(5):839–848, 1994.

[Wolfram, 1984] Stephen Wolfram. Cellular automata as models of complexity. *Nature*, 311(5985):419–424, 1984.

[Yaylali *et al.*, 2014] Emine Yaylali, Julie Simmons Ivy, and Javad Taheri. Systems engineering methods for enhancing the value stream in public health preparedness: the role of markov models, simulation, and optimization. *Public Health Reports*, 129(Suppl 4):145, 2014.

[Zhao *et al.*, 2005a] C. Zhao, M. Bhushan, and V. Venkatasubramanian. Phasuite: An automated hazop analysis tool for chemical processes part i knowledge engineering framework. *Process Safety and Environmental Protection*, 83(6):509–532, 2005.

[Zhao *et al.*, 2005b] C Zhao, M Bhushan, and V Venkatasubramanian. Phasuite: An automated hazop analysis tool for chemical processes: Part ii: Implementation and case study. *Process Safety and Environmental Protection*, 83(6):533–548, 2005.

Appendix A

TeCSMART Failure Analysis Tables

A.1 Bhopal Gas Tragedy

TeCSMART				
			Bhopal Disaster	
View 7	Societal View	*Time Scale*	Decades	
		Agents	India society	
		Key Failures	*Key Failure*	*Specific Examples*
			4.1 Communication failure with external entities	The community living near the plant had never been told of the significance of the danger alarm. The danger alarm had sounded several times accidentally in the past and resembled a nearby factory's shift change hooter. Many people on hearing the alarm after the gas leak actually rushed towards the factory. The community had never been informed about the dangers posed by the materials used in the plant. Several neighbours thought that the plant made medicines.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	India Government	
		Key Failures	*Key Failure*	*Specific Examples*
			3.2 Late response	Amnesty International is not aware of any information that indicates that either the central or the state government took or asked UCIL/UCC to take any specific steps to assess the risk to local communities or the environment, or to review or augment safety mechanisms.
			2.1 Model failures	In 1984, just a few months before the fatal leak, the state government conferred legal titles to a large number of houses that had come up close to the perimeter of the plant.
			2.2 Inadequate or incorrect local decisions	The liberalization of trade and the deregulation and privatization of state functions have coincided with an expansion in the power of large transnational corporations. According to one source, the largest 300 firms control about 25% of the world's productive assets.288 The vast resources of many transnational corporations have enabled unscrupulous companies to abuse their power and influence.
				A number of pesticides and drugs banned or heavily restricted elsewhere are being knowingly imported or manufactured in India.
			1.3 Significant errors in monitoring	As well as an inadequate legislative framework and lack of institutional preparedness, the government appears also to have lacked the political will to discipline Union Carbide.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	state government of Madhya Pradesh, Industrial Safety and Health Department	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	The Indian government was obliged to ensure that UCC and UCIL complied with existing safety regulations in order to avoid gas leaks. However, government officials of Madhya Pradesh state failed to act effectively on numerous occasions when less serious but nonetheless alarming incidents had occurred.
			1.1 Failure to monitor	MIC was being transported from Bhopal to several locations in India without any regulations.
			1.2 Failure to monitor effectively	The Director of the Industrial Safety and Health Department in the state government of Madhya Pradesh had the primary responsibility for ensuring that the Bhopal plant took adequate steps to ensure occupational safety and to guard against possible risks from hazardous substances or processes. The Department's safety inspectors were responsible for inspecting the plant. Before 1984 the Department had recorded at least six accidents at the plant. Inspections following each of the accidents recorded recommendations or instructions, but the Department did not follow up the
			1.3 Significant errors in monitoring	There was only one corporate health and safety audit over the seven years of plant operations. No follow-up check was undertaken after 1982 even though conditions were becoming visibly worse, and local newspapers and politicians had raised alarm signals.
			5.3 Operating procedure failures	At the time of the accident the Factories Act of 1948 that governed health and safety regulations did not have any specific provisions to regulate or deal with hazardous technology and processes, nor was there any kind of legislation on environment protection.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 4	Market View	*Time Scale*	Months	
		Agents	multinational chemical industry	
		Key Failures	*Key Failure*	*Specific Examples*
			2.3 Inadequate or incorrect global decisions	Multinational corporations have repeatedly exported banned drugs and pesticides and even entire factories to the Third World.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.1: Bhopal Gas Tragedy failure analysis table part 1

TeCSMART				
			Bhopal Disaster	
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	UCC, UCIL	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	UCC, in its drive for cost cutting, had used pipes and valves made of inexpensive carbon steel instead of stainless steel, against its own safety rules.
			3.2 Late response	UCC management was aware of safety problems at the Bhopal plant for some time before December 1984, but no evidence showed that the Bhopal plant took actions regarding the warnings.
			1.1 Failure to monitor	The company never installed in Bhopal the computerized pressure/temperature sensing system, which it has used for several years in the US plant as a warning device. Maintenance and operational practices had sharply deteriorated. Chemical reactors, piping and valves were not purged, washed and aired before maintenance operations, which caused the death by phosgene in 1981. Lack of adequate spare parts meant that vital devices like pressure gauges were not functioning.
			2.5 Conflict of interest	Between the beginning of 1983 and the time of the disaster, a series of cost-cutting measures was implemented. Damaged or malfunctioning equipment was patched up rather than repaired, or replaced by sub-standard material.
				The only conclusion possible is that the Union Carbide did not care about safety, and, in a developing country, with inadequate government regulations and a relatively uninformed public, it was simply cheaper and more profitable to neglect.
			5.3 Operating procedure failures	No system to inform public authorities or the people living adjacent to the plant. No emergency plan shared with communities living adjacent to the plant; no system to disseminate information regarding emergency to the public with the exception of a loud siren.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	Bhopal plant	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Refrigeration unit had been turned off since June 1984.
				Personal protective gear and breathing air equipment not easily accessible, inadequate and of poor quality.
				The Bhopal plant's management gave little heed to safety and maintenance. Engineering control equipment had not been working for a long time before the December gas disaster, the result of an indiscriminate economy drive.
			2.4.3 Training failures	No one in Bhopal who had any idea of the chemistry of MIC. Engineers at the plant went by operating manuals only and did not know the plant design. Efforts to locate the original designers of the factory to learn more about the system had also failed.
				By 1983 the MIC unit only had six operators compared to 13 in 1980, while the number of maintenance personnel was reduced to just two. It became established practice in the plant to move workers from their regular positions to wherever there was a shortage. The quality and length of training suffered. While thousands slept in their huts around the pesticide factory on the night of December 2/3, a skeleton staff of 120 workers inside the factory ended its evening shift around 10.45 pm and a new shift took over around 11 pm.
			5.3 Operating procedure failures	No evidence of an effective instrument maintenance program. Safety valve testing program largely ineffective and no proper records maintained of reviews of instruments, valves and alarm systems, etc.
				The operating manual supplied by the US company was also grossly inadequate. The MIC control room plant manual did not have instructions for procedures to follow in the event of a rise in temperature or pressure of stored tanks of MIC.
			5.2 Maintenance failures	The factory has a network of water jets. But they could not reach the height at which the MIC was gushing into the air. Second, the MIC storage tanks are connected to a 30-t refrigeration system which keeps the liquid MIC at 0°C. The refrigeration system had been closed down in June 1984, and the gas was at 15°-20°C. Had the refrigeration system been working or capable of working, the MIC could have been cooled. Refrigeration would have increased the time available for detection of the chemical reaction and safe disposal of the material before the reaction reached a dangerous speed. Third, the Bhopal plant had three tanks, each with a 60-capacity, one of which was to be always kept empty for contingencies. But all the tanks contained MIC that night.
			5.1 Design failures	MIC tanks used a cooling system based on brine (highly reactive with MIC).
			4.1 Communication failure with external entities	As the workers realized it was a massive MIC leak, Qureshi ordered all water sources in the area shut off. Over three hours before, a Calcutta battery factory owned by Carbide had asked a novice operator to clean a pipe. The supervisor told him to open a nozzle on the pipes and put a water hose in to clean the inside. The pipe took filtered MIC to the storage tanks. It had a valve that had been closed. The slip blind which ought to have been inserted to make sure the water did not leak through the valve, was missing. Valves in the plant were notorious for leaking. Qureshi claimed there were no instruments either to check leaky valves.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.2: Bhopal Gas Tragedy failure analysis table part 2

TeCSMART				
			Bhopal Disaster	
View 1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	MIC sotrage, emergency safety system, operators	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	High production capacity of MIC but low processing capacity. MIC stored in large quantities for long periods of time.
			2.2 Inadequate or incorrect local decisions	About 11.30 pm, workers in the plant realized there was an MIC leak somewhere: their eyes began to tear. A few of them walked around the MIC structure and spotted a drip of liquid about 50 feet off the ground and some yellowish-white gas accompanying the drip. They told Qureshi about the leak at about 11.45 pm. Qureshi, however, decided to deal with the leak after the tea-break, scheduled for 12.15 am. Qureshi says he was told only of a water leak. But by the time the tea-break ended at 12.40 am, events were moving very fast.
			2.4.3 Training failures	Operators put in charge without sufficient training.
				Underqualified people were running the plant engineering backgrounds had been replaced by less skilled operators.
			1.1 Failure to monitor	No computerized monitoring of instruments and processes. Relied solely on manual observation.
				No lab analysis of quality was undertaken. MIC stored for long periods without testing for contamination.
				The flow meter did not indicate that the circulation of caustic soda — the neutralising agent — had started. No one also knew of the caustic soda concentration because no analysis had been made since October.
			5.1 Design failures	MIC tanks used a cooling system based on brine (highly reactive with MIC).
			5.2 Maintenance failures	One valve remained to protect Tank 610, the nitrogen outflow valve, but this was known to be leaking as engineers had been unable to pressurize the tank on 26 November.
				No emergency caustic scrubber to neutralize any MIC leak.
				MIC tanks had not been under nitrogen pressure since October 1984.
				Suman Dey then rushed to turn on the vent gas scrubber to neutralise the escaping gas. The scrubber had been under maintenance and had been removed from an "operating mode to a standby mode".
				As the workers realized it was a massive MIC leak, Qureshi ordered all water sources in the area shut off. Over three hours before, a Calcutta battery factory owned by Carbide had asked a novice operator to clean a pipe. The supervisor told him to open a nozzle on the pipes and put a water hose in to clean the inside. The pipe took filtered MIC to the storage tanks. It had a valve that had been closed. The slip blind which ought to have been inserted to make sure the water did not leak through the valve, was missing. Valves in the plant were notorious for leaking. Qureshi claimed there were no instruments either to check leaky valves.

Figure A.3: Bhopal Gas Tragedy failure analysis table part 3

A.2 Space Shuttle Challenger Accident

TeCSMART				
			Space Shuttle Challenger Disaster	
View 7	Societal View	*Time Scale*	Decades	
		Agents	U.S. society	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	U.S. Government	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	NASA	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Given [118] the extent of the ice on the pad (see photos pages 112 and 113), the admitted unknown effect of the Solid Rocket Motor and Space Shuttle Main Engines ignition on the ice, as well as the fact that debris striking the Orbiter was a potential flight safety hazard, the Commission finds the decision to launch questionable under those circumstances. In this situation, NASA appeared to be requiring a contractor to prove that it was not safe to launch, rather than proving it was safe. Nevertheless, the Commission has determined that the ice was not a cause of the 51-L accident and does not conclude that NASA's decision to launch specifically overrode a no-launch recommendation by an element contractor. (Findings, 2, line 3-6)
			2.2 Inadequate or incorrect local decisions	NASA and Thiokol accepted escalating risk apparently because they "got away with it last time." (Findings, line 11)
			2.4.1 Lack of resources	Reductions in the safety, reliability and quality assurance work force at Marshall and NASA Headquarters have seriously limited capability in those vital functions. (Findings, line 1)
				Limited human resources and an organization that placed reliability and quality assurance functions under the director of Science and Engineering reduced the capability of the "watch dog" role. ([155], line 7-8)
			1.3 Significant errors in monitoring	As the flight rate increased, the Marshall safety, reliability and quality assurance work force was decreasing, which adversely affected mission safety. (Findings, line 6)
			5.3 Operating procedure failures	Organizational structures at Kennedy and Marshall have placed safety, reliability and quality assurance offices under the supervision of the very organizations and activities whose efforts they are to check. (Findings, line 2-3)
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 4	Market View	*Time Scale*	Months	
		Agents	Areospace industry	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	The capabilities of the system were stretched to the limit to support the flight rate in winter 1985/1986. Projections into the spring and summer of 1986 showed a clear trend; the system, as it existed, would have been unable to deliver crew training software for scheduled flights by the designated dates. The result would have been an unacceptable compression of the time available for the crews to accomplish their required training. (Findings, line 1-3)
				The scheduled flight rate did not accurately reflect the capabilities and resources. The flight rate was not reduced to accommodate periods of adjustment in the capacity of the work force. There was no margin in the system to accommodate unforeseen hardware problems. Resources were primarily directed toward supporting the flights and thus not enough were available to improve and expand facilities needed to support a higher flight rate. (Findings, line 12-14)
				The capabilities of the system were stretched to the limit to support the flight rate in winter 1985/1986. Projections into the spring and summer of 1986 showed a clear trend; the system, as it existed, would have been unable to deliver crew training software for scheduled flights by the designated dates. The result would have been an unacceptable compression of the time available for the crews to accomplish their required training. (Findings, line 1-3)
			5.3 Operating procedure failures	There was no system which made it imperative that launch constraints and waivers of launch constraints be considered by all levels of management. ([104] Findings, 2)
			4.3 Inter-level communication failure	Problem reporting requirements are not concise and fail to get critical information to the proper levels of management. (Findings, line 4)
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.4: Space Shuttle Challenger Accident failure analysis table part 1

TeCSMART				
			Space Shuttle Challenger Disaster	
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	NASA, Thiokol (contractor)	
		Key Failures	***Key Failure***	***Specific Examples***
			3.1 Flawed actions including supervision	Given [118] the extent of the ice on the pad (see photos pages 112 and 113), the admitted unknown effect of the Solid Rocket Motor and Space Shuttle Main Engines ignition on the ice, as well as the fact that debris striking the Orbiter was a potential flight safety hazard, the Commission finds the decision to launch questionable under those circumstances. In this situation, NASA appeared to be requiring a contractor to prove that it was not safe to launch, rather than proving it was safe. Nevertheless, the Commission has determined that the ice was not a cause of the 51-L accident and does not conclude that NASA's decision to launch specifically overrode a no-launch recommendation by an element contractor. (Findings, 2, line 3-6)
				Morton Thiokol, Inc., the contractor, did not accept the implication of tests early in the program that the design had a serious and unanticipated flaw. 1 NASA did not accept the judgment of its engineers that the design was unacceptable, and as the joint problems grew in number and severity NASA minimized them in management briefings and reports. 2 Thiokol's stated position was that "the condition is not desirable but is acceptable." ([120], line 3-5)
				Neither organization developed a solution to the unexpected occurrences of O-ring erosion and blow-by even though this problem was experienced frequently during the Shuttle flight history. Instead, Thiokol and NASA management came to accept erosion and blow-by as unavoidable and an acceptable flight risk. (Findings, line 4-6)
				A careful analysis of the flight history of O-ring performance would have revealed the correlation of O-ring damage and low temperature. Neither NASA nor Thiokol carried out such an analysis; consequently, they were unprepared to properly evaluate the risks of launching the 51-L mission in conditions more extreme than they had encountered before. (Findings, line 19-20)
				[N]either Thiokol nor NASA responded adequately to internal warnings about the faulty seal design. (Findings, line 3)
			3.2 Late response	While Thiokol did establish plans for putty tests to determine how it was affected by the leak check in response to the 41-C action item, their progress in completing the tests was slow. The action item was supposed to be completed by May 30, 1984, but as late as March 6, 1985, there are Marshall internal memos that complain that Thiokol had not taken any action on Marshall's December 1983 directive to provide data on putty behavior as affected by the joint leak check stabilization pressure. ([134], line 26-29)
			2.2 Inadequate or incorrect local decisions	In the 51-L readiness reviews, it appears that neither Thiokol management nor the Marshall Level III project managers believed that the O-ring blow-by and erosion risk was critical. The testimony and contemporary correspondence show that Level III believed there was ample margin to fly with O-ring erosion, provided the leak check was performed at 200 pounds per square inch. ([85], line 9-10)
				The Commission concluded that the Thiokol Management reversed its position and recommended the launch of 51-L, at the urging of Marshall and contrary to the views of its engineers in order to accommodate a major customer. ([104] Findings, 4)
				Morton Thiokol, Inc., the contractor, did not accept the implication of tests early in the program that the design had a serious and unanticipated flaw. 1 NASA did not accept the judgment of its engineers that the design was unacceptable, and as the joint problems grew in number and severity NASA minimized them in management briefings and reports. 2 Thiokol's stated position was that "the condition is not desirable but is acceptable." ([120], line 3-5)
				At no time did management either recommend a redesign of the joint or call for the Shuttle's grounding until the problem was solved. ([120], line 7-8)
				NASA management and Thiokol still considered the joint to be a redundant seal even after the change from Criticality 1R to 1. ([126], line 23-24)
				NASA and Thiokol accepted escalating risk apparently because they "got away with it last time." (Findings, line 11)
				NASA's system for tracking anomalies for Flight Readiness Reviews failed in that, despite a history of persistent O-ring erosion and blow-by, flight was still permitted. It failed again in the strange sequence of six consecutive launch constraint waivers prior to 51-L, permitting it to fly without any record of a waiver, or even of an explicit constraint. Tracking and continuing only anomalies that are "outside the data base" of prior flight allowed major problems to be removed from, and lost by, the reporting system. (Findings, line 15-17)
				NASA has always taken a positive approach to problem solving and has not evolved to the point where its officials are willing to say they no longer have the resources to respond to proposed changes. ([172], line 6-7)
			2.1 Model failures	Prior to the accident, neither NASA nor Thiokol fully understood the mechanism by which the joint sealing action took place. (Findings, line 9-10)
			2.4.1 Lack of resources	The part of the system responsible for turning the mission requirements and objectives into flight software, flight trajectory information and crew training materials was struggling to keep up with the flight rate in late 1985, and forecasts showed it would be unable to meet its milestones for 1986. It was falling behind because its resources were strained to the limit, strained by the flight rate itself and by the constant changes it was forced to respond to within that accelerating schedule. ([164], line 16-18)
				NASA was being too bold in shuffling manifests. The total resources available to the Shuttle program for- allocation were fixed. As time went on, the agency had to focus those resources more and more on the near term-worrying about today's problem and not focusing on tomorrow's. ([172], line 14-15)
			2.4.2 Inadequate allocation of resources	NASA was being too bold in shuffling manifests. The total resources available to the Shuttle program for- allocation were fixed. As time went on, the agency had to focus those resources more and more on the near term-worrying about today's problem and not focusing on tomorrow's. ([172], line 14-15)
			2.5 Conflict of interest	Customers occasionally have notified NASA Headquarters of a desire to change their scheduled launch date because of development problems, financial difficulties or changing market conditions. NASA generally accedes to these requests and has never imposed the penalties available. ([167], line 11-12)
				Costs were the primary concern of NASA's selection board, particularly those incurred early in the program. ([120], line 11)
				Cost consideration overrode any other- objections, they decided. We concluded that the main criticisms of the Thiokol proposal in the Mission Suitability evaluation were technical in nature, were readily correctable, and the costs to correct did not negate the sizable Thiokol cost advantage," the selection officials concluded. ([121], line 2-3)
				From the inception of the Shuttle, NASA had been advertising a vehicle that would make space operations "routine and economical." The greater the annual number of flights, the greater the degree of routinization and economy, so heavy emphasis was placed on the schedule. However, the attempt to build up to 24 missions a year brought a number of difficulties, among them the compression of training schedules, the lack of spare parts, and the focusing of resources on nearterm problems. ([164], line 12-14)

Figure A.5: Space Shuttle Challenger Accident failure analysis table part 2

TeCSMART				
			Space Shuttle Challenger Disaster	
			1.1 Failure to monitor	NASA also did not have a way to forecast the effect of a change of a manifest. ([172], line 16)
			1.2 Failure to monitor effectively	The O-ring erosion history presented to Level I at NASA Headquarters in August 1985 was sufficiently detailed to require corrective action prior to the next flight. (Findings, line 18) [But NASA didn't.]
				Furthermore, Thiokol and NASA did not make a timely attempt to develop and verify a new seal after the initial design was shown to be deficient. (Findings, line 4)
			5.1 Design failures	That testimony reveals failures in communication that resulted in a decision to launch 51-L based on incomplete and sometimes misleading information, a conflict between engineering data and management judgments, and a NASA management structure that permitted internal flight safety problems to bypass key Shuttle managers. (line 9-10)
			4.1 Communication failure with external entities	[I]n the launch preparation for 51-L relevant concerns of Level III NASA personnel and element contractors were not, in the following crucial areas, adequately communicated to the NASA Level I and II management responsible for the launch: The objections to launch voiced by Morton Thiokol c engineers about the detrimental effect of cold temperatures on the performance of' the Solid Rocket Motor joint seal. The degree of concern of Thiokol and Marshall about the erosion of the joint seals in prior Shuttle flights, notably 51-C (January, 1985) and 51-B (April, 1985). ([84], line 1-4)
			4.2 Peer to Peer communication failure	Another path was the examination at each Flight Readiness Review of evidence of earlier flight anomalies. For 51-L, the data presented in this latter path, while it reached Levels I and II, never referred to either test anomalies or flight anomalies with O-rings. ([85], line 2-4)
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	An analysis of all of the testimony and interviews establishes that Rockwell's recommendation on launch was ambiguous. The Commission finds it difficult, as did Mr. Aldrich, to conclude that there was a no-launch recommendation. Moreover, all parties were asked specifically to contact Aldrich or Moore about launch objections due to weather. Rockwell made no phone calls or further objections to Aldrich or other NASA officials after the 9:00 Mission Management Team meeting and subsequent to the resumption of the countdown. (Findings, 1)
				While Mr. Moore was not being intentionally deceived, he was obviously misled. The reporting system simply was not making trends, status and problems visible with sufficient accuracy and emphasis. ([159], line 16-17)
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	Marshall, Kennedy, Shuttle Program, Challenger Space Shuttle	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Since December, 1982, the O-rings had been designated a "Criticality 1" feature of the Solid Rocket Booster design, a term denoting a failure point-without back-up-that could cause a loss of 'life or vehicle if' the component fails. In July 1985, after a nozzle joint on STS 51-B showed erosion of a secondary O-ring, indicating that the primary seal failed, a launch constraint was placed on flight 51-F and subsequent launches. These constraints had been imposed and regularly waived by the Solid Rocket Booster Project Manager at Marshall, Lawrence B. Mulloy. ([84], line 14-17)
				An analysis of all of the testimony and interviews establishes that Rockwell's recommendation on launch was ambiguous. The Commission finds it difficult, as did Mr. Aldrich, to conclude that there was a no-launch recommendation. Moreover, all parties were asked specifically to contact Aldrich or Moore about launch objections due to weather. Rockwell made no phone calls or further objections to Aldrich or other NASA officials after the 9:00 Mission Management Team meeting and subsequent to the resumption of the countdown. (Findings, 1)
				Five weeks after the 51-L accident, the criticality of the Solid Rocket Motor field joint was still not properly documented in the problem reporting system at Marshall. (Findings, line 7)
				[T]here was no representative of safety on the Mission Management Team that made key decisions during the countdown on January 28, 1986. ([152], line 3-4)
				Stated manifesting policies are not enforced. Numerous late manifest changes (after the cargo integration review) have been made to both major payloads and minor payloads throughout the Shuttle program. Late changes to major payloads or program requirements can require extensive resources (money, manpower, facilities) to implement. If many late changes to "minor" payloads occur, resources are quickly absorbed. Payload specialists frequently were added to a flight well after announced deadlines. Late changes to a mission adversely affect the training and development of procedures for subsequent missions. (Findings, line 6-11)
			2.2 Inadequate or incorrect local decisions	They did not have a clear understanding of Rockwell's concern that it was not safe to launch because of ice on the pad. If the decisionmakers had known all of the facts, it is highly unlikely that they would have decided to launch 51-L on January 28, 1986. (line 3-4)
				In the 51-L readiness reviews, it appears that neither Thiokol management nor the Marshall Level III project managers believed that the O-ring blow-by and erosion risk was critical. The testimony and contemporary correspondence show that Level III believed there was ample margin to fly with O-ring erosion, provided the leak check was performed at 200 pounds per square inch. ([85], line 9-10)
				The Commission concluded that there was a serious flaw in the decision making process leading up to the launch of flight 51-L. A well structured and managed system emphasizing safety would have flagged the rising doubts about the Solid Rocket Booster joint seal. Had these matters been clearly stated and emphasized in the flight readiness process in terms reflecting the views of most of the Thiokol engineers and at least some of the Marshall engineers, it seems likely that the launch of 51-L might not have occurred when it did. ([104] Findings, 1)
				Two things are apparent from the Rockwell testimony. First, Rockwell did not feel it had sufficient time to research and resolve the ice on the pad problem. ([116], line 8-10)
				Those who made that decision were unaware of the recent history of problems concerning the O-rings and the joint and were unaware of the initial written recommendation of the contractor advising against the launch at temperatures below 53 degrees Fahrenheit and the continuing opposition of the engineers at Thiokol after the management reversed its position. (line 1-3)
				Spare parts are in critically short supply. The Shuttle program made a conscious decision to postpone spare parts procurements in favor of budget items of perceived higher priority. Lack of spare parts would likely have limited flight operations in 1986. (Findings, line 4-5)
			2.3 Inadequate or incorrect global decisions	Elements within the Shuttle program tried to adapt their philosophy, their attitude and their requirements to the "operational era." But that era came suddenly, and in some cases, there had not been enough preparation for what "operational" might entail. ([170], line 14-15)

Figure A.6: Space Shuttle Challenger Accident failure analysis table part 3

TeCSMART				
			Space Shuttle Challenger Disaster	
			2.5 Conflict of interest	The Commission is troubled by what appears to be a propensity of management at Marshall to contain potentially serious problems and to attempt to resolve them internally rather than communicate them forward. This tendency is altogether at odds with the need for Marshall to function as part of a system working toward successful flight missions, interfacing and communicating with the other parts of the system that work to the same end. ([104] Findings, 3)
			5.3 Operating procedure failures	It should be noted that there were other and independent paths of system reporting that were designed to bring forward information about the Solid Rocket Booster joint anomalies. One path was the task force of Thiokol engineers and [85] Marshall engineers who had been conducting subscale pressure tests at Wasatch during 1985, a source of documented rising concern and frustration on the part of some of the Thiokol participants and a few of the Marshall participants. But Level II was not in the line of reporting for this activity. ([84], line 20-22) (system reporting procedure failure)
				When flights come in rapid succession, current requirements do not ensure that critical anomalies occurring during one flight are identified and addressed appropriately before the next flight. (Findings, line 16)
			4.1 Communication failure with external entities	Two things are apparent from the Rockwell testimony. Second, even though there was considerable discussion about ice, Rockwell's position on launch described above was not clearly communicated to NASA officials in the launch decision chain during the hours preceding 51-L's launch. ([116], line 8-10)
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	That testimony reveals failures in communication that resulted in a decision to launch 51-L based on incomplete and sometimes misleading information, a conflict between engineering data and management judgments, and a NASA management structure that permitted internal flight safety problems to bypass key Shuttle managers. (line 9-10)
				Neither the launch constraint, the reason for it, or the six consecutive waivers prior to 51-L were known to Moore (Level I) or Aldrich (Level II) or Thomas at the time of the Flight Readiness Review process for 51-L. ([84], line 18-19)
View 1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	operators, engineers, processes	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Little or no trend analysis was performed on O-ring erosion and blow-by problems. (Findings, line 5)
			2.2 Inadequate or incorrect local decisions	The sensitivity of the O-ring sealing performance to these factors has been investigated in extensive tests and analyses. The sensitivity to each factor was evaluated independently and in appropriate combinations to assess the potential to cause or contribute to the 51-L aft field joint failure. Most of the testing was done on either laboratory or subscale equipment. In many cases, the data from these tests are considered to be directly applicable to the seal performance in full scale. However, in some cases there is considerable uncertainty in extrapolating the data to full-scale seal performance. Where such is the case, it is noted in the following discussions. ([58], line 14-17)
				Thiokol reported these initial test findings to the NASA program office at Marshall. Thiokol engineers did not believe the test results really proved that "joint rotation" would cause significant problems, and scheduled no additional tests for the specific purpose of confirming or disproving the joint gap behavior. ([123], line 6-7)
			2.4.1 Lack of resources	Training simulators may be the limiting factor on the flight rate: the two current simulators cannot train crews for more than 12-15 flights per year. (Findings, line 15)
			5.1 Design failures	In view of the findings, the Commission concluded that the cause of the Challenger accident was the failure of the pressure seal in the aft field joint of the right Solid Rocket Motor. The failure was due to a faulty design unacceptably sensitive to a number of factors. These factors were the effects of temperature, physical dimensions, the character of materials, the effects of reusability, processing, and the reaction of the joint to dynamic loading. (Conclusion, line 1-3)
			5.3 Operating procedure failures	The Commission concluded that the freeze protection plan for launch pad 39B was inadequate. The Commission believes that the severe cold and presence of so much ice on the fixed service structure made it inadvisable to launch on the morning of January 28, and that margins of safety were whittled down too far. (Findings, 3)
				The joint test and certification program was inadequate. There was no requirement to configure the qualifications test motor as it would be in flight, and the motors were static tested in a horizontal position, not in the vertical flight position. (Findings, line 7-8)
				Stated manifesting policies are not enforced. Numerous late manifest changes (after the cargo integration review) have been made to both major payloads and minor payloads throughout the Shuttle program. Late changes to major payloads or program requirements can require extensive resources (money, manpower, facilities) to implement. If many late changes to "minor" payloads occur, resources are quickly absorbed. Payload specialists frequently were added to a flight well after announced deadlines. Late changes to a mission adversely affect the training and development of procedures for subsequent missions. (Findings, line 6-11)
			5.2 Maintenance failures	Launch site records show that the right Solid Rocket Motor segments were assembled using approved procedures. However, significant out-of-round conditions existed between the two segments joined at the right Solid Rocket Motor aft field joint (the joint that failed). ([70] Findings, 5)

Figure A.7: Space Shuttle Challenger Accident failure analysis table part 4

A.3 Piper Alpha Disaster

TeCSMART				
			Piper Alpha Disaster	
View 7	Societal View	*Time Scale*	Decades	
		Agents	U.K. society	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	U.K. Government	
		Key Failures	*Key Failure*	*Specific Examples*
			2.5 Conflict of interest	Before the Piper Alpha accident, Carson(s) had already pointed out that the British government, eager to benefit from North Sea petroleum, had adopted a handsoff attitude compared, for example, to that of the Norwegian government where the tradition of regulation and inspection was generally much stronger. The result was a set of relatively loose and dispersed connections between the British oil industry and several regulatory authorities.
			5.1 Design failures	It was also argued that consolidating the regulatory bodies would allow the oil companies to deal with one single authority in a more consistent and effective manner.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	Department of Energy	
		Key Failures	*Key Failure*	*Specific Examples*
			2.5 Conflict of interest	Department of Energy held multiple responsibilities including enforcing safety and collecting profit from leasing. The safety enforcement responsibility was moved to Health and Safety Executive (HSE) (Albert's comment)
			1.3 Significant errors in monitoring	It is clear from the evidence that the Den inspectors do not become involved to any extent with the onshore management of safety except in an incidental way. These considerations led me to doubt whether the type of inspection practised by the Den was an effective means of assessing or monitoring the management of safety by operators. (15.50, pp254)
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 4	Market View	*Time Scale*	Months	
		Agents	Offshore oil industry	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.8: Piper Alpha Disaster failure analysis table part 1

TeCSMART				
			Piper Alpha Disaster	
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	Occidental Petroleum senior managers	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Flaws in Some of Guidelines for Topside Layout.
			2.2 Inadequate or incorrect local decisions	Approximately one year before the explosion, company management had been cautioned in an engineering report that a large fire from escaping gas could pose serious concerns with respect to the safe evacuation of the platform. However, management discounted the likelihood of such an event, citing existing protective systems. In fact, the gas risers upstream of the emergency isolation valves on Piper Alpha were not protected against fire exposure and, because of the diameter and length of the inter-platform gas lines, several days would be required to depressurize the pipelines in the event of a breach. It was the failure of these lines that destroyed Piper Alpha and prevented its evacuation.
				Key organizational factors that are at the root of the decisions identified in the previous section are the following: (1) questionable judgment in the management of productivity vs. safety; (2) flaws in the design philosophy and the design guidelines; (3) problems of personnel management; and (4) insufficient attention to maintenance and inspection (see Fig. 4).
				There may well be situations in which evacuation by helicopters is not possible, at any rate in time to avert danger from personnel on the platform. Evacuation by lifeboats of the conventional type, and even more so escape by life raft, can be both difficult and dangerous. Neither Captain Clayson nor occidental in common with the industry at that time, were able to suggest any significant improvement on the methods of evacuation which already could be used on Piper. In my view the difficulties which aced Occidental were real ones and made it all the more imperative that both incident prevention and the means of fighting any fire should have been of the highest standard. (14.18, pp227)
			2.3 Inadequate or incorrect global decisions	The result was that safety features that may have been adequate in the beginning became insufficient for this new layout, with new couplings and higher risks of accident that may not have been realized (or sufficiently questioned) at the time when the additions were made.
			2.4.3 Training failures	As regards Occidental personnel who were to act as Designated Authorities it is clear that occidental provided no formal training in the permit to work system. (11.6)
				As regards full-scale emergency scenarios, no such exercise had taken place in the 3 years before the disaster, let alone been "assessed by qualified personnel external to the installation". No total shutdown emergency scenario had taken place in the 3 years prior to the disaster. (13.17, pp215)
			2.5 Conflict of interest	At the time of the Piper Alpha accident, the number of people who were operating the system in Phase 1 was the minimum required and appears to have been insufficient. In many cases, operators, when overburdened by several functions, choose to attend to the most pressing problems. As with many other organizational issues, these problems are rooted in the way strategies to cut production costs are implemented.
			1.3 Significant errors in monitoring	Although the loss prevention Department provided advice on qualitative and quantitative risk analysis for the auditing of the blowdown and relief system Mr Gordon could not recall that this report had considered the impossibility of blowing down the inventory of the pipelines in any reasonable time. The type of scenario that happened in the disaster in which the inventories of pipelines vented on Piper had never been considered by his department. (14.22, pp229)
				Senior management were too easily satisfied that the PTW system was being operated correctly, relying on the absence of any feedback of problems as indicating that all was well. They failed to provide the training required to ensure that an effective PTW system was operated in practice. In the face of a known problem with the deluge system they did not become personally involved in probing the extent of the problem and what should be done to resolve it as soon as possible. They adopted a superficial response when issues of safety were raised by others, as for example at the time of Mr Saldana's report and the Sutherland prosecution. They failed to ensure that emergency training was being provided as they intended. Platform personnel and management were not prepared for a major emergency as they should have been. (14.52, pp238)
			5.1 Design failures	No organizational redundancy; disruption of to the OIM position (OP). No organizational redundancy; disruption of the chain of command (OP). Equipment design; insufficient fire proofing and smoke filters (DES). Design/planning of evacuation routes (lack of redundancies) (DES).
				There appeared to be no system for ensuring that fire and gas panels were reactivated as soon as the need for locking them off had ceased. The reactivation depended upon whether action was taken by either the Control Room operator or the Designated Authority and in either case whether he knew that the work for which the fire and gas panels had been locked off was either completed or suspended.
			5.3 Operating procedure failures	Suspended permits were not kept in the Control Room but in the safety Office, apparently on the ground that there was not enough room in the Control Room to display them there. The correlation of suspended with active permits were not filed according to location but according to the trade involved. This made it difficult for any supervisor to check readily which equipment was isolated for maintenance.
				The diesel-powered fire pumps had been placed in manual control mode due to the presence of divers in the water around the platform. This practice was more conservative than company policies and a 1983 fire protection audit report had recommended that this practice be discontinued. Placing the pumps in manual meant that personnel would have had to reach the pumps to start them after the explosion. However, conditions prevented this and, as a result, the Piper Alpha deluge system was unavailable.
				Evacuation was not ordered, and even if it had been ordered, could not have been fully carried out given the location of the living quarters, the layout of the topside, and the ineffectiveness of the safety equipment. Many evacuation routes were blocked and the life boats, all in the same location, were mostly inaccessible. The fire fighting equipment on board could not be operated because the diesel pumps, which had been put on manual mode, were inaccessible and seem to have been damaged from the beginning. Fire boats were at hand, but waited for orders from OIM to fight the fire. When the master of one of the vessels on-site decided to assume the role of on-scene-commander (OSC), his fire-fighting monitors did not function properly. Piper Alpha was eventually lost in a sequence of structural failures
				For significant periods there were large numbers of suspended permits in the Safety Office, some of which had been suspended for months. In February 1988 it was found that 124 permits to work were outstanding. The safety staff accepted the need to reduce this number and to police
				The Safety Handbook prepared by Occidental for piper and Claymore in May 1987 contained information on 3 pages relating to the permit to work system. However a comparison between its statements and the system as it was in fact operated on Piper demonstrated a number of significant differences, some of which could have important implications for safety. The hand book was dangerously misleading. This fell a long way short of what should have been provided, namely a systematic and consistent set of training notes explaining in relation to the permit form the full and exact responsibilities of the Performing Authority and the safety implications of full compliance with laid down procedure. (11.8)
				The procedure does not mention the need to cross-reference permits where one piece of work may affect another. Without this there is a danger that on completion of one task isolations which are critical to another piece of work may be removed. (11.12)
				The procedure does not draw attention to the danger which is involved in the recommissioning of suspended maintenance work. (11.12)
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.9: Piper Alpha Disaster failure analysis table part 2

TeCSMART				
			Piper Alpha Disaster	
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	supervisors, managers	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Evacuation drills were not conducted weekly as required (one 6 month period recorded only 13 drills). No full-scale shutdown drill had been conducted in the three years prior to the explosion.
				An examination of a number of permits to work, which appeared to be typical of recent practice, showed numerous errors in completion of various details which are required under the procedure, such as errors in regard to signatories, the description of work, the carrying out of gas tests, the effecting of electrical isolation and the affixing of red tags, the insertion of dates and times, the completion of declarations and certificates, the deletion of inapplicable alternatives and the details of extensions, suspensions and safety precautions.
				When Performing Authority returned permits to the Control Room shortly before the end of the day-shift they would sign off all copies of the permit and leave them on the desk of the lead production operator for his subsequent attention. This was contrary to Occidental procedure which required the Performing Authority and the Designated Authority to meet. This deficient practice had developed because the lead production operators were engaged in their handover at this time. It will also be recalled from Chapter 6 that the evidence of Mr Rankin was that before returning to the Control Room to suspend the permit at 18.00 hours he did not inspect the work site. This also was contrary to the occidental procedure. It was, of course, contrary to good practice in that as supervisor he failed to ensure that the work was in a safe condition to be left overnight.
				Suspended permits were filed in the Safety office overnight. However, Occidental procedure by section 3.6 required Designated Authorities to retain the suspended permits.
				Contrary to the written procedure the Performing Authority's copy of the permit was frequently not displayed at the job site. It was not uncommon for the Performing Authority to keep it in his pocket, as Mr Rankin did.
				The procedure required by section 3.2 that the Performing Authority take the permit to the Approving Authority in person, but this was often not done in practice.
				Designated Authorities would regularly but not always sign off permits both for completion and for suspension prior to having the job site inspected. This was contrary to Occidental procedure at section 3.5.
			2.2 Inadequate or incorrect local decisions	Decision to promote personnel to critical positions on a temporary basis (OP).
				Lack of redundancies in the design of trip signals (DES).
				Delay in the decision of the Tharos master to take charge as OSC in time (OP).
				Layout decisions; lack of physical separation (DES).
				Decision to ignore early warning that the platform could not sustain severe fire loads for more than 10 min.
				In fact, even when an accident does occur, appropriate measures to avoid its recurrence are not necessarily taken. The permit-to-work system, for example, had failed before, in particular on Piper Alpha in 1987, when a worker was killed in an accident in the A module (Ref. 1, p. 197). The accident was the result of a breakdown of communications in the permit-to-work system and an error in the shift handovers. In spite of memos and warnings to other OIMs, the lesson was not learned on Piper Alpha itself.
			2.1 Model failures	[O]perators, production engineers, and/or system designers are not aware of all the dependencies of a naturally complex system; (2) undertrained and under-experienced people are allowed to run the operations; and (3) negative experiences and stories of near-misses and incidents tend to be ignored and suppressed because they run counter to the general philosophy.
			2.4.3 Training failures	Platform managers had not been trained on their response to such an emergency on another platform (Note: that the various platforms were owned or operated by different companies.)
			2.4.1 Lack of resources	There were not enough qualified and trained personnel on board at the time of the accident. Temporary promotions allowed fulfillment of critical functions by available people. Therefore, some less experienced personnel, contract maintenance crews, operators, and production workers were allowed to run Piper Alpha at a time when high-level activity should have required special care, attention, and the ability to recognize abnormal signs in order to diagnose and fix problems immediately.
				The lack of an exact format or content for the induction training; the brevity of the time devoted to it; the almost cursory assessment of whether an individual required to attend the training; the uncertainty on the part of safety personnel as to the time interval before a repeat of the induction training was required; the failure to ensure that each person was shown the location of the his lifeboat; and the errors in the safety handbook all point to a failure to ensure that all were properly informed on matters critical to their safety in an emergency. (13.12, pp214)
			2.5 Conflict of interest	Inspection and maintenance of safety features seem to have been low on the priority list.
			1.1 Failure to monitor	Although the PTW system was monitored by the lead safety operator, no indications of problems were reported, and management did not independently review the operation of the system. Based upon an absence of information to the contrary, management assumed that they "knew that things were going all right." It is noted that a senior maintenance technician had voiced his concerns about the PTW system at a meeting at corporate headquarters earlier in the year. In addition, the company had entered a guilty plea in a civil legal proceeding involving a worker fatality caused, in part, by a PTW system problem; however, no substantive improvements in the PTW system resulted.
				While the platform management did not exhibit the leadership required in this important area of training, the onshore safety staff did not operate an effective monitoring system with regard to emergency training. Where strong critical comment was called for they were ineffective. (13.25, pp218)
			1.2 Failure to monitor effectively	[T]he limitation of sampling, especially on the basis of "what catches the eye" within a relatively short visit to an installation runs a plain risk of missing what lies deeper than a surface inspection and of failing to reach a true assessment of the installation as a whole. (15.50, pp254)
			5.1 Design failures	Poor design of control mechanisms: spark arrestors and deluge system (DES). [Poor] [d]esign of the Main Control Room (location of the detector module rack) (DES).
				Evacuation was not ordered, and even if it had been ordered, could not have been fully carried out given the location of the living quarters, the layout of the topside, and the ineffectiveness of the safety equipment. Many evacuation routes were blocked and the life boats, all in the same location, were mostly inaccessible. The fire fighting equipment on board could not be operated because the diesel pumps, which had been put on manual mode, were inaccessible and seem to have been damaged from the beginning. Fire boats were at hand, but waited for orders from OIM to fight the fire. When the master of one of the vessels on-site decided to assume the role of on-scene-commander (OSC), his fire-fighting monitors did not function properly. Piper Alpha was eventually lost in a sequence of structural failures
				[Poor][d]esign of the low-gas alarm system (DES). [Poor][d]esign of the gas detection system: couplings to the electric power system (DES).
				Poor design of the manual fire-fighting system (DES): bad location, no redundancy, and poor protection of the pumps against fires and blasts.

Figure A.10: Piper Alpha Disaster failure analysis table part 3

TeCSMART				
			Piper Alpha Disaster	
			5.3 Operating procedure failures	No alternative official authority when OIM is incapacitated (OP).
				Apart from the case where it had been planned to carry out a major shutdown, there was no consistently used system for affixing a tag to an isolation valve which had been closed as part of the isolation of equipment for maintenance where the tag warned that the valve should not be opened. Unlike the practice of locking-off for electrical isolation, there was no consistent practice of physically locking-off isolation valves which had been closed in order to prevent their being opened inadvertently. Even where equipment had been locked-off, there was nothing to tell an operator what was the reason.
				Where the work under on permit could affect the work under another there was no cross-referencing of the two permits. Reliance was placed on the memory of the Designated Authority. As stated above section D10 of the permit might be ticked but no further detail was supplied. Further, the system of filing active permits in the Control Room according to the location of the equipment meant that work affecting associated equipment on different levels would not be filed together.
			5.2 Maintenance failures	To put the previous two observations in perspective, the structural steel on Piper Alpha had no fireproofing and it was known (at least to management) that "... structural integrity could be lost with 10-15 minutes if a fire was fed from a large pressurized hydrocarbon inventory."
				Failure to properly locate, install, and inspect emergency exit equipment, rafts, and boats. Poor location of the lifeboats; no redundancy (DES; OPM).
				Failure of the Tharos fire-fighting equipment (DES; OP).
			4.2 Peer to Peer communication failure	Occidental procedure required by section 3.1 that the precise nature of the task should be set out on the permit by the Performing Authority. It will be recalled from Chapter 6 that when Mr White, the maintenance superintendent, signed the permit for PSV 504 he entered the number and location of the valve on the permit. This necessary information had not been included by Mr Rankin, the Performing Authority.
Communication Channel			***Key Failure***	***Specific Examples***
			n/a	n/a
		Time Scale	Real Time (secs/mins)	
		Agents	operators, engineers, contractors	
			Key Failure	***Specific Examples***
			3.1 Flawed actions including supervision	During shift turnover, the status of the pump work was addressed, but no mention was made of the RV work, and there was no mention of it in the control room or maintenance logs. Continuing problems with the adequacy of turnovers and log entries were a problem known to some (one staff member: "It was a surprise when you found out some things which were going on.")
				The work permits for the pump and the RV did not reference each other, and it is likely that the permits had been filed in separate locations (one on the control room and one in the Safety Office). When the on-line condensate pump failed later in the shift, creating an imperative to start the spare to enable continued production, control room personnel were only aware of the pump repair work permit, and proceeded to have the pump returned to service.
				Contrary to the written procedure multiple jobs were undertaken on a single permit. A particular example of this was provided by the permit issued in March 1988 in respect of the refurbishment of both PSV 504 and 505 which were attached to the pipework of different condensate injection pumps.
				Error in fitting of the blind flange (OPM). Failure of the OIM to give evacuation orders (OP).
			3.2 Late response	The permit to work (PTW) system was often not implemented according to procedure ("... the procedure was knowingly and flagrantly disregarded."). For example, (1) omissions (e.g., signatures and gas test results) were common, (2) operations representatives often did not inspect the jobsite before suspending the permit at the end of the shift, or closing the permit indicating the work had been completed, and (3) craft supervisors often left permits on the control room desk at the end of a shift, rather than personally returning them to the responsible operations representative, as required by the procedure.

Figure A.11: Piper Alpha Disaster failure analysis table part 4

TeCSMART				
			Piper Alpha Disaster	
View 1	Equipment View	*Key Failures*	2.2 Inadequate or incorrect local decisions	Decision to produce in the Phase 1 (high-pressure level) mode (OP).
				Decision to remove PSV 504 in pump A and to replace it by a blind flange (OPM).
				Decision to store fuel above the production modules; spatial couplings (OP).
				Decision to turn off the automatic system to protect divers (OP).
			2.4.3 Training failures	The investigation revealed that emergency response training given to new platform personnel was cursory and not uniformly provided. Workers were required to be trained if they had not been on Piper Alpha in the last six months. However, training was often waived even if the interval was considerably longer, or if the individual reported that he had previously worked off-shore elsewhere. A number of survivors reported that they had never been trained on the location of the life rafts or how to launch them.
				Poor training for evacuation (OP).
			1.1 Failure to monitor	Failure of the control room operator to read and interpret the signals. Possible error of detection of potential ignition source (OPM).
				Failure of operator to check origin of gas alarms from detector module rack (OP).
				No inspection of the assembly work (OPM).
				Failure to properly inspect and maintain inflatable rafts (OPM).
			5.1 Design failures	The layout of the topside allowed the fire to propagate quickly from production modules B and C to critical centers, and to destroy the control room and the radio room in the early stages of the accident.
				Faulty warning systems for gas release. Lack of redundancy in the fire pumps (DES; OP). Deluge system of limited effectiveness (DES). Failure to upgrade some safety functions to Phase 1 mode (DES; CONST; OP). No blast control panels; fire walls with little resistance to blast pressures (DES). Couplings in the design of the modules (insufficient space separation) (DES). Couplings due to poor protection against fire propagation (DES). Insufficient protection of critical equipment against blast projectiles (DES). Poor fire insulation (DES). Lack of Specific Fire Criteria in Design of Structure.
				Failure to fix the warning system after it &: Poor design of the monitoring panels in the control room.
				No automatic fire protection upon gas detection in west half of module C (DES). No specific fire load provisions in design of structure (DES).
			5.3 Operating procedure failures	Electric power generation, public address, general alarm, emergency shutdown, and fire detection and protection systems also failed shortly after the first explosions.
				Section D10 of the permit form asked "Is there any other work which may effect (sic) this work?" This section was seldom used. At most it might be ticked but no detail supplied as to the work or its effect.
				Individual initiatives to escape and jump off against previous information about survivability of jumping in the sea from more than 60 ft. (OP).
			5.2 Maintenance failures	Had firewater been available, its efficacy might have been limited. Distribution piping, including that in the platform module where the fires were most severe, was badly corroded and pluggage of sprinkler heads was a known problem dating back to 1984. Various fixes had been attempted and a project to replace the fire protection piping had been initiated, but work was lagging behind schedule. Tests in May 1988 revealed that approximately 50% of the sprinkler heads in the subject module were plugged.
				Two redundant pumps inoperative in module C: condensate pump "B" trips; the redundant pump "A" was shut down for maintenance. Failure of a blind flange assembly at the site of Pressure Safety Valve 504 in Module C. Release of condensate vapors in module C (-45 kg, filling -25% of the module volume); failure of gas detectors and emergency shutdown. Failure of C/D fire wall. No blowout panel to contain explosion inside the module. Failures of the emergency shutdown and of the deluge system (E, and E7) and failure of containment function (E,) led to further explosions. Failure of fire pumps: automatic pumps have been turned off; manual (manually started, diesel powered) pumps in module D are damaged by failure of C/D fire wall. Rupture of riser (Tartan to Piper Alpha) caused by pool fire beneath it; "high temperature reducing the pipe steel strength to below the hoop stress induced by internal pressures".
			4.2 Peer to Peer communication failure	Two separate work permits had been issued for the condensate pump, one for the pump repair and one for testing the RV. The RV job had not been completed by the end of the shift and, rather than working overtime to complete it, it was decided to terminate the permit for that day and continue on the next. The craft supervisor suspended the permit and returned it to the control room without notifying operations staff of the job status.
				Failure of the maintenance crew to inform the night shift that pump A was out and that the PSV was missing (hence, an operator error in trying to restart pump A) (OPM).
				At shift changeover lead production operators would not review or discuss the active or suspended permits. Accordingly there was a gap in the system of communication.

Figure A.12: Piper Alpha Disaster failure analysis table part 5

A.4 SARS Epidemic

TeCSMART				
			SARS Outbreak	
View 7	Societal View	*Time Scale*	Decades	
		Agents	global surveillance system and worldwide public health system (individuals, NGOs, Academia, Community-based groups, intergovernmental organizations, multinational corporations, national media agency (CCTV))	
		Key Failures	*Key Failure*	*Specific Examples*
			2.2 Inadequate or incorrect local decisions	Irresponsible actions put the health and safety of many others at risk. (irresponsible actions that patients went out without masks and visited many doctors.)
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	China failed to issue a warning as the virus spread across the country and outside its borders.
				Government reporting of a high number of false SARS cases resulted in negative feelings among the public about the effectiveness of the government's efforts to control the outbreak (i.e., China?)
				In Taiwan, failed attempts to conceal information about the outbreak by public officials created an environment of fear and paranoia (e.g., a poll conducted in May found that 1 in 5 people felt they might have been infected)
				Lack of communication to the public resulted in community fear and confusion making it difficult for disseminating important health information (i.e., China)
View 6	Government View	*Time Scale*	Years	
		Agents	National government structure, UN, WHO, WTO, FAO	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Increased concentration of environmental degradation from intensive production systems and its inappropriate disposal of this waste
			2.4.1 Lack of resources	Resource-constraint countries often have laboratories that lack sufficient or well maintained equipment, and may have not been able to fully comply with biosecurity and biosafety guidelines
			5.1 Design failures	In China, disease outbreaks are investigated and controlled by local health officials, who typically refer outbreaks up the command chain only when they need help. Only a few diseases must be reported immediately to higher authorities, and even these have to be reported only after the source has been investigated and confirmed locally. This system worked well when people were much less mobile and stayed put in their counties or provinces. With rapid economic development and increased mobility, however, the old system could not respond fast enough to a new threat like SARS.
				For example, in China, public health had been delegated to provinces and the central government didn't have legislation that would require a provincial level to work with them on the SARS outbreak
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	national CDC, Ministry of Health, national animal health control department (USDA APHIS), food regulatory agencies	
		Key Failures	*Key Failure*	*Specific Examples*
			2.2 Inadequate or incorrect local decisions	Enforcement of isolation and quarantine in Taiwan during SARS was dependent on having the disease listed as a reportable disease (although it was later added to the list)
			1.3 Significant errors in monitoring	Lack of strict environmental regulation regarding disposal and treatment of waste from concentrated agricultural operation, which might allow for transmission of intestinal pathogens into humans
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 4	Market View	*Time Scale*	Months	
		Agents	national surveillance system (human, animal, wildlife)	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	In all super-spreading events, infection control was lacking.
			3.2 Late response	Local communities are well aware of infection patterns, but do not participate in the reporting processes because of lack of incentives
			2.2 Inadequate or incorrect local decisions	Responsibility for zoonotic disease surveillance and reporting in companion animals, with exceptions of rabies in dogs and psittacosis in pet birds, has not been placed under the purview of any department in any country
			2.4.3 Training failures	Lack of training experience in dealing with a novel agent as the SARS coronavirus
			1.2 Failure to monitor effectively	Delayed recognition of cases—for example, in Taiwan, Hoping Hospital failed to identify SARS as potential cause of disease of a patient and thus it took hours to isolate him, which resulted in 62% attack rate among those hospital workers initially exposed to the patient
			4.2 Peer to Peer communication failure	Failed communication among sectors can lead to delays in detecting and confirming emerging zoonotic disease outbreaks
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	The disease was barely covered by the media, creating a fertile environment for the spread of rumours.
				Slow communication about details of the SARS cases in Ontario Province to the federal government resulted in WHO losing confidence on the Canadian response and issuing in April 2003 a travel advisory asking people to avoid travel to Toronto

Figure A.13: SARS Epidemic failure analysis table part 1

TeCSMART				
			SARS Outbreak	
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	provinces/states government, public health agencies	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	B.C. CDC's dissemination of information about China events was probably responsible for the prompt isolation of the first SARS case in a Vancouver hospital; alerts were also issued by local and provincial public health officials in Ontario, however, uptake was apparently inconsistent thus health workers were not looking for atypical type activity flu
				Use of facemasks outside of the hospital environment was adopted by a large percentage of the population although guidelines for the use of this and other preventive measures were often vague and inconsistent
			3.2 Late response	The serious effects of delaying or blocking the exchange of public and scientific information are evident: rumours and myths replace facts and science. And once credibility is damaged, trust takes a long time to return.
				First case appeared in November 2002 in Guangdong but it was not until the end of January 2003 that Guangdong Province instituted province-wide reporting requirements for atypical pneumonia
			2.2 Inadequate or incorrect local decisions	Health workers safety agency not included in the management of hospital outbreaks (Canada)
			2.4.3 Training failures	Workplace inspectors in Ontario Province in Canada had little or no training on infectious disease issues and had never been involved in an infectious-disease-related inspection of a health care facility
			2.4.2 Inadequate allocation of resources	The 593 cases treated at the Princess Margaret Hospital made up 34% of all SARS cases in Hong Kong—more than the number treated in any other hospital. Although the hospital managed at first to avoid infections among its staff, the outbreak took a heavy toll. A core team of intensive-care-unit doctors and nurses were infected in the first week of April. (Princess Margaret hospital got overwhelmed and its staff started to develop symptoms.)
			2.5 Conflict of interest	Ministry of Labor of the Ontario Province was not given a primary role at the Provincial Operations Centre, and it was not seen as having a central responsibility in protecting health workers; as a contrast, in B.C., the Workers' Compensation Board was widely recognized as having clear authority and jurisdiction over workplace safety
			1.1 Failure to monitor	Lapses in following standard procedures and partly because of initial lack of awareness of the mode of spread of the virus
			1.3 Significant errors in monitoring	Lack of awareness of potential fomite (i.e., infected surfaces) transmission of SARS
			5.1 Design failures	In China, disease outbreaks are investigated and controlled by local health officials, who typically refer outbreaks up the command chain only when they need help. Only a few diseases must be reported immediately to higher authorities, and even these have to be reported only after the source has been investigated and confirmed locally. This system worked well when people were much less mobile and stayed put in their counties or provinces. With rapid economic development and increased mobility, however, the old system could not respond fast enough to a new threat like SARS.
	Communication Channel		*Key Failure*	*Specific Examples*
			n/a	n/a
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	local public health and food regulatory agencies, hospitals, community health clinics, pharmacies, laboratories, public transportation	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Index cases that showed symptoms suggestive of SARS may not have been treated with strict isolation precautions (e.g., Toronto hospital did not use N95 respirators as standard respiratory protection)
			2.2 Inadequate or incorrect local decisions	Airport control measures were not as strict since it allowed asymptomatic cases to travel (only those with fever were stopped from traveling by air)
				No prior infection control audits in the Toronto hospital with a high number of secondary infections
				Contact tracing at Metropole Hotel in relation to the first case of SARS was not conducted although it is believed it would have not stopped the spread of SARS to other countries
				Responsibility for zoonotic disease surveillance and reporting in companion animals, with exceptions of rabies in dogs and psittacosis in pet birds, has not been placed under the purview of any department in any country
			2.4.3 Training failures	Husbandry practices and lack of knowledge about zoonotic disease transmission resulted in an increased risk to emergence of SARS
				Lack of training experience in dealing with a novel agent as the SARS coronavirus
				Cadre responsible for the clean up of patient's feces and urine in some hospitals with secondary transmission were less trained in infection control procedures
			2.4.1 Lack of resources	But aside from Dr Oshitani, there was only Dr Elizabeth Miranda (on a short-term assignment in rabies control) in CSR at the Regional Office, under Dr Brian Doberstyn, Director of the Division for Combating Communicable Disease. No response team stood ready to act at the first sign of a major outbreak.
				Hospitals in China lacked even essential equipment such as masks and gloves to undertake isolation needed for cases and suspect cases. Public health had been underfunded for years, as surveillance and rural health care were shunted aside in favour of revenue-earning services.
			1.2 Failure to monitor effectively	Delayed recognition of cases—for example, in Taiwan, Hoping Hospital failed to identify SARS as potential cause of disease of a patient and thus it took hours to isolate him, which resulted in 62% attack rate among those hospital workers initially exposed to the patient
			5.1 Design failures	Negative pressure rooms were built at hospitals during the SARS outbreak in Taiwan
			5.3 Operating procedure failures	In southern China, the local penchant for exotic foods, the presence of unhygienic wet markets, high population density, and poor animal-husbandry practices—farm animals are often reared right beside pets and people—all favour the transfer of a virus from an animal to a human host.
				High risk medical procedures increased transmission among hospital workers despite the use of protective equipment
			4.2 Peer to Peer communication failure	Failed communication among sectors can lead to delays in detecting and confirming emerging zoonotic disease outbreaks
	Communication Channel		*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.14: SARS Epidemic failure analysis table part 2

TeCSMART				
			SARS Outbreak	
View 1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	health care workers, physicians, wet market farmers and customers, residence and public transportation sanitors	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	At the time of contact, all hospital workers had used masks but not necessarily other protective devices.
				Improper fit or use of N95 respirators by health workers
				Prince of Wales doctors attributed the super-spreading event involving Mr CT to failure to apply proper isolation precautions and use of a nebulized bronchodilator.
				Lack of reviews that could have identified health care workers failing to follow standard infection control procedures
				In Taiwan, enforcement of quarantine was difficult as many people skipped quarantine
			3.2 Late response	Local communities are well aware of infection patterns, but do not participate in the reporting processes because of lack of incentives
			2.2 Inadequate or incorrect local decisions	Physician treating suspected SARS cases in Guangdong Province developed symptoms, but after treating himself decided he was well enough to travel from Guangdong Province to Hong Kong where he spread the unknown disease at the Metropole Hotel
			2.4.3 Training failures	Feces and urine also provided another transmission route but the health workers responsible for the clean-up were less trained in control procedures
			2.5 Conflict of interest	Producers who discover sick animals may try to sell or dispose of them without reporting infection (e.g., Nipah virus outbreak in Malaysia in 1998–1999 was exacerbated because of the transport of infected pigs by a "fire sale" that moved grower pigs from Perak to Negri Sembilan, Selangor, Penang, Malacca, and Johore)
			5.1 Design failures	WHO experts concluded that an odd combination of factors had conspired to spread SARS through the building. First, the index case very likely had a high viral load in his faeces because of his medical condition. Second, bathroom drain traps had dried out or been removed, creating an open path for aerosol or droplets to enter the units via drains in the bathroom floor. Third, many residents had bought bathroom exhaust fans that were six to ten times more powerful than needed for use in a small space. These fans, when run with the bathroom door closed, could draw air from the waste pipe through the floor drain. Contaminated exhaust air from nearby bathroom vents could also have carried droplets from adjoining bathrooms via the light well, releasing contaminants through an open window on one floor, and transferring such contaminants into other living units several floors away.
			5.2 Maintenance failures	Feces and urine also provided another transmission route in the community setting (e.g., Hong Kong building complex outbreak)
			4.2 Peer to Peer communication failure	Grace Hospital physicians and nurses had no warning about events in China from the public health authorities (contrast to the experience at Vancouver General Hospital)

Figure A.15: SARS Epidemic failure analysis table part 3

A.5 Space Shuttle Columbia Accident

TeCSMART				
			Space Shuttle Columbia Disaster	
View 7	Societal View	*Time Scale*	Decades	
		Agents	U.S. society	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	U.S. Government	
		Key Failures	*Key Failure*	*Specific Examples*
			2.5 Conflict of interest	Safety and Mission Assurance organizations supporting the Shuttle Program are largely dependent upon the Program for funding, which hampers their status as independent advisors.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	NASA	
		Key Failures	*Key Failure*	*Specific Examples*
			2.3 Inadequate or incorrect global decisions	System safety engineering and management is separated from mainstream engineering, is not vigorous enough to have an impact on system design, and is hidden in the other safety disciplines at NASA Headquarters.
			2.4.1 Lack of resources	Throughout its history, NASA has consistently struggled to achieve viable safety programs and adjust them to the constraints and vagaries of changing budgets. Yet, according to multiple high level independent reviews, NASA's safety system has fallen short of the mark.
			1.2 Failure to monitor effectively	Over the last two decades, little to no progress has been made toward attaining integrated, independent, and detailed analyses of risk to the Space Shuttle system.
			1.3 Significant errors in monitoring	The dependence of Safety, Reliability & Quality Assurance personnel on Shuttle Program support limits their ability to oversee operations and communicate potential problems throughout the organization.
			5.3 Operating procedure failures	The Associate Administrator for Safety and Mission Assurance is not responsible for safety and mission assurance execution, as intended by the Rogers Commission, but is responsible for Safety and Mission Assurance policy, advice, coordination, and budgets. This view is consistent with NASA's recent philosophy of management at a strategic level at NASA Headquarters but contrary to the Rogers' Commission recommendation.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 4	Market View	*Time Scale*	Months	
		Agents	Areospace industry	
		Key Failures	*Key Failure*	*Specific Examples*
			2.3 Inadequate or incorrect global decisions	System safety engineering and management is separated from mainstream engineering, is not vigorous enough to have an impact on system design, and is hidden in the other safety disciplines at NASA Headquarters.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.16: Space Shuttle Columbia Accident failure analysis table part 1

TeCSMART

			Space Shuttle Columbia Disaster	
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	NASA	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	NASA failed to adequately perform trend analysis on foam losses. This greatly hampered the agency's ability to make informed decisions about foam losses.
				There were lapses in leadership and communication that made it difficult for engineers to raise concerns or understand decisions. Management failed to actively engage in the analysis of potential damage caused by the foam strike.
				The repair option, while logistically viable using existing materials onboard Columbia, relied on so many uncertainties that NASA rated this option "high risk."
				NASA has not followed its own rules and requirements on foam-shedding. Although the agency continuously worked on the foam-shedding problem, the debris impact requirements have not been met on any mission.
			3.2 Late response	Foam bipod debris-shedding incidents on STS-52 and STS-62 were undetected at the time they occurred, and were not discovered until the Board directed NASA to examine External Tank separation images more closely.
			2.2 Inadequate or incorrect local decisions	NASA does not fully understand the mechanisms that cause foam loss on almost all flights from larger areas of foam coverage and from areas that are sculpted by hand.
				NASA's current tools, including the Crater model, are inadequate to evaluate Orbiter Thermal Protection System damage from debris impacts during pre-launch, on-orbit, and post-launch activity.
				Senior Safety, Reliability & Quality Assurance and element managers do not use the Lessons Learned Information System when making decisions. NASA subsequently does not have a constructive program to use past lessons to educate engineers, managers, astronauts, or safety personnel.
				NASA has an inadequate number of spare Reinforced Carbon-Carbon panel assemblies.
			2.5 Conflict of interest	There are conflicting roles, responsibilities, and guidance in the Space Shuttle safety programs. The Safety & Mission Assurance Pre-Launch Assessment Review process is not recognized by the Space Shuttle Program as a requirement that must be followed (NSTS 22778). Failure to consistently apply the Pre-Launch Assessment Review as a requirements document creates confusion about roles and responsibilities in the NASA safety organization.
				Throughout its history, NASA has consistently struggled to achieve viable safety programs and adjust them to the constraints and vagaries of changing budgets. Yet, according to multiple high level independent reviews, NASA's safety system has fallen short of the mark.
			1.2 Failure to monitor effectively	The Board found instances of left bipod ramp shedding on launch that NASA was not aware of, bringing the total known left bipod ramp shedding events to 7 out of 72 missions for which imagery of the launch or External Tank separation is available.
			5.3 Operating procedure failures	Thirty percent of all missions lacked sufficient imagery to determine if foam had been lost.
				The Space Shuttle Systems Integration Office handles all Shuttle systems except the Orbiter. Therefore, it is not a true integration office.
				The Integration office did not have continuous responsibility to integrate responses to bipod foam shedding from various offices. Sometimes the Orbiter Office had responsibility, sometimes the External Tank Office at Marshall Space Flight Center had responsibility, and sometime the bipod shedding did not result in any designation of an In-Flight Anomaly. Integration did not occur.
				NASA information databases such as The Problem Reporting and Corrective Action and the Web Program Compliance Assurance and Status System are marginally effective decision tools.
			4.1 Communication failure with external entities	Risk information and data from hazard analyses are not communicated effectively to the risk assessment and mission assurance processes. The Board could not find adequate application of a process, database, or metric analysis tool that took an integrated, systemic view of the entire Space Shuttle system.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
		Time Scale	Real Time (hours/days)	
		Agents	managers, Shuttle Program, Columbia Space Shuttle	
			Key Failure	*Specific Examples*
			3.1 Flawed actions including supervision	Despite the constant shedding of foam, the Shuttle Program did little to harden the Orbiter against foam impacts through upgrades to the Thermal Protection System. Without impact resistance and strength requirements that are calibrated to the energy of debris likely to impact the Orbiter, certification of new Thermal Protection System tile will not adequately address the threat posed by debris.
				The Team routed its request for imagery through Johnson Space Center's Engineering Directorate rather than through the Mission Evaluation Room to the Mission Management Team to the Flight Dynamics Officer, the channel used during a mission. This routing diluted the urgency of their request. Managers viewed it as a non-critical engineering desire rather than a critical operational need.
				The assumptions (and their uncertainties) used in the analysis were never presented or discussed in full to either the Mission Evaluation Room or the Mission Management Team.
				While engineers and managers knew the foam could have struck RCC panels; the briefings on the analysis to the Mission Evaluation Room and Mission Management Team did not address RCC damage, and neither Mission Evaluation Room nor Mission Management Team managers asked about it.
				Managers asked "Who's requesting the photos?" instead of assessing the merits of the request. Management seemed more concerned about the staff following proper channels (even while they were themselves taking informal advice) than they were about the analysis.
				In both the Mission Evaluation Room and Mission Management Team meetings over the Debris Assessment Team's results, the focus was on the bottom line – was there a safety-of-flight issue, or not? There was little discussion of analysis, assumptions, issues, or ramifications.
				There were lapses in leadership and communication that made it difficult for engineers to raise concerns or understand decisions. Management failed to actively engage in the analysis of potential damage caused by the foam strike.

Figure A.17: Space Shuttle Columbia Accident failure analysis table part 2

TeCSMART				
			Space Shuttle Columbia Disaster	
View 2	**Plant View**	***Key Failures***	2.2 Inadequate or incorrect local decisions	Columbia re-entered the atmosphere with a pre-existing breach in the left wing.
				Since 2001, Kennedy Space Center has used a non-standard approach to define foreign object debris. The industry standard term "Foreign Object Damage" has been divided into two categories, one of which is much more permissive.
				A Debris Assessment Team began forming on Flight Day two to analyze the impact. Once the debris strike was categorized as "out of family" by United Space Alliance, contractual obligations led to the Team being Co-Chaired by the cognizant contractor sub-system manager and her NASA counterpart. The team was not designated a Tiger Team by the Mission Evaluation Room or Mission Management Team.
				After Program managers learned about the foam strike, their belief that it would not be a problem was confirmed (early, and without analysis) by a trusted expert who was readily accessible and spoke from "experience." No one in management questioned this conclusion.
				When the Integration Office convenes the Integration Control Board, the Orbiter Office usually does not send a representative, and its staff makes verbal inputs only when requested.
			2.1 Model failures	Shuttle Program Managers entered the mission with the belief, recently reinforced by the STS-113 Flight Readiness Review, that a foam strike is not a safety-of-flight issue.
			1.1 Failure to monitor	If Program managers were able to unequivocally determine before Flight Day Seven that there was potentially catastrophic damage to the left wing, accelerated processing of Atlantis might have provided a window in which Atlantis could rendezvous with Columbia before Columbia's limited consumables ran out.
			5.3 Operating procedure failures	Though the Team was clearly reporting its plans (and final results) through the Mission Evaluation Room to the Mission Management Team, no Mission manager appeared to "own" the Team's actions. The Mission Management Team, through the Mission Evaluation Room, provided no direction for team activities, and Shuttle managers did not formally consult the Team's leaders about their progress or interim results.
				Mission Management Team meetings occurred infrequently (five times during a 16 day mission), not every day, as specified in Shuttle Program management rules.
				The Space Shuttle Program has a wealth of data tucked away in multiple databases without a convenient way to integrate and use the data for management, engineering, or safety decisions.
			4.1 Communication failure with external entities	Safety representatives from the appropriate organizations attended meetings of the Debris Assessment Team, Mission Evaluation Room, and Mission Management Team, but were passive, and therefore were not a channel through which to voice concerns or dissenting views.
			4.2 Peer to Peer communication failure	Communication was stifled by the Shuttle Program attempts to find out who had a "mandatory requirement" for imagery.
				Program Managers did not actively communicate with the Debris Assessment Team. Partly as a result of this, the Team went through institutional, not mission-related, channels with its request for imagery, and confusion surrounded the origin of imagery requests and their subsequent denial.
			4.3 Inter-level communication failure	Much of Program managers' information came through informal channels, which prevented relevant opinion and analysis from reaching decision makers.
Communication Channel			***Key Failure***	***Specific Examples***
			4.3 Inter-level communication failure	Team members never realized that management's decision against seeking imagery was not intended as a direct or final response to their request.
				Communication did not flow effectively up to or down from Program managers.

Figure A.18: Space Shuttle Columbia Accident failure analysis table part 3

TeCSMART				
			Space Shuttle Columbia Disaster	
Layer1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	operators, engineers, processes	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Contamination from zinc leaching from a primer under the paint topcoat on the launch pad structure increases the opportunities for localized oxidation.
				Quality assurance processes for bolt catchers (a Criticality 1 subsystem) were not adequate to assure contract compliance or product adequacy.
				The bipod ramp foam debris critically damaged the leading edge of Columbia's left wing.
				The Team's assessment of possible tile damage was performed using an impact simulation that was well outside Crater's test database. The Boeing analyst was inexperienced in the use of Crater and the interpretation of its results. Engineers with extensive Thermal Protection System expertise at Huntington Beach were not actively involved in determining if the Crater results were properly interpreted.
				No one in the operational chain of command for STS-107 held a security clearance that would enable them to understand the capabilities and limitations of National imagery resources.
			3.2 Late response	The STS-112 assignment for the External Tank Project to "identify the cause and corrective action of the bipod ramp foam loss event" was not due until after the planned launch of STS-113, and then slipped to after the launch of STS-107.
			2.2 Inadequate or incorrect local decisions	The certification of the bolt catchers flown on STS-107 was accomplished by extrapolating analysis done on similar but not identical bolt catchers in original testing. No testing of flight hardware was performed.
				Foam bipod debris-shedding events were classified as In-Flight Anomalies up until STS-112, which was the first known bipod foam-shedding event not classified as an In-Flight Anomaly.
				No External Tank configuration changes were made after the bipod foam loss on STS-112.
				Crater initially predicted tile damage deeper than the actual tile depth, but engineers used their judgment to conclude that damage would not penetrate the densified layer of tile. Similarly, RCC damage conclusions were based primarily on judgment and experience rather than analysis.
			2.4.3 Training failures	The Team's assessment of possible tile damage was performed using an impact simulation that was well outside Crater's test database. The Boeing analyst was inexperienced in the use of Crater and the interpretation of its results. Engineers with extensive Thermal Protection System expertise at Huntington Beach were not actively involved in determining if the Crater results were properly interpreted.
			2.4.1 Lack of resources	Evaluation of STS-107 debris impact was hampered by lack of high resolution, high speed cameras (temporal and spatial imagery data).
			2.5 Conflict of interest	?Foam-shedding, which had initially raised serious safety concerns, evolved into "in-family" or "no safety-of-flight" events or were deemed an "accepted risk."
			1.1 Failure to monitor	The current long-range camera assets on the Kennedy Space Center and Eastern Range do not provide best possible engineering data during Space Shuttle ascents.
				By the time data indicating problems was telemetered to Mission Control Center, the Orbiter had already suffered damage from which it could not recover.
			5.1 Design failures	The wing leading edge Reinforced Carbon-Carbon composite material and associated support hardware are remarkably tough and have impact capabilities that far exceed the minimal impact resistance specified in their original design requirements. Nevertheless, these tests demonstrate that this inherent toughness can be exceeded by impacts representative of those that occurred during Columbia's ascent.
			5.3 Operating procedure failures	There are no qualified non-destructive evaluation techniques for the as-installed foam to determine the characteristics of the foam before flight.
				Current inspection techniques are not adequate to assess structural integrity of the RCC components.
				The Board found markedly different criteria for margins of micrometeoroid and orbital debris safety between the International Space Station and the Shuttle.
				There is lack of effective processes for feedback or integration among project elements in the resolution of In-Flight Anomalies.
			5.2 Maintenance failures	After manufacturer's acceptance non-destructive evaluation, only periodic visual and touch tests are conducted.
				RCC components are weakened by mass loss caused by oxidation within the substrate, which accumulates with age. The extent of oxidation is not directly measurable, and the resulting mission life reduction is developed analytically.
				To date, only two flown RCC panels, having achieved 15 and 19 missions, have been destructively tested to determine actual loss of strength due to oxidation.
				Board-directed testing of a small sample size demonstrated that the "as-flown" bolt catchers do not have the required 1.4 margin of safety.
				The foam strike was first seen by the Intercenter Photo Working Group on the morning of Flight Day Two during the standard review of launch video and high-speed photography. The strike was larger than any seen in the past, and the group was concerned about possible damage to the Orbiter. No conclusive images of the strike existed. One camera that may have provided an additional view was out of focus because of an improperly maintained lens.

Figure A.19: Space Shuttle Columbia Accident failure analysis table part 4

A.6 Northeast Blackout

TeCSMART			Northeast Blackout	
Layer7	Societal View	*Time Scale*	Decades	
		Agents	U.S. and Canada	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
Layer6	Government View	*Time Scale*	Years	
		Agents	U.S. and Canada Government	
		Key Failures	*Key Failure*	*Specific Examples*
			5.3 Operating procedure failures	At a federal policy level, clarification is needed on expenditures and investments for bulk system reliability (including investments in new technologies) and how such expenditure will be recoverable through transmission rates.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
Layer5	Regulatory View	*Time Scale*	Years	
		Agents	NERC, FERC of U.S. and NEB of Canada	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	The NERC compliance programs did not identify and resolve specific compliance violations before those violations led to a cascading blackout. The approach used for monitoring and assuring compliance with NERC and regional reliability standards prior to August 14 delegated much of the responsibility and accountability to the regional level. Due to confidentiality considerations, NERC did not receive detailed information about violations of specific parties prior to August 14. This approach meant that the NERC compliance program was only as effective as that of the weakest regional reliability council
				NERC operating policies do not specify what tools are specifically required of control areas and reliability coordinators, such as state estimation and network analysis tools, although the policies do specify the expected outcomes of analysis. FERC did not promote strong national energy infrastructure, including adequate transmission facilities and oversee of mandatory reliability standards for the bulk power system
			5.3 Operating procedure failures	Problems identified in studies of prior large-scale blackouts were repeated on August 14, including deficiencies in vegetation management, operator training, and tools to help operators better visualize system conditions. Although these issues had been previously reported, NERC and some regions did not have a systematic approach to tracking successful implementation of those prior recommendations.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
Layer4	Market View	*Time Scale*	Months	
		Agents	MAAC-ECAR-NPCC power grid	
		Key Failures	*Key Failure*	*Specific Examples*
			2.3 Inadequate or incorrect global decisions	Many generators had pre-designed protection points that shut the unit down early in the cascade, so there were fewer units on-line to prevent island formation or to maintain balance between load and supply within each island after it formed. In particular, it appears that some generators tripped to protect the units from conditions that did not justify their protection, and many others were set to trip in ways that were not
			2.4.1 Lack of resources	On August 14, the lack of adequate dynamic reactive reserves, coupled with not knowing the critical voltages and maximum import capability to serve native load, left the Cleveland- Akron area in a very vulnerable state.
			2.4.2 Inadequate allocation of resources	On August 14, the lack of adequate dynamic reactive reserves, coupled with not knowing the critical voltages and maximum import capability to serve native load, left the Cleveland- Akron area in a very vulnerable state.
			2.5 Conflict of interest	These protections should be set tight enough to protect the unit from the grid, but also wide enough to assure that the unit remains connected to the grid as long as possible. This coordination is a risk management issue that must balance the needs of the grid and customers relative to the needs of the individual assets.
			5.1 Design failures	Many generators had pre-designed protection points that shut the unit down early in the cascade, so there were fewer units on-line to prevent island formation or to maintain balance between load and supply within each island after it formed. In particular, it appears that some generators tripped to protect the units from conditions that did not justify their protection, and many others were set to trip in ways that were not coordinated with the region's under-frequency load-shedding, rendering that UFLS scheme less effective.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.20: Northeast Blackout failure analysis table part 1

TeCSMART

			Northeast Blackout	
Layer3	Management View	*Time Scale*	Months (quarterly)	
		Agents	FE, AEP, MISO, PJM	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	ECAR does not conduct exacting regionwide analyses, but compiles individual members' internal studies of N-2 and multiple contingencies. The last such study conducted was published in 2000, projecting system conditions for 2003. That study did not include any contingency cases that resulted in 345-kV line overloading or voltage violations on 345-kV buses.
				ECAR and its member companies did not adequately follow ECAR Document 1 to conduct regional and interregional system planning studies and assessments.
			1.1 Failure to monitor	MISO did not discover that Harding- Chamberlin had tripped until after the blackout, when MISO reviewed the breaker operation log that evening.
			1.2 Failure to monitor effectively	From 15:05 EDT to 15:41 EDT, during which MISO did not recognize the consequences of the Hanna-Juniper loss, and FE operators knew neither of the line's loss nor its consequences. PJM and AEP recognized the overload on Star-South Canton, but had not expected it because their earlier contingency analysis did not examine enough lines within the FE system to foresee this result of the Hanna- Juniper contingency on top of the Harding-Chamberlin outage.
			1.3 Significant errors in monitoring	Contingency analysis simulation of the conditions following the loss of the Harding-Chamberlin 345-kV circuit at 15:05 EDT showed that the system would be unable to sustain some contingencies without line overloads above emergency ratings. However, when Eastlake 5 was modeled as in service and fully available in those simulations, all overloads above emergency limits were eliminated, even with the loss of Harding-Chamberlin.
			2.4.1 Lack of resources	There is no UVLS system in place within Cleveland and Akron; had such a scheme been implemented before August, 2003, shedding 1,500 MW of load in that area before the loss of the Sammis-Star line might have prevented the cascade and blackout.
			5.1 Design failures	In ECAR, data used to model loads and generators were inaccurate due to a lack of verification through benchmarking with actual system data and field testing.
				In ECAR, planning studies, design assumptions, and facilities ratings were not consistently shared and were not subject to adequate peer review among operating entities and regions.
			5.3 Operating procedure failures	FirstEnergy has historically relied upon the ECAR regional assessments to identify anticipated reactive power requirements and recommended corrective actions. But ECAR over the past five years has not conducted any detailed analysis of the Cleveland- Akron area and its voltage-constrained import capability
				ECAR did not have a coordinated procedure to develop and periodically review reactive power margins.
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	ECAR and MISO did not precisely define "critical facilities" such that the 345-kV lines in FE that caused a major cascading failure would have to be identified as critical facilities for MISO. MISO's procedure in effect on August 14 was to request FE to identify critical facilities on its system to MISO.
		Time Scale	Real Time (hours/days)	
		Agents	Eastlake 5 generation, Harding-Chamberlin line	
			Key Failure	*Specific Examples*
			3.1 Flawed actions including supervision	Numerous control areas in the Eastern Interconnection, including FE, were not correctly tagging dynamic schedules, resulting in large mismatches between actual, scheduled, and tagged interchange on August 14.
				NERC policy requires that critical facilities be identified and that neighboring control areas and reliability coordinators be made aware of the status of those facilities to identify the impact of those conditions on their own facilities. However, FE never identified these capacitor banks as critical and so did not pass on status information to others.
				The loss of Eastlake 5 followed by the loss of Perry are contingencies that should be assessed in the operations planning timeframe, to develop measures to readjust the system between contingencies. Since FirstEnergy did not conduct such contingency analysis planning and develop these advance measures, it was in violation of NERC Planning Standard 1A, Category C3.
				FE has specific written procedures and plans for dealing with resource deficiencies, voltage depressions, and overloads, and these include instructions to adjust generators and trip firm loads. After the loss of the Star-South Canton line, voltages were below limits, and there were severe line overloads. But FE did not follow any of these procedures on August 14, because FE did not know for most of that time that its system might need such treatment.
			3.2 Late response	FE personnel told the investigation team that the alarm processing application had failed on occasions prior to August 14, leading to loss of the alarming of system conditions and events for FE's operators. However, FE said that the mode and behavior of this particular failure event were both first time occurrences and ones which, at the time, FE's IT personnel neither recognized nor knew how to correct.

Figure A.21: Northeast Blackout failure analysis table part 2

TeCSMART				
			Northeast Blackout	
Layer2	Plant View	*Key Failures*	2.2 Inadequate or incorrect local decisions	The investigation team probed deeply into voltage management issues within the Cleveland-Akron area. The team conducted extensive voltage stability studies (discussed below), concluding that FE's 90% minimum voltage level was not only far less stringent than nearby interconnected systems (most of which set the pre-contingency minimum voltage criteria at 95%), but was not adequate for secure system operations.
				FE uses minimum acceptable normal voltages which are lower than and incompatible with those used by its interconnected neighbors.
				Unlike many other transmission grid control rooms, FE's control center did not have a map board (which shows schematically all major lines and plants in the control area on the wall in front of the operators), which might have shown the location of significant line and facility outages within the control area.
			2.1 Model failures	One of MISO's primary system condition evaluation tools, its state estimator, was unable to assess system conditions for most of the period between 12:15 and 15:34 EDT, due to a combination of human error and the effect of the loss of DPL's Stuart- Atlanta line on other MISO lines as reflected in the state estimator's calculations.
			2.4.1 Lack of resources	Eastlake Unit 5 is a 597 MW (net) generating unit located west of Cleveland on Lake Erie. It is a major source of reactive power support for the Cleveland area. It tripped at 13:31 EDT. The cause of the trip was that as the Eastlake 5 operator sought to increase the unit's reactive power output (Figure 4.3), the unit's protection system detected that VAr output exceeded the unit's VAr capability and tripped the unit off-line. The loss of the Eastlake 5 unit did not put the grid into an unreliable state—i.e., it was still able to withstand safely another contingency. However, the loss of the unit required FE to import additional power to make up for the loss of the unit's output (612 MW), made voltage management in northern Ohio more challenging, and gave FE operators less flexibility in operating their system.
			1.1 Failure to monitor	MISO did not discover that Harding- Chamberlin had tripped until after the blackout, when MISO reviewed the breaker operation log that evening.
			1.2 Failure to monitor effectively	The Cleveland-Akron area's voltage problems were well-known and reflected in the stringent voltage criteria used by control area operators until 1998.
				From 15:05 EDT to 15:41 EDT, during which MISO did not recognize the consequences of the Hanna-Juniper loss, and FE operators knew neither of the line's loss nor its consequences. PJM and AEP recognized the overload on Star-South Canton, but had not expected it because their earlier contingency analysis did not examine enough lines within the FE system to foresee this result of the Hanna- Juniper contingency on top of the Harding-Chamberlin outage.
			1.3 Significant errors in monitoring	Contingency analysis simulation of the conditions following the loss of the Harding-Chamberlin 345-kV circuit at 15:05 EDT showed that the system would be unable to sustain some contingencies without line overloads above emergency ratings. However, when Eastlake 5 was modeled as in service and fully available in those simulations, all overloads above emergency limits were eliminated, even with the loss of Harding-Chamberlin.
			5.1 Design failures	FE did not have an effective generation redispatch plan and did not have sufficient redispatch resources to relieve overloaded transmission lines supplying northeastern Ohio. FE did not have an effective load reduction plan.
				The discrepancy between actual measured system flows (with Stuart-Atlanta off-line) and the MISO model (which assumed Stuart-Atlanta on-line) prevented the state estimator from solving correctly.
				Although MISO received SCADA input of the line's status change, this was presented to MISO operators as breaker status changes rather than a line failure. Because their EMS system topology processor had not yet been linked to recognize line failures, it did not connect the breaker information to the loss of a transmission line. Thus, MISO's operators did not recognize the Harding-Chamberlin trip as a significant contingency event and could not advise FE regarding the event or its consequences. Further, without its state estimator and associated contingency analyses, MISO was unable to identify potential overloads that would occur due to various line or equipment outages.
				FE did not have an adequate load reduction capability, whether automatic or manual, to relieve overloaded transmission lines supplying northeastern Ohio
				After the Harding-Chamberlin 345-kV line outage at 15:05 EDT, the flowgate monitoring tool produced incorrect (obsolete) results, because the outage was not reflected in the model.
			5.3 Operating procedure failures	MISO was hindered because it lacked clear visibility, responsibility, authority, and ability to take the actions needed in this circumstance. MISO had interpretive and operational tools and a large amount of system data, but had a limited view of FE's system.
				The PJM and MISO reliability coordinators lacked an effective procedure on when and how to coordinate an operating limit violation observed by one of them in the other's area. The lack of such a procedure caused ineffective communications between PJM and MISO regarding PJM's awareness of a possible overload on the Sammis-Star line as early as 15:48
				FE did not have an effective contingency analysis capability cycling periodically on-line and did not have a practice of running contingency analysis manually as an effective alternative for identifying contingency limit violations
				The PJM and MISO did not have effective procedures to coordinate an operating limit violation
				The investigation team could not find FirstEnergy contingency plans or operational procedures for operators to manage the FirstEnergy control area and protect the Cleveland-Akron area from the unexpected loss of the Perry plant.
				FE's internal control room procedures and protocols did not prepare it adequately to identify and react to the August 14 emergency.

Figure A.22: Northeast Blackout failure analysis table part 3

TeCSMART				
			Northeast Blackout	
			5.2 Maintenance failures	FE had no periodic diagnostics to evaluate and report the state of the alarm processor, nothing about the eventual failure of two EMS servers would have directly alerted the support staff that the alarms had failed in an infinite loop lockup
				FE's Area Control Error (ACE), the primary control signal used to adjust generators and imports to match load obligations, did not function between 14:54 EDT and 15:08 EDT and later between 15:46 EDT and 15:59 EDT, when the two servers were down.
			4.1 Communication failure with external entities	The Stuart-Atlanta 345-kV line, operated by DPL, and monitored by the PJM reliability coordinator, tripped at 14:02 EDT. However, since the line was not in MISO's footprint, MISO operators did not monitor the status of this line and did not know it had gone out of service. This led to a data mismatch that prevented MISO's state estimator (a key monitoring tool) from producing usable results later in the day at a time when system conditions in FE's control area were deteriorating.
			4.3 Inter-level communication failure	FE failed to inform its reliability coordinator and adjacent control areas when they became aware that system conditions had changed due to unscheduled equipment outages that might affect other control areas.
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	FE did not have an effective protocol for sharing operator information within the control room and with others outside the control room
Layer1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	operators and equipment	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	FE control center computer support staff did not fully test the functionality of applications, including the alarm processor, after a server failover and restore
				To troubleshoot the problem the analyst had turned off the automatic trigger that runs the state estimator every five minutes. After fixing the problem he forgot to re-enable it, so although he had successfully run the SE and RTCA manually to reach a set of correct system analyses, the tools were not returned to normal automatic operation. Thinking the system had been successfully restored, the analyst went to lunch.
				Even though FE's Information Technology support staff knew of the problems and were working to solve them, and the absence of alarms and other symptoms offered many clues to the operators of the EMS system's impaired state. Thus, without a functioning EMS or the knowledge that it had failed, FE's system operators remained unaware that their electrical system condition was beginning to degrade.
				Loss of the first server caused an auto-page to be issued to alert FE's EMS IT support personnel to the problem. When the back-up server failed, it too sent an auto-page to FE's IT staff. They did not notify control room operators of the problem. The IT staff did not confirm that the alarm system was again working properly with the control room operators.
				On August 14 at about 12:15 EDT, MISO's state estimator produced a solution with a high mismatch (outside the bounds of acceptable error). This was traced to an outage of Cinergy's Bloomington-Denois Creek 230-kV line— although it was out of service, its status was not updated in MISO's state estimator.
				FE's operators were not aware that the system was operating outside first contingency limits after the Harding-Chamberlin trip (for the possible loss of Hanna-Juniper or the Perry unit), because they did not conduct a contingency analysis.
			2.2 Inadequate or incorrect local decisions	MISO operators use non-realtime topology information for critical lines mapped into its state estimator
			2.4.3 Training failures	The FE operators did not recognize the information they were receiving as clear indications of an emerging system emergency
				Since FE operators have numerous information screen options, and one or more screens are commonly "nested" as sub-screens to one or more top level screens, operators' ability to view, understand and operate their system through the EMS would have slowed to a frustrating crawl.
				FE operators did not understand how much of their system was being lost, and did not realize the degree to which their perception of their system was in error versus true system conditions, despite receiving clues via phone calls from AEP, PJM and MISO, and customers. The FE operators were not aware of line outages that occurred after the trip of Eastlake 5 at 13:31 EDT until approximately 15:45 EDT, although they were beginning to get external input describing aspects of the system's weakening condition. Since FE's operators were not aware and did not recognize events as they were occurring, they took no actions to return the system to a
				Neither group of operators had significant training, documentation, or actual experience for how to handle an emergency of this type and magnitude.
			1.1 Failure to monitor	The Stuart-Atlanta 345-kV line, operated by DPL, and monitored by the PJM reliability coordinator, tripped at 14:02 EDT. However, since the line was not in MISO's footprint, MISO operators did not monitor the status of this line and did not know it had gone out of service. This led to a data mismatch that prevented MISO's state estimator (a key monitoring tool) from producing usable results later in the day at a time when system conditions in FE's control area were deteriorating.
			4.2 Peer to Peer communication failure	FE computer support staff did not effectively communicate the loss of alarm functionality to the FE system operators after the alarm processor failed at 14:14, nor did they have a formal procedure to do so
				Loss of the first server caused an auto-page to be issued to alert FE's EMS IT support personnel to the problem. When the back-up server failed, it too sent an auto-page to FE's IT staff. They did not notify control room operators of the problem. The IT staff did not confirm that the alarm system was again working properly with the control room operators.
				The most critical factor delaying the assessment and synthesis of the clues was a lack of information sharing between the FE system operators.

Figure A.23: Northeast Blackout failure analysis table part 4

A.7 BP Texas City Refinery Explosion

TeCSMART				
			BP Texas City Refinery Explosion	
View 7	Societal View	*Time Scale*	Decades	
		Agents	U.S. society	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	U.S. Government	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	OSHA, NPRA, EPA	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	In the years prior to the incident OSHA conducted several inspections, primarily in response to fatalities at the refinery, but did not identify the likelihood for a catastrophic incident, nor did OSHA prioritize planned inspections of the refinery to enforce process safety regulations, despite warning signs.
				The NPRA did not provide sufficient suggestions to the members to improve the refinery safety.
				OSHA did not conduct a comprehensive inspection of any of the other 29 process units at the Texas City refinery.
				EPA records show that the BP Texas City facility had not received a planned RMP rule audit prior to the ISOM incident.
			3.2 Late response	BP Texas City was a facility with very high risk for a catastrophe, but OSHA did not target the refinery for comprehensive planned inspections.
			2.1 Model failures	The OSHA inappropriately accepted BP's reports without further investigation
			2.4.1 Lack of resources	OSHA's compliance directive for the PSM standard states that the main vehicle for enforcement is planned PQV inspections. However, PQV inspections are infrequent and an insufficient number of inspectors are qualified to conduct them.
			2.4.2 Inadequate allocation of resources	The incident at Texas City and its connection to serious process safety deficiencies at the refinery emphasize the need for OSHA to refocus resources on preventing catastrophic accidents through greater PSM enforcement.
Communication Channel				
View 4	Market View	*Time Scale*	Months	
		Agents	Oil refining industry	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.24: BP Texas City Refinery Explosion failure analysis table part 1

TeCSMART				
			BP Texas City Refinery Explosion	
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	BP senior management	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Consistent with the lack of an effective focus on process safety performance, BP management did not establish appropriate operational expectations regarding process safety performance at its U.S. refineries.
				BP's executive management either did not receive refinery-specific information that suggested process safety deficiencies at some of the U.S. refineries or did not effectively respond to the information that they did receive.
				The Board of Directors of BP p.l.c. has not ensured, as a best practice, that BP's management has implemented an integrated, comprehensive, and effective process safety management system for BP's five U.S. refineries.
				BP's safety management system does not ensure timely compliance with internal process safety standards and programs at the refineries.
				BP's safety management system does not ensure timely implementation of external good engineering practices that support and could improve process safety performance at BP's five U.S. refineries.
				BP's process safety management system does not effectively translate corporate expectations into measurable criteria for the management of process risk, or define the appropriate role of qualitative and quantitative risk
				BP's process safety management system likely results in under reporting of incidents and near misses at BP's five U.S. refineries.
			2.2 Inadequate or incorrect local decisions	Cost-cutting and failure to invest in the 1990s by Amoco and then BP left the Texas City refinery vulnerable to a catastrophe. BP targeted budget cuts of 25 percent in 1999 and another 25 percent in 2005, even though much of the refinery's infrastructure and process equipment were in disrepair. Also, operator training and staffing were downsized.
				BP has emphasized personal safety but not process safety.
				BP's corporate initiatives have overloaded personnel at its five U.S. refineries, to the possible detriment of process safety.
			2.4.3 Training failures	BP has not adequately ensured that its U.S. refinery personnel and contractors have sufficient process safety knowledge and competence.
			2.4.1 Lack of resources	BP has not always ensured that it identified and provided the resources required for strong process safety performance at its U.S. refineries, including both financial and human resources.
			2.5 Conflict of interest	Cost-cutting, failure to invest and production pressures from BP Group executive managers impaired process safety performance at Texas City.
				BP directs a great deal of attention to short-term performance that is capable of quick measurement, analysis, and feedback
			1.1 Failure to monitor	BP mistakenly used improving personal safety performance (i.e., personal injury rates) as an indication of acceptable process safety performance at its five U.S. refineries
			1.2 Failure to monitor effectively	BP's investigation system has not instituted effective root cause analysis procedures to identify systemic causal factors.
			1.3 Significant errors in monitoring	The BP Board of Directors did not provide effective oversight of BP's safety culture and major accident prevention programs. The Board did not have a member responsible for assessing and verifying the performance of BP's major accident hazard prevention programs.
				BP did not effectively incorporate process safety considerations into management decision-making that affects the U.S. refineries. BP tended to have a short-term focus, and its decentralized management system and entrepreneurial culture have delegated substantial discretion to U.S. refinery plant managers without clearly defining process safety expectations, responsibilities, or accountabilities.
			5.1 Design failures	BP has not instilled a common, unifying process safety culture among its U.S. refineries.
				BP does not have a designated, high-ranking leader for process safety dedicated to its refining business.
				BP's decentralized management system and entrepreneurial culture have delegated substantial discretion to U.S. refinery managers without clearly defining process safety expectations, responsibilities, or accountabilities.
				BP did not have a shift turnover communication requirement for its operations staff.
				BP has not provided effective process safety leadership. BP has not adequately established process safety as a core value across all its five U.S. refineries.
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	While BP has the aspirational goal that there be "no accidents, no harm to people," it appears that refinery managers have not received effective operational guidance from corporate-level refining management about how to achieve this goal.

Figure A.25: BP Texas City Refinery Explosion failure analysis table part 2

TeCSMART				
			BP Texas City Refinery Explosion	
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	BP Texas City Refinery; refinery managers	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Operations and maintenance personnel at BP's five U.S. refineries sometimes work high rates of overtime.
				BP Texas City managers did not effectively implement their pre-startup safety review policy to ensure that nonessential personnel were removed from areas in and around process units during startups, an especially hazardous time in operations. Cost-cutting, failure to invest and production pressures from BP Group executive managers impaired process safety performance at Texas City
			3.2 Late response	Neither Amoco nor BP replaced blowdown drums and atmospheric stacks, even though a series of incidents warned that this equipment was unsafe. In the years prior to the incident, eight serious releases of flammable material from the ISOM blowdown stack had occurred, and most ISOM startups experienced high liquid levels in the splitter tower. Neither Amoco nor BP investigated these events
			2.2 Inadequate or incorrect local decisions	Neither Amoco nor BP managers replaced blowdown drums and atmospheric stacks, even though a series of incidents warned that this equipment was unsafe
				Reliance on the low personal injury rate at Texas City as a safety indicator failed to provide a true picture of process safety performance and the health of the safety culture.
				A "check the box" mentality was prevalent at Texas City, where personnel completed paperwork and checked off on safety policy and procedural requirements even when those requirements had not been met.
				Safety campaigns, goals, and rewards focused on improving personal safety metrics and worker behaviors rather than on process safety and management safety systems. While compliance with many safety policies and procedures was deficient at all levels of the refinery, Texas City managers did not lead by example regarding safety.
				Most of BP's five U.S. refineries have had high turnover of refinery plant managers, and process safety leadership appears to have suffered as a result.
			2.4.3 Training failures	BP Texas City lacked a reporting and learning culture. Personnel were not encouraged to report safety problems and some feared retaliation for doing so. The lessons from incidents and near-misses, therefore, were generally not captured or acted upon.
			1.1 Failure to monitor	Numerous measures for tracking various types of operational, environmental[,] and safety performance, but no clear focus on the leading indicators for the potential catastrophic or major incidents
				A lack of supervisory oversight and technically trained personnel during the startup, an especially hazardous period, was an omission contrary to BP safety guidelines. An extra board operator was not assigned to assist, despite a staffing assessment that recommended an additional board operator for all ISOM startups.
			1.2 Failure to monitor effectively	BP Texas City did not effectively assess changes involving people, policies, or the organization that could impact process safety.
				Deviations from safe practices, lack of operating discipline, and apparent complacency toward serious process safety risk at the Texas City refinery have been well chronicled in a variety of BP documents.
			5.1 Design failures	Occupied trailers were sited too close to a process unit handling highly hazardous materials. All fatalities occurred in or around the trailers
				The size of the blowdown drum was insufficient to contain the liquid sent to it by the pressure relief valves
				This blowdown system was an antiquated and unsafe design; it was originally installed in the 1950s, and had never been connected to a flare system to safely contain liquids and combust flammable vapors released from the process.
			5.3 Operating procedure failures	Outdated and ineffective procedures did not address recurring operational problems during startup, leading operators to believe that procedures could be altered or did not have to be followed during the startup process
			5.2 Maintenance failures	Neither Amoco nor BP replaced blowdown drums and atmospheric stacks, even though a series of incidents warned that this equipment was unsafe.
				Deficiencies in BP's mechanical integrity program resulted in the "run to failure" of process equipment at Texas City.
				rupture disk/relief valve spaces at the Carson, Texas City, Toledo, and Whiting refineries were found to have been pressurized without timely follow-up or corrective action
				Many procedures for testing of critical instruments and emergency shut-down systems were out of date and some were missing. Interval-based inspections and risk-based inspection tasks were not integrated into one inspection management system for execution and tracking.
			4.1 Communication failure with external entities	BP and Amoco did not cooperate well to investigate pervious incidents and replace blowdown drum
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	Supervisors and operators poorly communicated critical information regarding the startup during the shift turnover
				at some of its U.S. refineries BP has not established a positive, trusting, and open environment with effective lines of communication between management and the workforce, including employee representatives.

Figure A.26: BP Texas City Refinery Explosion failure analysis table part 3

TeCSMART				
			BP Texas City Refinery Explosion	
View 1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	raffinate splitter tower operators, engineers, contractors, ISOM	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	the operator flawed to turn off the level control valve
				operator closed the level control valve accidentally and did not realize that the pressure relief valves were open
				Numerous heat exchanger tube thickness measurements were not taken. Some pressure vessels, storage tanks, piping, relief valves, rotating equipment, and instruments were overdue for inspection in six operating units evaluated
				During the startup, operations personnel pumped flammable liquid hydrocarbons into the tower for over three hours without any liquid being removed, which was contrary to startup procedure instructions.
			2.2 Inadequate or incorrect local decisions	The process unit was started despite previously reported malfunctions of the tower level indicator, level sight glass, and a pressure control valve.
			2.4.3 Training failures	The operator training program was inadequate. The central training department staff had been reduced from 28 to eight, and simulators were unavailable for operators to practice handling abnormal situations, including infrequent and high hazard operations such as startups and unit upsets.
				Hourly employees at all refineries also stated during interviews that formal and informal mentoring was rare or nonexistent.
			2.5 Conflict of interest	a significant number of hourly workers stated during interviews that incidents, near misses, and safety-related concerns sometimes did not get reported because of fear of repercussion, and in some cases out of a belief that the refinery would not act on the report.
			1.1 Failure to monitor	Critical alarms and control instrumentation provided false indications that failed to alert the operators of the high level in the tower.
			5.2 Maintenance failures	Employees in some process safety functional groups at Toledo, Texas City, and Whiting provided high negative response rates regarding the prioritization of inspection and maintenance at their refineries.
			4.2 Peer to Peer communication failure	the night lead operator left early but very limited information about his control cations was given to day board operator

Figure A.27: BP Texas City Refinery Explosion failure analysis table part 4

A.8 Subprime Crisis

TeCSMART				
			Subprime Crisis	
View 7	Societal View	*Time Scale*	Decades	
		Agents	Worldwide	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	a combination of excessive borrowing, risky investments, and lack of transparency put the financial system on a collision
				the corrosion of mortgage-lending standards and the securitization pipeline that transported toxic mortgages from neighborhoods across America to investors around the globe
			2.5 Conflict of interest	As one recent study argues, many economists were "agnostics" on housing, unwilling to risk their reputations or spook markets by alleging a bubble without finding support in economic theory.
			1.3 Significant errors in monitoring	the rising incidence of mortgage fraud, which flourished in an environment of collapsing lending standards and lax regulation
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	U.S. and Foreign Governments	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	the government's inconsistent handling of major financial institutions during the crisis increased uncertainty and panic in the market. It did not surprise the Commission that an industry of such wealth and power would exert pressure on policy makers and regulators
			5.1 Design failures	Where were Citigroup's regulators while the company piled up tens of billions of dollars of risk in the CDO business? Citigroup had a complex corporate structure and, as a result, faced an array of supervisors. The Federal Reserve supervised the holding company but, as the Gramm-Leach-Bliley legislation directed, relied on others to monitor the most important subsidiaries: the Office of the Comptroller of the Currency (OCC) supervised the largest bank subsidiary, Citibank, and the SEC supervised the securities firm, Citigroup Global Markets. Moreover, Citigroup did not really align its various businesses with the legal entities. An individual working on the CDO desk on an intricate transaction could interact with various components of the firm in complicated ways.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.28: Subprime Crisis failure analysis table part 1

TeCSMART				
			Subprime Crisis	
View 5	Regulatory View	*Time Scale*	Years	
		Agents	FED, SEC, FDIC, OCC, OTC, Treasury Department, the Department of Housing and Urban Development, and the Office of Federal Housing Enterprise Oversight	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	The Fed's failure to stop predatory practices infuriated consumer advocates and some members of Congress.
				The Fed did not begin routinely examining subprime subsidiaries until a pilot program in July 2007, under new chairman Ben Bernanke. The Fed did not issue new rules under HOEPA until July 2008, a year after the subprime market had shut down.
				In the end, regulators declined to introduce standards for LTV ratios or for documentation for home mortgages.
				Lehman's regulators did not restrain its rapid growth. The SEC, Lehman's main regulator, knew of the firm's disregard of risk management.
				Regulators reacted weakly. As early as 2005, supervisors recognized that CDOs and credit default swaps (CDS) could actually concentrate rather than diversify risk, but they concluded that Wall Street knew what it was doing. Supervisors issued guidance in late 2006 warning banks of the risks of complex structured finance transactions— but excluded mortgage-backed securities and CDOs, because they saw the risks of those products as relatively straightforward and well understood.
			3.2 Late response	government agencies could have taken actions to prevent the crisis. For example, the Securities and Exchange Commission could have required more capital and halted risky practices at the big investment banks. The Federal Reserve Bank of New York and other regulators could have clamped down on Citigroup's excesses in the run-up to the crisis. Policy makers and regulators could have stopped the runaway mortgage securitization train
				Declining underwriting standards and new mortgage products had been on regulators' radar screens in the years before the crisis, but disagreements among the agencies and their traditional preference for minimal interference delayed action.
				Regulators had been taking notice of the mortgage market for several years before the crisis. As early as 2004, they recognized that mortgage products and borrowers had changed during and following the refinancing boom of the previous year, and they began work on providing guidance to banks and thrifts. But too little was done, and too late, because of interagency discord, industry pushback, and a widely held view that market participants had the situation well in hand.
			2.2 Inadequate or incorrect local decisions	key policy makers—the Treasury Department, the Federal Reserve Board, and the Federal Reserve Bank of New York—who were best positioned to watch over our markets were ill prepared for the events of 2007 and 2008
			2.3 Inadequate or incorrect global decisions	The Fed's monetary policy kept short-term interest rates low. Low rates cut the cost of homeownership. An adjustable-rate mortgage (ARM) gave buyers even lower initial payments or made a larger house affordable—unless interest rates rose. All stimulate the growth of housing market.
				As the housing market expanded, another problem emerged, in subprime and prime mortgages alike: inflated appraisals. Changes in regulations reinforced the trend toward laxer appraisal standards.
			2.4.1 Lack of resources	In an interview with the FCIC, Greenspan went further, arguing that with or without a mandate, the Fed lacked sufficient resources to examine the nonbank subsidiaries. Worse, the former chairman said, inadequate regulation sends a misleading message to the firms and the market. But if resources were the issue, the Fed chairman could have argued for more. It was always mindful, however, that it could be subject to a government audit of its finances.
			2.5 Conflict of interest	*The need for guidance was controversial within the agencies, too. "We got tremendous pushback from the industry as well as Congress as well as, you know, internally," the Fed's Siddique told the FCIC. "Because it was stifling innovation, potentially, and it was denying the American dream to many people."
			1.1 Failure to monitor	due to the complexity, it is hard to monitor the financial market, however, lack of government oversight contributes to the crisis (academic analysis about financial market may be helpful for monitoring the financial market)
				the record reflects that senior public officials did not recognize that a bursting of the bubble could threaten the entire financial system
			1.2 Failure to monitor effectively	*Meanwhile, banks and regulators were not prepared for significant losses on triple-A mortgage-backed securities, which were, after all, supposed to be among the safest investments. Nor were they prepared for ratings downgrades due to expected losses, which would require banks to post more capital.
				More than 30 years later, the SEC got limited authority to oversee NRSROs in the Credit Rating Agency Reform Act of 2006. That law, taking effect in June 2007, focused on mandatory disclosure of the rating agencies' methodologies; however, the law barred the SEC from regulating "the substance of the credit ratings or the procedures and methodologies."
			5.3 Operating procedure failures	The SEC suggested the creation of the Consolidated Supervised Entity (CSE) program to oversee the holding companies of investment banks and all their subsidiaries. The SEC did not have express legislative authority to require the investment banks to submit to consolidated regulation, so it proposed that the CSE program be voluntary; the SEC crafted the new program out of its authority to make rules for the broker-dealer subsidiaries of investment banks.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.29: Subprime Crisis failure analysis table part 2

TeCSMART				
			Subprime Crisis	
View 4	Market View	*Time Scale*	Months	
		Agents	financial market	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	the corrosion of mortgage-lending standards and the securitization pipeline that transported toxic mortgages from neighborhoods across America to investors around the globe
			2.5 Conflict of interest	*The need for guidance was controversial within the agencies, too. "We got tremendous pushback from the industry as well as Congress as well as, you know, internally," the Fed's Siddique told the FCIC. "Because it was stifling innovation, potentially, and it was denying the American dream to many people."
			2.1 Model failures	For decades, a version of the originate-to-distribute model produced safe mortgages. But some saw that the model now had problems. "If you look at how many people are playing, from the real estate agent all the way through to the guy who is issuing the security and the underwriter and the underwriting group and blah, blah, blah, then nobody in this entire chain is responsible to anybody…"
			5.3 Operating procedure failures	These mark-to-market accounting rules received a good deal of criticism in recent years, as firms argued that the lower market prices did not reflect market values but rather fire-sale prices driven by forced sales.
			4.2 Peer to Peer communication failure	In theory, every participant along the securitization pipeline should have had an interest in the quality of every underlying mortgage. In practice, their interests were often not aligned.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	financial institutions, credit rating agencies	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Struggling to remain dominant, Fannie and Freddie loosened their underwriting standards, purchasing and guaranteeing riskier loans, and increasing their securities purchases. Yet their regulator, the Office of Federal Housing Enterprise Oversight (OFHEO), focused more on accounting and other operational issues than on Fannie's and Freddie's increasing investments in risky mortgages and securities.
				In theory, the rating agencies were important watchdogs over the securitization process. They described their role as being "an umpire in the market." But they did not review the quality of individual mortgages in a mortgage-backed security, nor did they check to see that the mortgages were what the securitizers said they were.
				It also appeared some institutions switched regulators in search of more lenient treatment.
				The Corporate Library, which rates firms' corporate governance, gave Citigroup a C. In early 2007, the Corporate Library would downgrade Citigroup to a D, "reflecting a high degree of governance risk." Among the issues cited: executive compensation practices that were poorly aligned with shareholder interests.
			2.2 Inadequate or incorrect local decisions	financial institutions' inadequate decisions of using excessive leverage and complex financial instruments
				deregulation and reliance of self-regulation by financial institutions had stripped away key safeguards. Many of these institutions grew aggressively through poorly executed acquisition and integration strategies that made effective management more challenging
				The new requirements put the rating agencies in the driver's seat. How much capital a bank held depended in part on the ratings of the securities it held.
				To estimate the probability of default, Moody's relied almost exclusively on its own ratings of the mortgage-backed securities purchased by the CDOs.
				They needed new products that, as prices kept rising, could make expensive homes more affordable to still-eager borrowers. The solution was riskier, more aggressive, mortgage products that brought higher yields for investors but correspondingly greater risks for borrowers.
			2.3 Inadequate or incorrect global decisions	The banks had gained their own securitization skills and didn't need the investment banks to structure and distribute. So the investment banks moved into mortgage origination to guarantee a supply of loans they could securitize and sell to the growing legions of investors. But they are lack of global views of the entire market.
			2.1 Model failures	financial institutions and credit rating agencies embraced mathematical models as reliable predictors of risks, replacing judgment in too many instances
				Moody's flawed computer models. The pressure from financial firms that paid for the ratings and OTC derivatives contributed to the crisis. The pressure may cause Moody's flawed rating model
			2.5 Conflict of interest	Many Moody's former employees said that after the public listing, the company [Moody's] culture changed—it went "from [a culture] resembling a university academic department to one which values revenues at all costs," according to Eric Kolchinsky, a former managing director.
				If Fannie Mae stayed the course, it would maintain its credit discipline, protect the quality of its book, preserve capital, and intensify the company's public voice on concerns. However, it would also face lower volumes and revenues, continued declines in market share, lower earnings, and a weakening of key customer relationships. It was simply a matter of relevance, former CEO Dan Mudd told the FCIC: "If you're not relevant, you're unprofitable, and you're not serving the mission. And there was danger to profitability.
				If an issuer didn't like a Moody's rating on a particular deal, it might get a better rating from another ratings agency. The agencies were compensated only for rated deals—in effect, only for the deals for which their ratings were accepted by the issuer. So the pressure came from two directions: in-house insistence on increasing market share and direct demands from the issuers and investment bankers, who pushed for better ratings with fewer conditions.
			1.1 Failure to monitor	Moody's did not sufficiently account for the deterioration in underwriting standards or a dramatic decline in home prices. And Moody's did not even develop a model specifically to take into account the layered risks of subprime securities until late 2006, after it had already rated nearly 19,000 subprime securities.
			1.2 Failure to monitor effectively	*Meanwhile, banks and regulators were not prepared for significant losses on triple-A mortgage-backed securities, which were, after all, supposed to be among the safest investments. Nor were they prepared for ratings downgrades due to expected losses, which would require banks to post more capital.
			1.3 Significant errors in monitoring	deregulation and reliance of self-regulation by financial institutions had stripped away key safeguards. Many of these institutions grew aggressively through poorly executed acquisition and integration strategies that made effective management more challenging
			5.3 Operating procedure failures	The five investment banks, however, did not meet the standard: the SEC was supervising their securities arms, but no one supervisor kept track of these companies on a consolidated basis. Thus all five faced an important decision: what agency would they prefer as their regulator?

Figure A.30: Subprime Crisis failure analysis table part 3

TeCSMART				
			Subprime Crisis	
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	dealers, inverstors, subprime related financial products	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Bankers would take those low investment-grade tranches, largely rated BBB or A, from many mortgage-backed securities and repackage them into the new securities—CDOs. Approximately 80% of these CDO tranches would be rated triple-A despite the fact that they generally comprised the lower-rated tranches of mortgage-backed securities.
				Synthetic CDOs multiplied the effects of the collapse in subprime.
			5.3 Operating procedure failures	In addition to the rising fraud and egregious lending practices, lending standards deteriorated in the final years of the bubble.
Communication Channel			*Key Failure*	*Specific Examples*
			4.1 Communication failure with external entities	the leverage was often hidden. Lenders rarely discuss the leverage and the associated high risk with their investors. Investors relied on the credit rating agencies, often blindly
View 1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	borrowers, subprime loans, lenders, brokers	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	a combination of excessive borrowing, risky investments, and lack of transparency put the financial system on a collision
				Lenders devised a way to get rid of these monthly fees that had added to the cost of homeownership: lower down payments that did not require insurance.
				CDO managers faced growing competitive pressures. More than had been the case three or four years earlier, in picking the collateral the managers were influenced by the underwriters—the securities firms that created and marketed the deals. An FCIC
			2.2 Inadequate or incorrect local decisions	In retrospect, it is clear that the agencies' CDO models made two key mistakes. First, they assumed that securitizers could create safer financial products by diversifying among many mortgage-backed securities, when in fact these securities weren't that
			2.4.3 Training failures	In theory, borrowers are the first defense against abusive lending. But many borrowers do not understand the most basic aspects of their mortgage. Borrowers with less access to credit are particularly ill equipped to challenge the more experienced person across the desk.
				most of financial personnel are well trained, however, the complex financial market is complicated
			2.5 Conflict of interest	borrowers likely took out mortgages that they never had the capacity or intention to pay

Figure A.31: Subprime Crisis failure analysis table part 4

A.9 BP Deepwater Horizon Oil Spill

TeCSMART				
			BP Deepwater Horizon Oil Spill	
View 7	Societal View	*Time Scale*	Decades	
		Agents	U.S. society	
		Key Failures	*Key Failure*	*Specific Examples*
			2.3 Inadequate or incorrect global decisions	Too dependent on fossil fuels
				Disinclined to conserve
			2.5 Conflict of interest	Less concerned with environmental impact, etc.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	U.S. Government	
		Key Failures	*Key Failure*	*Specific Examples*
			2.3 Inadequate or incorrect global decisions	The federal courts in particular offer some redress, although mostly in a reactive mode, so the effect on systemic risk going forward is unclear.
			5.3 Operating procedure failures	In the BP Deepwater Horizon case, BOEMRE has conflicting responsibilities.
				Aligning with to industry and generally deregulatory policies
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	BOEMRE (MMS), Coast Guard, EPA	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Minerals Management Service (MMS) regulation of the offshore oil and gas industry failed to address the risks of deepwater drilling. The agency lacked technical expertise, large enough staff, political backing, etc. Staff were also found to be guilty of serious ethical lapses.
				For the Macondo drilling plans, safety and environmental reviews were lacking (National Commission Report, p.77-79, p.82-84, etc) also US Coast Guard and the Republic of the Marshall Islands didn't inspect the rig thoroughly or often enough
				after the incident happened, Coast Guard and BOEMRE started to find the flawed activities involved in BP Deepwater Horizon
				Coast Guard and Republic of the Marshall Islands also less vigilant than necessary.
			2.2 Inadequate or incorrect local decisions	MMS was too quick to approve plans and changes in all phases of the design and drilling of the Macondo well, and in some cases missed errors in permit applications.
			2.4.3 Training failures	MMS's failures throughout the process, including too few and poorly qualified offshore oil and gas inspectors and permit reviewers.
			2.5 Conflict of interest	MMS conflict of interest, given financial incentive to promote offshore drilling while ostensibly regulating it...
				Well design was not covered in detail by MMS regulations. MMS staff were also reluctant to point out risky design and call for changes, because they didn't want to be held accountable for potential problems.
			1.3 Significant errors in monitoring	The offshore oil and gas industry's increasing reliance on hyper-specialized contractors hasn't been matched by adequate oversight, coordination and communication, for example, BP failed to respond to longstanding concerns about the performance of
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 4	Market View	*Time Scale*	Months	
		Agents	Offshore oil drilling industry	
		Key Failures	*Key Failure*	*Specific Examples*
			1.3 Significant errors in monitoring	The offshore oil and gas industry's increasing reliance on hyper-specialized contractors hasn't been matched by adequate oversight, coordination and communication, for example, BP failed to respond to longstanding concerns about the performance of Halliburton's cementing engineer
			2.2 Inadequate or incorrect local decisions	Lax safety and general cost cutting, speedups
			4.1 Communication failure with external entities	Oil and gas companies and their partners and contractors were also often unaware of one another's capabilities/competence and roles/responsibilities
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.32: BP Deepwater Horizon Oil Spill failure analysis table part 1

TeCSMART				
			BP Deepwater Horizon Oil Spill	
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	BP senior management	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	BP's flawed safety program, although even that not followed
			2.2 Inadequate or incorrect local decisions	Decisions to pursue hydrocarbons in hard to reach and environmentally sensitive areas without adequately assessing and preparing for the risks
			2.3 Inadequate or incorrect global decisions	Decision to send the Schlumberger cement log team back to shore
			2.4.3 Training failures	Transocean hadn't trained its dynamic positioning officers for emergency situations
			2.4.2 Inadequate allocation of resources	BP's failure to manage its personnel effectively, e.g., not supporting junior engineer in key design tasks, not properly a vetting substitute well site leader, etc.
			1.1 Failure to monitor	BP's failure to have engineers monitor the drilling from shore, despite having the equipment and real-time data feeds for doing so
				BP managers accepted the wrong monitoring results and the outside contractors did not question BP's decision based on their modeling results
			5.1 Design failures	Well design omitted a protective casing for the production casing
			5.3 Operating procedure failures	BP also failed to have any formal risk analysis or expert review process for the changes made to the well design and drilling procedures in the several week lead-up to the blowout. [company level failure, since shared responsibility of rig and onshore staff]
				Inadequate standard practices, for example, there were no standard cement test procedures or interpretation methods
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	BP failed to send the operations note on the temporary abandonment of the well until the morning of the procedure, so, for instance, the rig crew didn't have detailed instructions for performing and interpreting the negative pressure test
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	BP Macondo managers, Transocean managers, Halliburton managers	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Inadequate cement tests
			2.2 Inadequate or incorrect local decisions	Between April 12 and April 20, the Macondo well team changed temporary abandonment procedure at least 3 times, although it could have been drafted and vetted earlier in the design process
				BP's decision to use a "long string" to complete the well, despite a "lost circulation event" [long string = "a single continuous wall of steel between the wellhead on the sea floor, and the oil and gas zone at the bottom of the well"]
				Cementing job, choice of nitrogen foam
			2.1 Model failures	Cementing plan was not calculated accurately
			2.4.3 Training failures	BP Well Site Leaders, in consultation with the crew, made a key error and mistakenly concluded the second negative test procedure had confirmed the well's integrity
				BP's onshore engineering staff failed to warn Macondo rig personnel about risks associated with the cementing and temporary abandonment procedure
			1.1 Failure to monitor	The rig crew flawed to monitor pressure in kill line rather than in drill pipe
			5.2 Maintenance failures	Transocean was lax in its maintenance of Deepwater Horizon and other vessels.
			4.1 Communication failure with external entities	BP failed to communicate with its outside contractors, especially failed to consult Halliburton about the cement job
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	failures of communication between an individual and another individual at a greater or lower level of authority within the same group and/or organization.
				BP failed to send the operations note on the temporary abandonment of the well until the morning of the procedure, so, for instance, the rig crew didn't have detailed instructions for performing and interpreting the negative pressure test
View 1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	BP engineers, Halliburton engineers, Transocean engineers and operators, cementing equipment, BOP, pressure test equipment	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Rerouting the returns to various mud pits, making it hard to gauge the amount of drilling mud returned from the well (a key indicator of the well's integrity)
				Directing the hydrocarbon mix through the mud-gas separator and not overboard
				Rig crew also performed several operations during the displacement of the drilling mud that made it difficult to detect the hydrocarbon kick
				Negative pressure test failed to test the well integrity
				Transocean crew's failure to perform risk analysis or plan for problems during the displacement of the drilling mud/fluids with sea water, nor did they have procedures for monitoring the processes or calculating expected pressures
			2.2 Inadequate or incorrect local decisions	Failure to interpret signs of trouble during the cementing job, including having to apply more than four times the design pressure to convert the float valve
			2.4.3 Training failures	Transocean didn't adequately prepare its crew for emergencies like hydrocarbon "kicks" and failed to pass on lessons learned from a recent similar incident; Halliburton poorly supervised the cementing job...
				Despite the unexplained negative pressure test results, BP and possibly Transocean personnel on the rig opted not to perform further tests or consult onshore experts
			2.4.1 Lack of resources	BP's choice of fewer (6) centralizers, despite internal modeling suggesting that it might lead to channeling (regardless of subsequent events, i.e. Halliburton's post-accident modeling); decision-making seems to have been guided by time and cost concerns vs safety and stability of the well. The rig crew also failed to notice that the additional centering rings sent to the rig were the right kind.
			1.1 Failure to monitor	Negative pressure test was flawed monitored and gas and fire system did not monitor the dangerous level of hydrocarbon gas, a kick was not detected and noticed by operators
			5.1 Design failures	cementing plan was not modeled, the geographical complexity was not considered throughly
			5.2 Maintenance failures	Failure to install additional physical barriers during temporary abandonment procedure
			4.2 Peer to Peer communication failure	operators and engineers did not communicate effectively, rig crew did not report suspicious results that caused the engineers aware their inadequate decision

Figure A.33: BP Deepwater Horizon Oil Spill failure analysis table part 2

A.10 Upper Big Branch Mine Explosion

TeCSMART

			Upper Big Branch Mine Explosion	
View 7	Societal View	*Time Scale*	Decades	
		Agents	U.S. society	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	U.S. Government	
		Key Failures	*Key Failure*	*Specific Examples*
			2.3 Inadequate or incorrect global decisions	The degradation of effective government by antigovernment ideology. The company was "receiving pressure" from the agency to spray water in the same area of the mine where Massey wants to study cracks in the mine floor for potential gas emissions
				many work safety experts are quick to note that the lax enforcement over the extraction industries represents a much broader trend, beginning well before Bush took office, and extending well beyond his exit. Along the way, federal enforcement agencies have been stacked, at times, with anti-regulation regulators — many of whom still remain. And the industries have showered millions of dollars on Congress in order to persuade
			5.3 Operating procedure failures	Congress would do well to recognize that trend as lawmakers contemplate reforms as diverse as those governing coal mines, oil rigs and Wall Street. When companies failed to protect their employees, government failed to enforce them to do so
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	MSHA	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Disregarding the documented risk of methane outbursts at UBB.
				Overlooking the deadly potential of a precarious ventilation system
			2.2 Inadequate or incorrect local decisions	Despite the fact that the Upper Big Branch mine was cited dozens of times in the year preceding the disaster for violating ventilation plan requirements, MSHA never cited Upper Big Branch for a flagrant violation. Even as they have asked for more enforcement tools, MSHA officials have not explained why they failed to use the "flagrant" tool at UBB.
				Neglecting to use its regulatory authority to force technological improvements to advance miners' safety
				Allowing the U.S. mine safety system to atrophy
			2.4.3 Training failures	State mine inspectors failed to recognize faulty ventilation and inadequate rock dusting because they lack sufficient training to develop specialized expertise in ventilation, because they do not have an adequate inspection force and because they rely on visual inspections rather than scientific testing to determine whether rock dusting is compliant with state law.
			2.5 Conflict of interest	A number of mine-safety experts have charged that MSHA leaders simply didn't want to confront the powerful mining industry, even in the name of miner safety.
				high-ranking MSHA officials apparently were aware that the agency was falling short in its responsibilities.
			1.1 Failure to monitor	MSHA's lack of transparency further diminishes confidence about the agency's ability to regulate the industry.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 4	Market View	*Time Scale*	Months	
		Agents	U.S. mining industry	
		Key Failures	*Key Failure*	*Specific Examples*
			2.5 Conflict of interest	The reality that powerful industries and their leaders cast long shadows over the state's government is not unique to West Virginia, nor is it unique to the coal industry. It is a problem facing regulators of any large industry.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	Massey Energy Co.	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	The Department of Labor said Massey misrepresented the injury data by as much as 37 percent. Underreporting of that magnitude can certainly skew the data and be the difference between an average or
				Despite Blankenship's protests to the contrary, Massey Energy's safety program in fact appeared to be just a slogan, at least to the workers at UBB.
			3.2 Late response	Massey Energy, which owns the UBB mine, have troubling safety records. We have a large and very wealthy parent corporation with a history of ignoring worker safety and health risks until it is too late
			2.4.2 Inadequate allocation of resources	Both evidence in the mine and testimonial evidence suggests that Massey Energy's management failed to properly ventilate UBB because they did not have adequate resources, knowledge and/or capability to develop a sound, workable ventilation plan to address the particular circumstances of UBB.
			5.3 Operating procedure failures	Despite the detailed requirements outlined in the law, evidence suggests that Massey did not have adequate procedures in place to ensure that the company complied with rock dust requirements.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.34: Upper Big Branch Mine Explosion failure analysis table part 1

TeCSMART				
			Upper Big Branch Mine Explosion	
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	managers, UBB mine	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	A search of citations indicates that on at least two occasions Upper Big Branch was cited for failing to calibrate coal-dust detectors on its equipment, meaning that they might not accurately read levels of coal dust, a possible cause of the explosion.
			3.2 Late response	In the days and months leading up to the explosion, federal investigators had cited the mine for a long list of safety violations. Ultimately, though, they didn't take any steps to close the operation down.
			2.2 Inadequate or incorrect local decisions	management failed to assign crews to rock dust designated areas of the mine each shift
			5.1 Design failures	At Upper Big Branch, physical evidence indicated that ventilation controls were missing at the Ellis Portal construction site. Investigators also found that the airflow traveling to the Bandytown fan from the headgate and tailgate sides of the longwall was restricted because of buildup of water and bad roof.
				The push-pull ventilation system at Upper Big Branch also had a design flaw: its fans were configured so that air was directed in a straight line even though miners worked in areas away from the horizontal path. As a result, air had to be diverted from its natural flow pattern into the working sections on the longwall, Headgate 22, Tailgate 22 and the crossover sections.
			5.3 Operating procedure failures	Likewise, section bosses and foremen appeared to lack a protocol by which they could determine whether the dusting was adequate.
			5.2 Maintenance failures	It's not surprising the two-man hoot owl dust crew had trouble with the orange duster, which was prone to failure because of its age and because it had not been adequately maintained. The lack of maintenance was immediately evident to investigators. Following the explosion, the very first time Massey employees attempted to use the duster to perform MSHA-required dusting, the motor burned up.
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	Managers did not pay attention to the worn-out equipments and operators did not let the managers know how important the maintenance is
View 1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	mining workers, engineers, water-spray system, ventilation system, methane monitors, and mining equipment	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	The monitors were altered and the alarms were bypassed by wire "bridges", which means miners can keep working without knowing the level of dangerous gases
				The operators failed to test spray unit by sending water, and they failed to monitor the methane gas level
				The operator failed to conduct a complete examination to assure compliance with the respirable dust control parameters specified in the methane dust control plan
				The operators ignored the warnings from methane monitors, which finally turned out to be the sign of the explosion
			2.4.3 Training failures	Stover testified that no one had explained to him how much rock dust to apply. About a week prior to the explosion a boss told him the rock dusting he and Young had been doing was inadequate suggesting that they were not applying enough dust which may well have been a result of the difficulty of getting enough dust into the mine.
			2.5 Conflict of interest	Workers bypassed the monitors and alarms so that they can keep working. They ignored the safety requirements underground
			5.2 Maintenance failures	The carbide cutting teeth on a piece of mining equipment inside the mine had worn down, which can increase the number of sparks from the machine. The worn bits likely caused an initial methane ignition
				The water-spray system that helps suppress explosive coal dust wasn't functioning properly
				The dusting, difficult to begin with because the small crew had to cover an extremely large area and contend with mine traffic, was further complicated by the fact that the big orange duster at UBB didn't work properly much of the time
			1.1 Failure to monitor	Operators failed to monitor the methane gas level
				The monitors were altered and the alarms were bypassed by wire "bridges", which means miners can keep

Figure A.35: Upper Big Branch Mine Explosion failure analysis table part 2

A.11 San Esteban Mine Collapse

TeCSMART				
			Chilean Mine Accident	
View 7	Societal View	*Time Scale*	Decades	
		Agents	Chile society	
		Key Failures	*Key Failure*	*Specific Examples*
			2.5 Conflict of interest	Carmon Espinoza, head of the Chilean NGO Programa de Economia del Trabajo (Labour Economy Program) remarked in late August that job insecurities mean miners "for logical reasons pay greater attention to keeping their jobs than to work safety"
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	Chile Government	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Chile failed to regulate inappropriate working schedules and working payments, and it didn't take actions to overcome informal employment.
			5.3 Operating procedure failures	This multiplicity of agencies is, in itself, regarded as a problem. With no clear dividing line between their functions, it can be a matter of chance which agency responds when problems are suspected in a company, and responsibilities can become diluted, sometimes allegedly leading to 'buck passing'.
				Chile failed to establish "coherent, efficient public policies or a national structure in the area of work safety and health."
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	SERNAGEOMIN (Chile's mining regulatory agency)	
		Key Failures	*Key Failure*	*Specific Examples*
			2.2 Inadequate or incorrect local decisions	The government ordered the closure of the San Jose mine after deaths in 2006 and 2007, but a year later a junior official, allegedly exceeding his powers, authorised its reopening without the owners having installed a stairway in the ventilation passages.
			2.4.1 Lack of resources	Chile, where vast fortunes have been made from mining, has only 16 mine inspectors to look after 4,500 mines.
				In an additional problem, the agencies tend to be understaffed, have stretched budgets and complain that their best employees are often headhunted, for higher salaries, by the companies they are responsible for supervising. This problem appears to be particularly acute in SERNAGEOMIN, whose responsibilities include mapping mineral resources and advising the government on the award of mining concessions in addition to supervising mine safety.
			1.1 Failure to monitor	The commission also outlined the responsibility of the National Service of Geology and Mines (Sernageomin), due to their lack of adequate inspections in the mine.
				Chile's regulation enforcement, especially in medium to small-size mines, is a problem
			3.1 Flawed actions including supervision	The government ordered the closure of the San Jose mine after deaths in 2006 and 2007, but a year later a junior official, allegedly exceeding his powers, authorised its reopening without the owners having installed a stairway in the ventilation passages.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 4	Market View	*Time Scale*	Months	
		Agents	Mining industry	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	long workdays, insufficient breaks, low pay, high turnover, and high levels of informal employment
			2.5 Conflict of interest	For many mine owners, it is more profitable to pay fines for breaking mine safety rules than to invest in improving safety conditions for their workers.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	San Esteban Mining Co.	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Mine owners didn't have adequate safety measures in place, required by the authorities
				The underground safety requires the owners to install a stairway in the ventilation passages and check the escape route periodically. However, the owners failed to do any of these
			2.2 Inadequate or incorrect local decisions	The company failed to establish proper working schedules. Miners worked for long time shift.
				Bosses may face charges as unions reveal pit had been closed after deaths but reopened, despite failure to meet safety requirements
				Previous accidents at the San Jose mine -- one as recently as July in which a worker lost a leg -- had shown that the walls of the mine, which has been in operation for over a century, required urgent strengthening. But the owners didn't strenthening them.
			2.5 Conflict of interest	The owners only cared about the production, and failed to pay great attention to the safety issues and workers' health
				owners used high salaries to attract miners to work longer at unsafe mines.
			1.2 Failure to monitor effectively	Previous accidents were not carefully analyzed and unsafe processes were not improved. The company continue production under high safety risks
			5.3 Operating procedure failures	The company did not have adequate safety measures in place.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.36: San Esteban Mine Collapse failure analysis table part 1

TeCSMART				
			Chilean Mine Accident	
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	San Jose mine, mine managers	
		Key Failures	*Key Failure*	*Specific Examples*
			5.1 Design failures	Mine neither had alternative exits, nor included an emergency ladder to allow miners escape from the mine
				The metallic screens, which protect the mine from collapsing, were not installed properly. All tunnels were not supported well, and a lack of support can lead to a collapse
				Engineers failed to design large enough tunnel to avoid collapse
			5.2 Maintenance failures	Previous accidents at the San Jose mine -- one as recently as July in which a worker lost a leg -- had shown that the walls of the mine, which has been in operation for over a century, required urgent strengthening. But the owners didn't strenthening them.
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	The miners neither detect the dangers prior to the collapse, nor notify the owners that the safety facilities were not placed properly
View 1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	miners, ventilation system, emergency escape system	
		Key Failures	*Key Failure*	*Specific Examples*
			2.4.3 Training failures	Miners are lack of safety training and escape exercise
			5.2 Maintenance failures	The refuge didn't have ventilation and energy was cut off. It wasn't in good condition.

Figure A.37: San Esteban Mine Collapse failure analysis table part 2

A.12 Fukushima Nuclear Plant Disaster

TeCSMART				
			Fukushima Daiichi Nuclear Plant Accident	
View 7	Societal View	*Time Scale*	Decades	
		Agents	Japan society	
		Key Failures	*Key Failure*	*Specific Examples*
			2.3 Inadequate or incorrect global decisions	*The underlying issue is the social structure that results in "regulatory capture," and the organizational, institutional, and legal framework that allows individuals to justify their own actions, hide them when inconvenient, and leave no records in order to avoid responsibility.
				Japan rarely tests the limits of the system and training of personnel by using highly unusual events or crafting scenarios that are impossible to recover from. Culturally, the Japanese do not accept failure as a learning opportunity. The Japanese system is largely designed to test the proficiency of the operators in responding to known scenarios. The problem with this approach is that if a scenario has not been incorporated into the design basis, the ability to anticipate and respond is lessened.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	the Kentei (Prime Minster's Office), Japan Government	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	The central government was not only slow in informing municipal governments about the nuclear power plant accident, but also failed to convey the severity of the accident.
				First of all, the group at the Kantei did not understand the proper role the Kantei should have taken in a crisis. A second point is that the direct intervention by the Kantei, including Prime Minister Kan's visit to the Fukushima Daiichi plant, disrupted the chain of command and brought disorder to an already dire situation at the site.
			3.2 Late response	The government, the regulators, TEPCO management, and the Kantei lacked the preparation and the mindset to efficiently operate an emergency response to an accident of this scope.
			2.3 Inadequate or incorrect global decisions	prior to the accident, revision and amendments of laws and regulations were only undertaken on a "patchwork" basis, in response to micro-concerns. The will to make large, significant changes in order to keep in step with the standards of the international community was utterly lacking.
			1.2 Failure to monitor effectively	The laws and regulations governing Japan's nuclear power industry at the time of the accident were outdated relative to those of other countries and, in some cases, obsolete.
				Japan had a system designed specifically to monitor, assess, and report on radioactive releases during emergencies. But, it was ignored during the early stages of the crisis and provided little or no help coordinating analyses and managing communication for the central government.
			1.3 Significant errors in monitoring	Ironically, in bypassing the existing nuclear emergency management system, the central government under the prime minister was solely reliant on information from TEPCO, a company he did not trust. The people he made responsible for dealing with TEPCO and the regulators had little or no experience with nuclear issues and were soon overwhelmed. Moreover, they were reluctant to challenge the views of the
			5.3 Operating procedure failures	Laws and regulations related to nuclear energy have only been revised as stopgap measures, based on actual accidents. They have not been seriously and comprehensively reviewed in line with the accident response and safeguarding measures of an international standard. As a result, predictable risks have not been addressed.
				All of the measures against a severe accident (SA) that were in place in Japan were practically ineffective. The assumptions made in SA countermeasures only included internal issues, such as operational human error, and did not include external factors such as earthquakes and tsunami, even though Japan is known to frequently suffer from these natural events.
			4.1 Communication failure with external entities	The failure of the government's accident response system to function in the early stages was one of the reasons that the Kantei increased its involvement in the response to the accident.
			4.3 Inter-level communication failure	There was great confusion over the evacuation, caused by prolonged shelter-in-place orders and voluntary evacuation orders. Some residents were evacuated to high dosage areas because radiation monitoring information was not provided. Some people evacuated to areas with high levels of radiation and were then neglected, receiving no further evacuation orders until April.
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	The chain of command was disrupted during the emergency.

Figure A.38: Fukushima Nuclear Plant Disaster failure analysis table part 1

TeCSMART				
			Fukushima Daiichi Nuclear Plant Accident	
View 5	Regulatory View	*Time Scale*	Years	
		Agents	NISA, NSC, METI	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	The regulatory agencies would explicitly ask about the operators' intentions whenever a new regulation was to be implemented.
				Since 2006, the regulators and TEPCO were aware of the risk that a total outage of electricity at the Fukushima Daiichi plant might occur if a tsunami were to reach the level of the site. They were also aware of the risk of reactor core damage from the loss of seawater pumps in the case of a tsunami larger than assumed in the Japan Society of Civil Engineers estimation. NISA knew that TEPCO had not prepared any measures to lessen or eliminate the risk, but failed to provide specific instructions to remedy the situation.
				No part of the required reinforcements had been implemented on Units 1 through 3 by the time of the accident. This was the result of tacit consent by NISA for a significant delay by the operators in completing the reinforcement.
			3.2 Late response	The government, the regulators, TEPCO management, and the Kantei lacked the preparation and the mindset to efficiently operate an emergency response to an accident of this scope.
				The Kantei, the regulators and TEPCO all understood the need to vent Unit 1. TEPCO had been reporting to NISA, as was the standard protocol, that it was in the process of venting. But there is no confirmation that the venting decision was conveyed to senior members of METI, or to the Kantei. This failure of NISA's function and the scarcity of information at TEPCO headquarters resulted in the Kantei losing faith in TEPCO.
				The Commission has verified that there was a lag in upgrading nuclear emergency preparedness and complex disaster countermeasures, and attributes this to regulators' negative attitudes toward revising and improving existing emergency plans.
			2.2 Inadequate or incorrect local decisions	The regulators also had a negative attitude toward the importation of new advances in knowledge and technology from overseas. If NISA had passed on to TEPCO measures that were included in the B.5.b subsection of the U.S. security order that followed the 9/11 terrorist action, and if TEPCO had put the measures in place, the accident may have been preventable.
				The regulators should have taken a strong position on behalf of the public, but failed to do so. As they had firmly committed themselves to the idea that nuclear power plants were safe, they were reluctant to actively create new regulations. Further exacerbating the problem was the fact that NISA was created as part of the Ministry of Economy, Trade & Industry (METI), an organization that has been actively promoting nuclear power.
			2.3 Inadequate or incorrect global decisions	prior to the accident, revision and amendments of laws and regulations were only undertaken on a "patchwork" basis, in response to micro-concerns. The will to make large, significant changes in order to keep in step with the standards of the international community was utterly lacking.
			2.1 Model failures	NISA was unprepared for a disaster of this scale, and failed in its function.
			2.4.3 Training failures	The lack of expertise resulted in "regulatory capture," and the postponement of the implementation of relevant regulations.
			2.5 Conflict of interest	The existing regulations primarily are biased toward the promotion of a nuclear energy policy, and not to public safety, health and welfare.
			1.2 Failure to monitor effectively	After the Niigata Earthquake in 2007, it was obvious that the assumption of a complex disaster should be included in nuclear accident prevention measures. Still, NISA continued with countermeasures based on assuming a low probability of a complex disaster. Meanwhile, the government also failed to assume a severe accident or a complex disaster in its comprehensive nuclear disaster drills.
			5.3 Operating procedure failures	The regulators should have taken a strong position on behalf of the public, but failed to do so. As they had firmly committed themselves to the idea that nuclear power plants were safe, they were reluctant to actively create new regulations. Further exacerbating the problem was the fact that NISA was created as part of the Ministry of Economy, Trade & Industry (METI), an organization that has been actively promoting nuclear power.
				The operator (TEPCO), the regulatory bodies (NISA and NSC) and the government body promoting the nuclear power industry (METI), all failed to correctly develop the most basic safety requirements—such as assessing the probability of damage, preparing for containing collateral damage from such a disaster, and developing evacuation plans for the public in the case of a serious radiation release.
				Laws and regulations related to nuclear energy have only been revised as stopgap measures, based on actual accidents. They have not been seriously and comprehensively reviewed in line with the accident response and safeguarding measures of an international standard. As a result, predictable risks have not been addressed.
				Prior to the accident, the regulatory bodies lacked an organizational culture that prioritized public safety over their own institutional wellbeing, and the correct mindset necessary for governance and oversight.
			4.2 Peer to Peer communication failure	Although the intervention of the Kantei contributed to the worsening of the accident, the failure of the Secretariat of the Nuclear Emergency Response Headquarters to gather and share information concerning the development of the accident and the response was a significant factor.
			4.3 Inter-level communication failure	There was great confusion over the evacuation, caused by prolonged shelter-in-place orders and voluntary evacuation orders. Some residents were evacuated to high dosage areas because radiation monitoring information was not provided. Some people evacuated to areas with high levels of radiation and were then neglected, receiving no further evacuation orders until April.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.39: Fukushima Nuclear Plant Disaster failure analysis table part 2

TeCSMART				
			Fukushima Daiichi Nuclear Plant Accident	
View 4	Market View	*Time Scale*	Months	
		Agents	Japan Nuclear Industry	
		Key Failures	*Key Failure*	*Specific Examples*
			n/a	n/a
Communication Channel			*Key Failure*	*Specific Examples*
			5. Structural failures	The chain of command was disrupted during the emergency.
View 3	Management View	*Time Scale*	Months (quarterly)	
		Agents	TEPCO	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	Neither did TEPCO's head office offer sufficient technical support.
				TEPCO crisis communication and management capabilities were also of particular concern to the safety authorities, but it appears that TEPCO did little to fundamentally change its approach.
			3.2 Late response	Delays in taking action contributed to the inappropriate response seen during the accident.
			2.2 Inadequate or incorrect local decisions	While TEPCO headquarters was supposed to provide support to the plant, in reality it became subordinate to the Kantei, and ended up simply relaying the Kantei's intentions. This was a result of TEPCO's mindset, which included a reluctance to take responsibility, epitomized by President Shimizu's inability to clearly report to the Kantei the intentions of the operators at the plant.
				TEPCO did not fulfil its responsibilities as a private corporation, instead obeying and relying upon the government bureaucracy of METI, the government agency driving nuclear policy. At the same time, through the auspices of the FEPC, it manipulated the cozy relationship with the regulators to take the teeth out of regulations.
				researchers repeatedly pointed out the high possibility of tsunami levels reaching beyond the assumptions made at the time of construction, as well as the possibility of core damage in the case of such a tsunami. TEPCO overlooked these warnings, and the small margins of safety that existed were far from adequate for such an emergency situation.
				The reason why TEPCO overlooked the significant risk of a tsunami lies within its risk management mindset—in which the interpretation of issues was often stretched to suit its own agenda.
				TEPCO's management mindset of "obedience to authority" hindered their response. The confusion over the "withdrawal" comment by President Shimizu and the intervention by the Kantei arose from this mindset. Rather than make strong decisions and clearly communicating them to the government, TEPCO insinuated what it thought the government wanted and therefore failed to convey the reality on the ground.
			2.5 Conflict of interest	From TEPCO's perspective, new regulations would have interfered with plant operations and weakened their stance in potential lawsuits. That was enough motivation for TEPCO to aggressively oppose new safety regulations and draw out negotiations with regulators via the Federation of Electric Power Companies (FEPC).
				As the nuclear power business became less profitable over the years, TEPCO's management began to put more emphasis on cost cutting and increasing Japan's reliance on nuclear power. While giving lip service to a policy of "safety first," in actuality, safety suffered at the expense of other management priorities. An emblematic example is the fact that TEPCO did not have the proper diagrams of piping and other instruments at the Daiichi plant. The absence of the proper diagrams was one of the factors that led to a delay in venting at a crucial time during the accident.
			5.1 Design failures	Embroiled in controversy since 1990 for several failures in its nuclear operations, TEPCO saw a series of senior managers resign as part of a ritual process for accepting blame for corporate misconduct, which included falsifying records and submitting false information to the regulators. While honor may have been satisfied, it is not clear that any change in corporate safety culture was achieved.
				The tsunami design bases for the Fukushima NPPs were not consistent with the level of protection required for NPPs. If the return period for a tsunami of the magnitude experienced in Japan is as short as reported (once every 1000 years), a risk-informed regulatory approach would have identified the existing design bases as inadequate.
			5.3 Operating procedure failures	The operator (TEPCO), the regulatory bodies (NISA and NSC) and the government body promoting the nuclear power industry (METI), all failed to correctly develop the most basic safety requirements—such as assessing the probability of damage, preparing for containing collateral damage from such a disaster, and developing evacuation plans for the public in the case of a serious radiation release.
				TEPCO did not plan measures for the IC operation, and had no manual or training regimens, so these are clearly organizational problems.
				TEPCO's manual for emergency response to a severe accident was completely ineffective, and the measures it specified did not function.
				TEPCO had not anticipated a severe earthquake and tsunami event, had no operational procedures to handle an extended SBO scenario, and had not practiced or learned from the Kashiwazaki Kariwa earthquake how to manage and communicate during a crisis.
				Sections in the diagrams of the severe accident instruction manual were missing. Workers not only had to work using this flawed manual, but they were pressed for time, and working in the dark with flash lights as their only light source. The Kantei's (Prime Minster's Office) distrust of TEPCO management was exacerbated by the slow response, but the actual work being done was extremely difficult.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.40: Fukushima Nuclear Plant Disaster failure analysis table part 3

TeCSMART				
			Fukushima Daiichi Nuclear Plant Accident	
View 2	Plant View	*Time Scale*	Real Time (hours/days)	
		Agents	Fukushima Daiichi Nuclear Plant managers, nuclear plant	
		Key Failures	***Key Failure***	***Specific Examples***
			3.1 Flawed actions including supervision	No attempt was made to prepare for depressurization of the RPV until these systems failed, and because of DC power failures and issues with providing alternative compressed nitrogen, depressurization to allow alternative water sources was delayed. Such accident management strategies need to be thought out in advance given the evolution of an accident.
			2.4.3 Training failures	Given the deficiencies in training and preparation—once the total station blackout occurred, including the loss of a direct power source, it was impossible to change the course of events.
			5.1 Design failures	The diesel generators and other internal power equipment, including the power distribution buses, were all located within or nearby the plant, and were inundated by the tsunami that struck soon after. The assumptions about a normal station blackout (SBO) did not include the loss of DC power, yet this is exactly what occurred.
				In addition to the design-basis tsunami being too low, additional flood protection for the batteries was not provided. Only the isolation condenser system was available as a makeup system, and because of lack of instrumentation, it was not clear how well it was working.
			5.3 Operating procedure failures	the guidelines for nuclear plant construction were insufficient at the time the construction permit was granted for Units 1 through 3 in the late 1960's
Communication Channel			***Key Failure***	***Specific Examples***
			n/a	n/a
View 1	Equipment View	*Time Scale*	Real Time (secs/mins)	
		Agents	Fukushima Daiichi Nuclear Plant opeartors, nuclear reactor units	
		Key Failures	***Key Failure***	***Specific Examples***
			3.1 Flawed actions including supervision	There was a back-up 66kV transmission line from the transmission network of Tohoku Electric Power Company, but the back-up line failed to feed Unit 1 via a metal-clad type circuit (M/C) of Unit 1 due to mismatched sockets.
				Recovery work, such as confirming the operation of the isolation condenser (IC) in Unit 1, should have been conducted swiftly because of the loss of DC power, but was not.
			2.2 Inadequate or incorrect local decisions	Priority was given to venting the containment when it should have been given to assuring core cooling, such as by restoring the isolation condenser system at reactor pressure or by lining up alternative water sources into the RPV and depressurizing the reactor system so that low-pressure pumps could be used.

Figure A.41: Fukushima Nuclear Plant Disaster failure analysis table part 4

A.13 India Blackouts

TeCSMART				
			India Blackouts	
View 7	Societal View	*Time Scale*	Decades	
		Agents	India society	
		Key Failures	*Key Failure*	*Specific Examples*
			2.2 Inadequate or incorrect local decisions	Some utilities prefer to draw power from the grid in the form of Unscheduled Interchange rather than availing power from organized market through long term, medium term and short term contracts without much consideration to the grid security. (page 126, para 7)
			3.1 Flawed actions including supervision	Electricity stealing and failures to bill and collect electricity charges as well as low technological efficiency levels, have contributed to the lower overall efficiency. (page 2, para 3)
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 6	Government View	*Time Scale*	Years	
		Agents	India Government	
		Key Failures	*Key Failure*	*Specific Examples*
			3.2 Late response	India has missed every annual target to increase electricity production capacity since 1951,according to a Bloomberg report. The country has seen the gap between demand and supply of power jump to 10.2 percent in March this year, from 7.7 percent in March 2011, according to The New York Times.
			2.2 Inadequate or incorrect local decisions	Agricultural and household electricity prices have been held down to very low levels. The distorted electricity pricing system is viewed as one of the factors behind the demand growth. (page 2, para 1)
				Cheap electricity prices under government policy have power utilities, including state distributors, to remain in the red. (page 2, para 2)
				The government has long said that coal shortages have impacted its ability to support India's massive population. And subsidies, price controls and inadequate investment in resources like coal and natural gas have hurt development of its power sector, according to the NYTimes report.
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 5	Regulatory View	*Time Scale*	Years	
		Agents	National Load Dispatch Center (NLDC), Central Electricity Regulatory Commission(CERC)	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	India has frequent rolling power cuts through the day, and in 2011, 289 million people or 25 percent of India's population had no access to electricity, according to a report from the International Energy Agency.
			3.2 Late response	While massive-scale power outages like the ones that have crippled the North of the country the past two days aren't frequent, India has long had power problems and rolling power-cuts are commonplace in parts of the country.
			2.2 Inadequate or incorrect local decisions	The existing provisions in the regulations for (Grant of Connectivity, Long-term Access and Medium-term Open Access in inter-State Transmission and related matters) permitting connectivity to the grid even without identification of beneficiaries at the time of application are resulting in unforeseen power flows across the synchronous grid. This coupled with unrestricted injection / drawal as Unscheduled Interchange (UI) within the IEGC frequency band results in large difference in power flow in real-time as compared to what was envisaged during planning stage and thereby results in critical loading of the transmission that endangers grid security. (page 126, para 3)
			1.3 Significant errors in monitoring	Under the present regulations there is no cap on the volume of Unscheduled Interchange as long as the frequency is within the stipulated operating range. In the antecedent conditions of both the grid disturbances, the efforts to curtail deviations from schedule failed to bring about the desired results probably because the frequency was within the stipulated operating range. (page 127, para 1)
			5.3 Operating procedure failures	The Regulations allow deviations from the schedule as long as the operating parameters are within the prescribed standards. There have been occasions when the utilities have continued to overdraw/ under inject even at low frequency or over generate/ under draw at high frequency. The various instances of grid indiscipline in the form of noncompliance of various provisions of the IEGC and the directions of RLDCs have been brought to the notice of the Hon'ble CERC in the form of petitions. (page 121, para 4)
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 4	Market View	*Time Scale*	Months	
		Agents	the NEW Grid	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	The Regulations allow deviations from the schedule as long as the operating parameters are within the prescribed standards. There have been occasions when the utilities have continued to overdraw/ under inject even at low frequency or over generate/ under draw at high frequency. The various instances of grid indiscipline in the form of noncompliance of various provisions of the IEGC and the directions of RLDCs have been brought to the notice of the Hon'ble CERC in the form of petitions. (page 121, para 4)
			2.4.1 Lack of resources	While electricity demand has been growing rapidly, India has failed to secure sufficient capacity for electricity generation, transmission and distribution. According to a report by the Indian Ministry of Power, electricity supply capacity has persistently fallen 10% short of peak demand since 2000. (page 2, para 2)
			5.1 Design failures	The load generation scenario in the synchronous Northeast-East-West-North (NEW) grid was highly skewed in the month of July. There was surplus condition in the Western Region (WR) due to high generation availability and heavy under drawal by the constituents of WR. This unscheduled interchange resulted in heavy power flow towards the Northern region from Western and Eastern Region in the antecedent conditions. (secondary consequence) (page 121, para 2)
				The constraints arising from the Unscheduled Interchanges are difficult to forecast and foresee. During the antecedent conditions of both the grid disturbances, the loading of transmission lines was below the thermal limit. (page 124, para 4-5)
				Further large capacity dedicated lines built within the meshed system without adequate redundancies could endanger grid security. (page 126, para 4)
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a

Figure A.42: India Blackouts failure analysis table part 1

TeCSMART				
			India Blackouts	
View 3	Management View	Time Scale	Months (quarterly)	
		Agents	regional power operators, State Load Dispatch Centers (SLDCs)	
		Key Failures	*Key Failure*	*Specific Examples*
			2.2 Inadequate or incorrect local decisions	Inadequate response by State Load Dispatch Centers (SLDCs) to the instructions of Regional Load Dispatch Centres (RLDCs) to reduce over-drawal by the Northern Region utilities and under-drawal/excess generation by the Western Region utilities
			1.2 Failure to monitor effectively	The larger integrated grid has a huge power number, i.e. the change in frequency even for a large change in Load or Generation is small. This situation may lead to dangerously high line loading at far end in case of contingencies like tripping of generating units, as the State utilities operate the grid with limited visibility of the State network and system frequency. This situation may end up with major grid disturbance if the frequency band is wider. (page 127, para 4)
			4.1 Communication failure with external entities	Visualization and situational awareness at the Load Despatch Centres in the antecedent condition as well as during restoration was severely constrained owing to non-availability of real time data at the Load Despatch Centres from a large number of locations. (page 124, para 2)
Communication Channel			*Key Failure*	*Specific Examples*
			4.3 Inter-level communication failure	Inadequate response by State Load Dispatch Centers (SLDCs) to the instructions of Regional Load Dispatch Centres (RLDCs) to reduce over-drawal by the Northern Region utilities and under-drawal/excess generation by the Western Region utilities
View 2	Plant View	Time Scale	Real Time (hours/days)	
		Agents	local power generators, Regional Load Despatch Centers (RLDCs)	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	In both the grid disturbances, failure of defence mechanisms/safety net in the form of load shedding schemes through Under Frequency Relays, Rate of change of frequency relays and islanding schemes in the Northern and Eastern Region were observed. (page 123, para 4)
				Under stressed network conditions, proper behavior of protective systems installed on transmission lines and generating units are vital. However in actual practice there are instances where settings of relays are corrected/changed with change in the fast expanding network. (page 125, para 5)
			2.2 Inadequate or incorrect local decisions	On 30th July, 400 kV Bina-Gwalior-Agra-II was under planned shutdown, while 400 kV Zerda-Kankroli was taken under emergency shutdown. On 31st July also 400 kV Bina- Gwalior-Agra-II was under planned shutdown, and subsequently 400 kV Zerda-Kankroli and Zerda-Bhinmal went under forced outage. This resulted in significant reduction in reliability margins. (page 123, para 1)
			4.2 Peer to Peer communication failure	Weak inter-regional power transmission corridors due to multiple existing outages (both scheduled and forced)
Communication Channel			*Key Failure*	*Specific Examples*
			n/a	n/a
View 1	Equipment View	Time Scale	Real Time (secs/mins)	
		Agents	operators	
		Key Failures	*Key Failure*	*Specific Examples*
			3.1 Flawed actions including supervision	High loading on 400 kV Bina–Gwalior–Agra link
				Loss of 400 kV Bina–Gwalior link due to mis-operation of its protection system
			1.1 Failure to monitor	Non-availability of the SCADA data including absence of status data also results in the operator's inability to run tools such as the State Estimator, Contingency Analysis and other tools which are designed to assist him the operation of the grid. (page 118, para 2) Non-availability of the SCADA data leads to incomplete visualization and situational awareness for the system in the control center. (page 118, para 3)
			4.2 Peer to Peer communication failure	The absence of the primary response from the generators was evident in both the grid disturbances. (page 123, para 6)

Figure A.43: India Blackouts failure analysis table part 2

Appendix B

Ontology Screenshots from Protégé

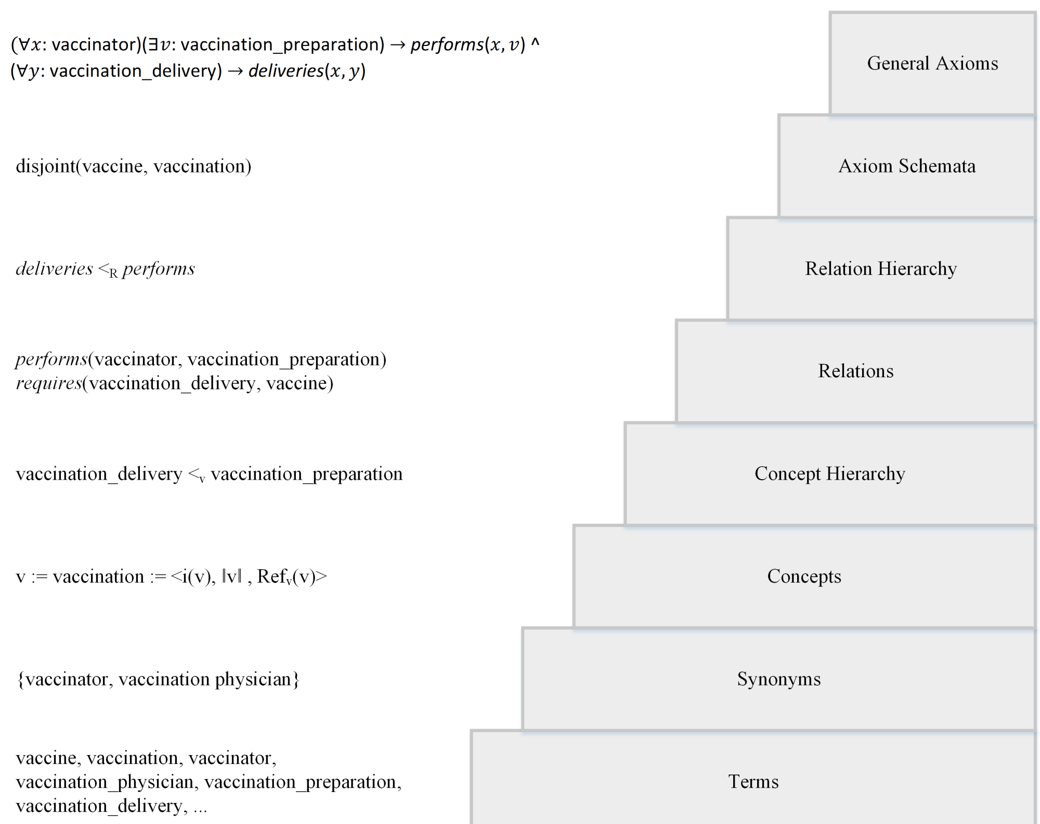


Figure B.1: Ontology layer representation (Adapted from Cimiano [Cimiano, 2006])

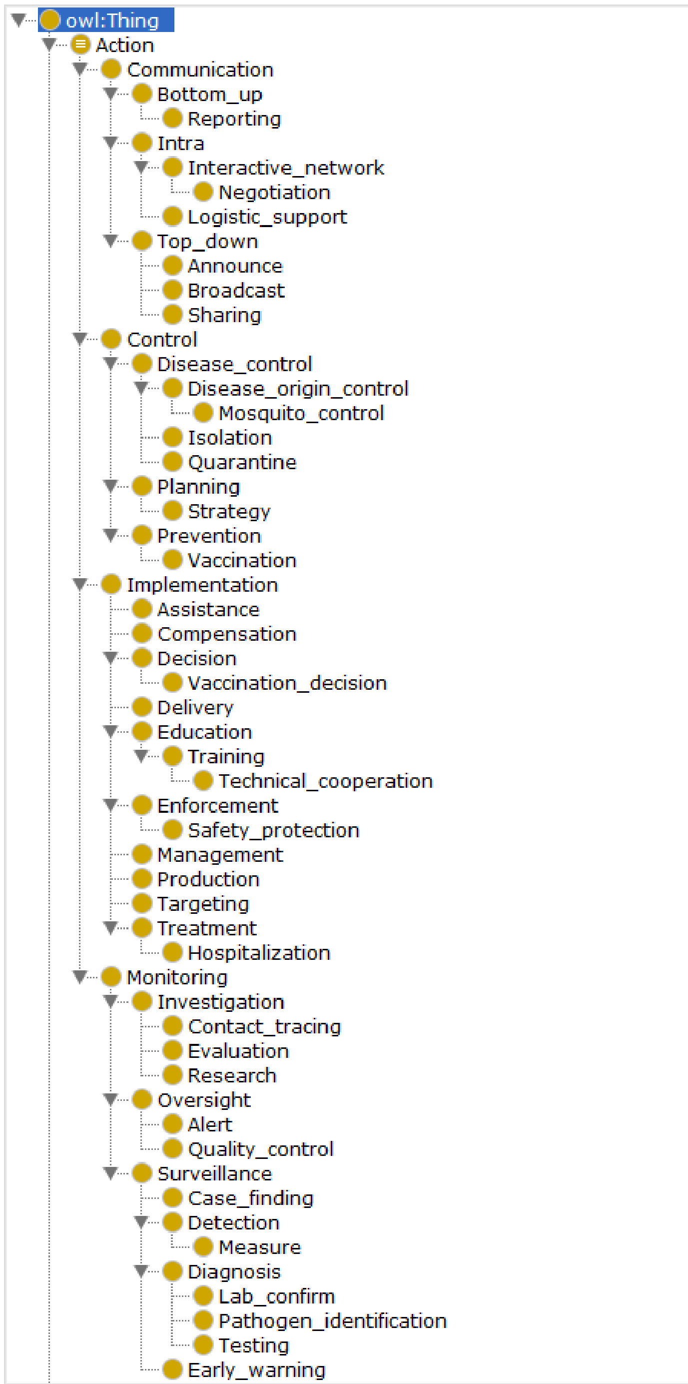


Figure B.2: Ontology classes part 1

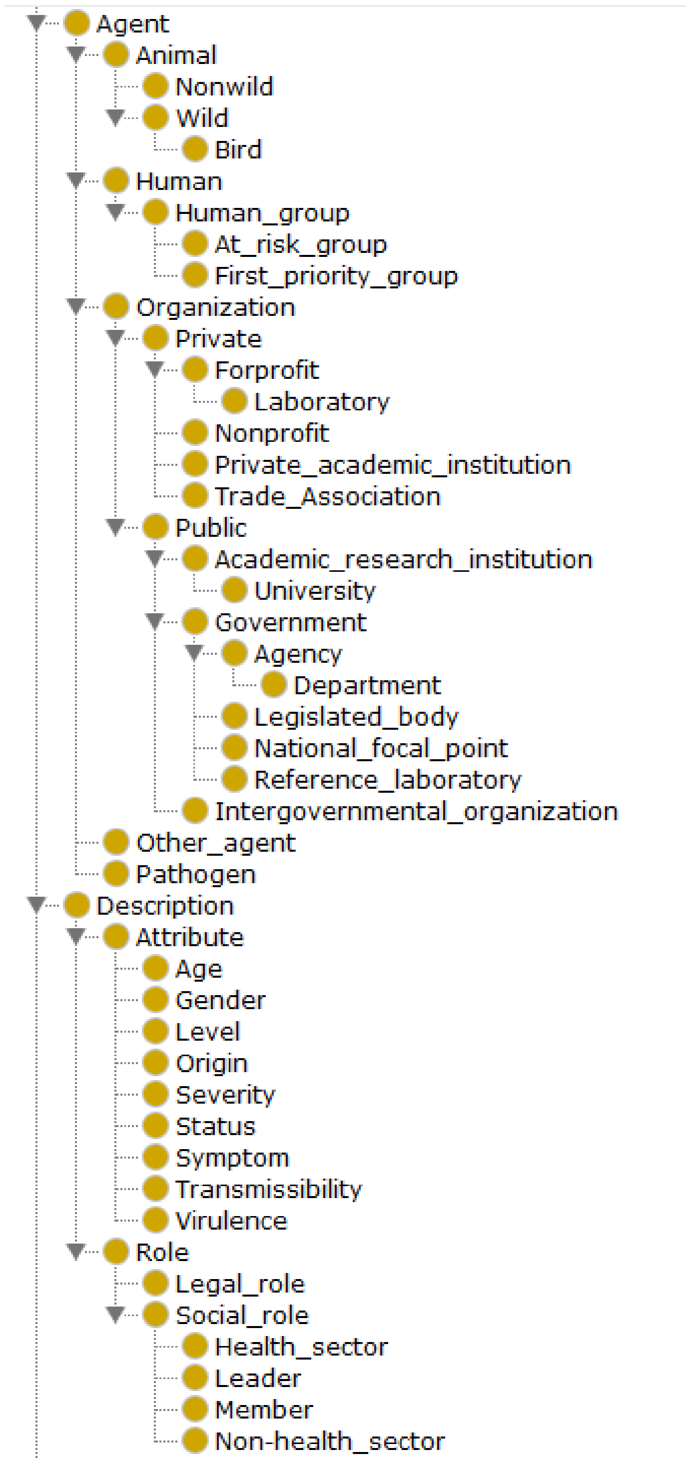


Figure B.3: Ontology classes part 2

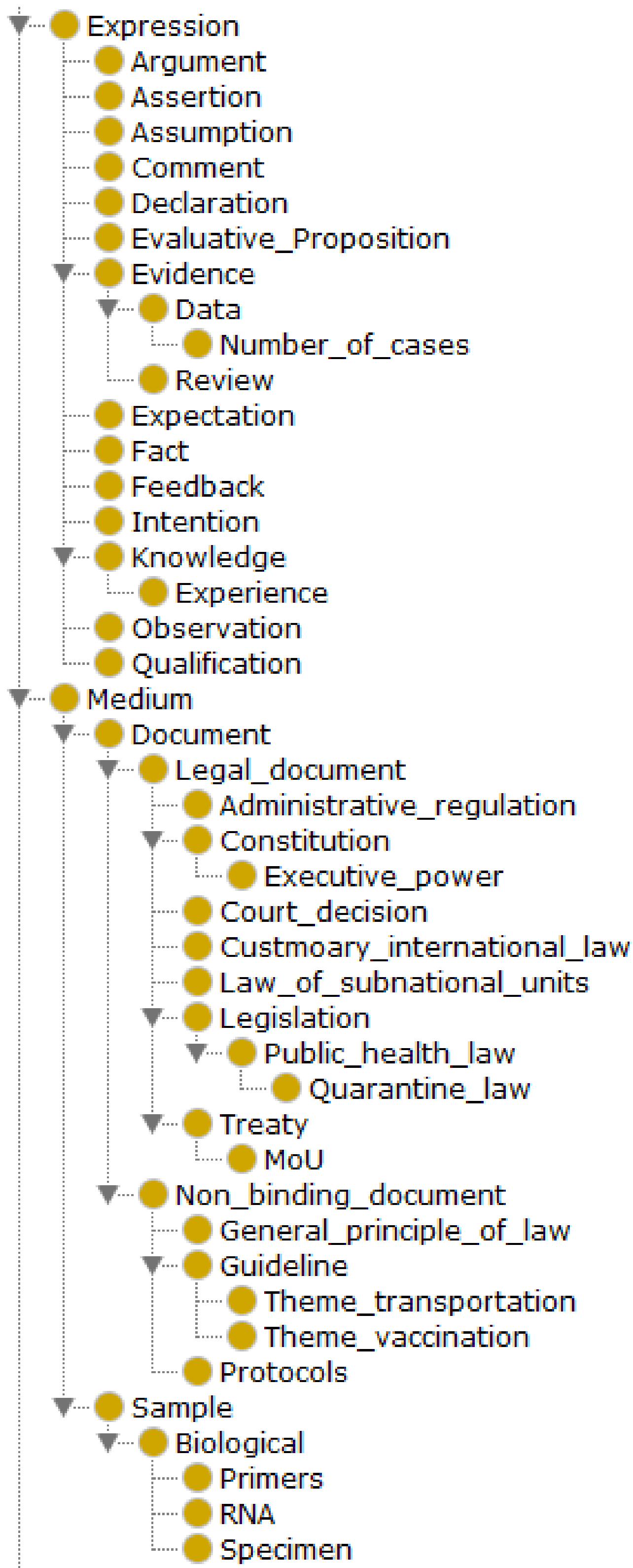


Figure B.4: Ontology classes part 3

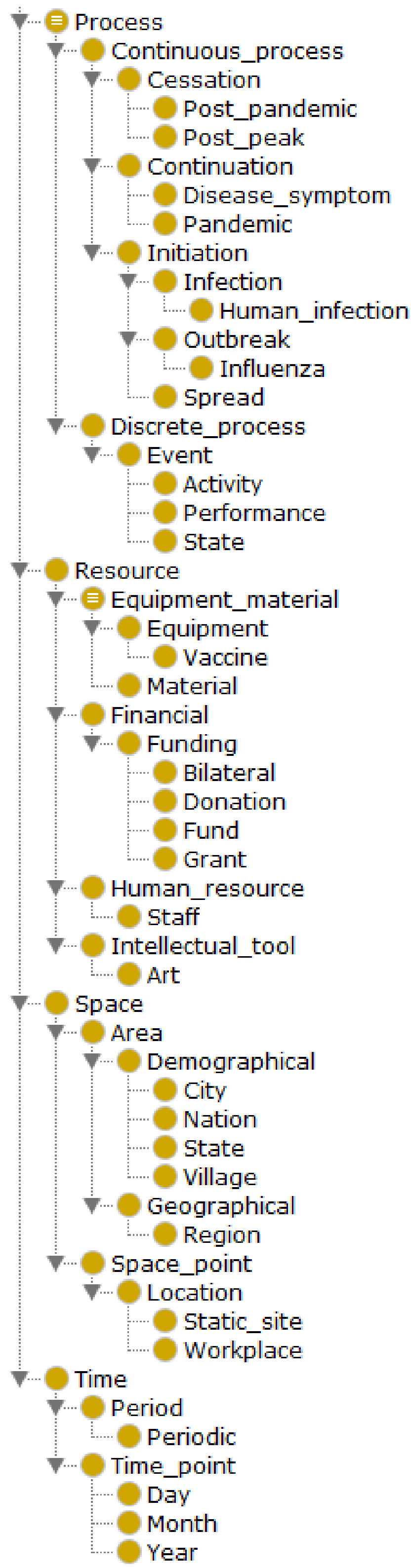


Figure B.5: Ontology classes part 4

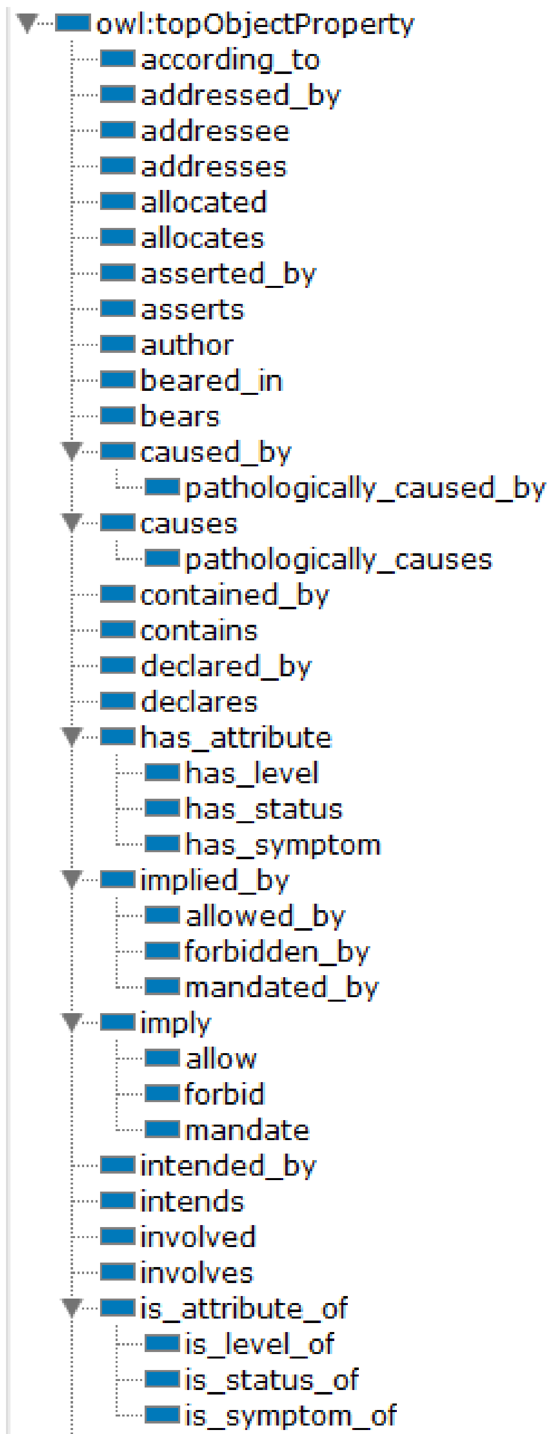


Figure B.6: Ontology properties part 1

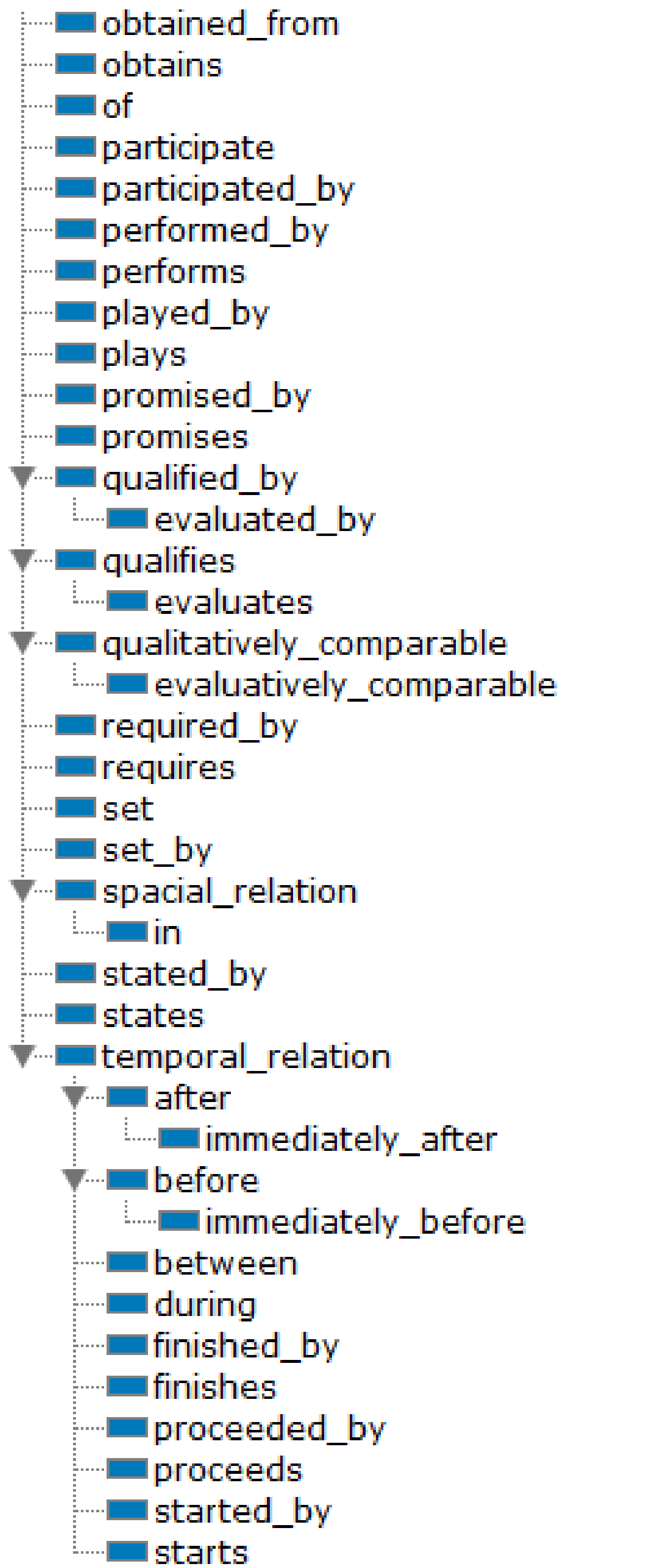


Figure B.7: Ontology properties part 2

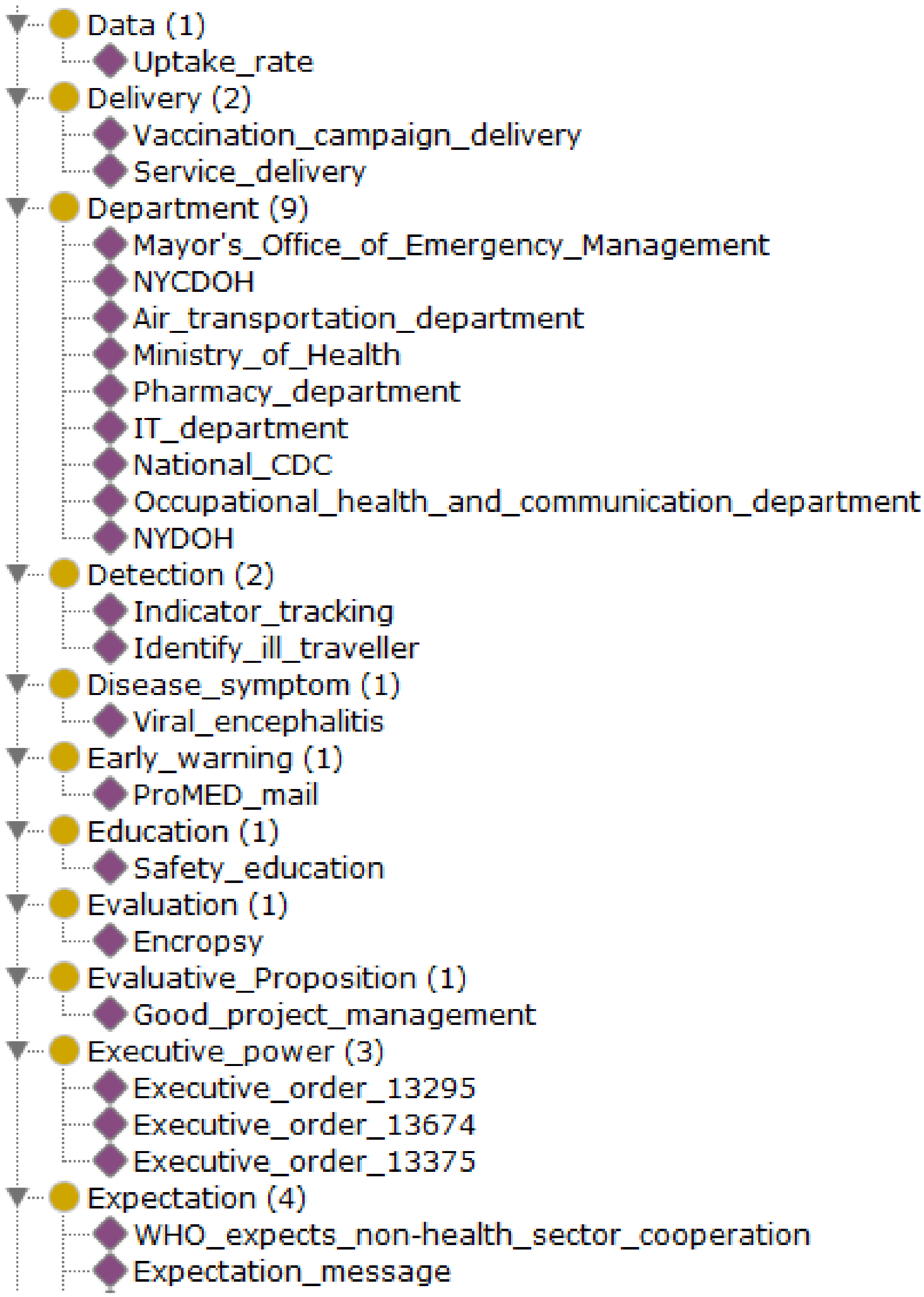


Figure B.8: Ontology individuals (selected)

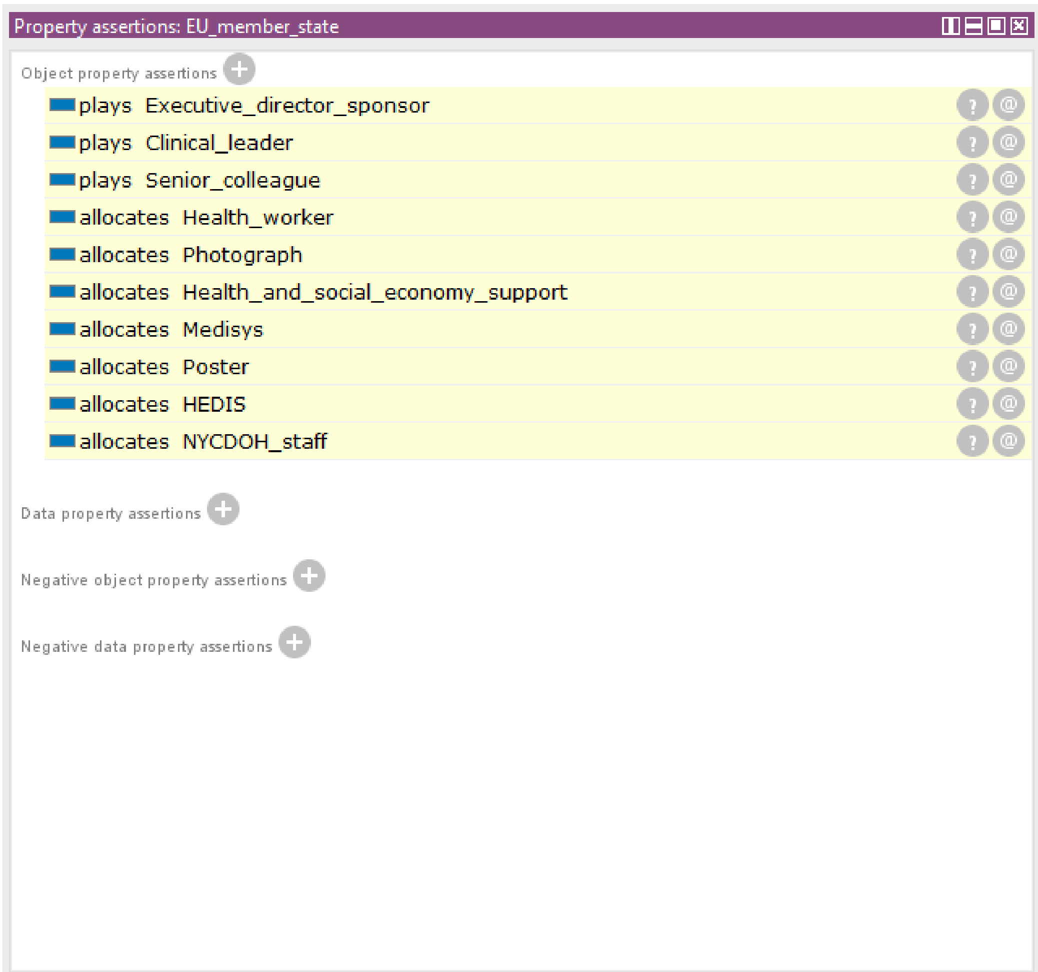


Figure B.9: Reasoning results for “EU_member_stat”

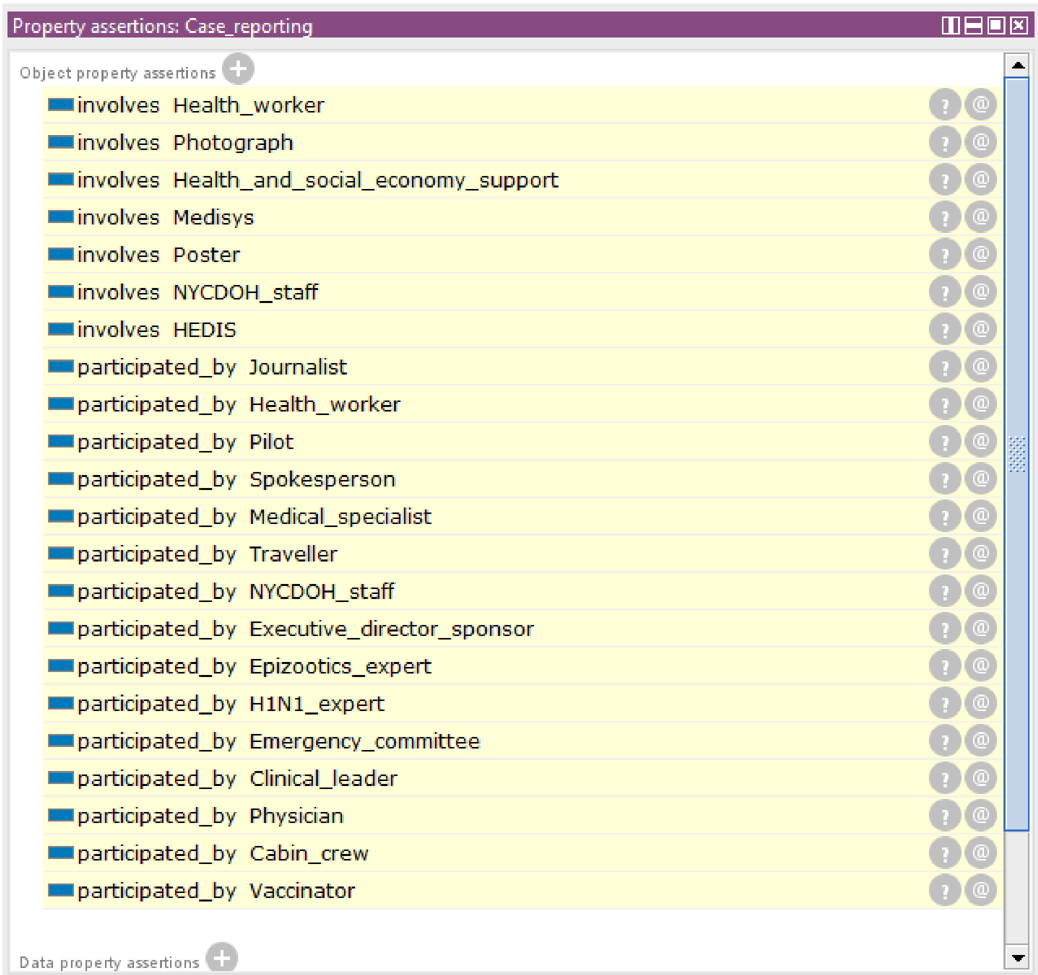


Figure B.10: Reasoning results for “Case_reporting”

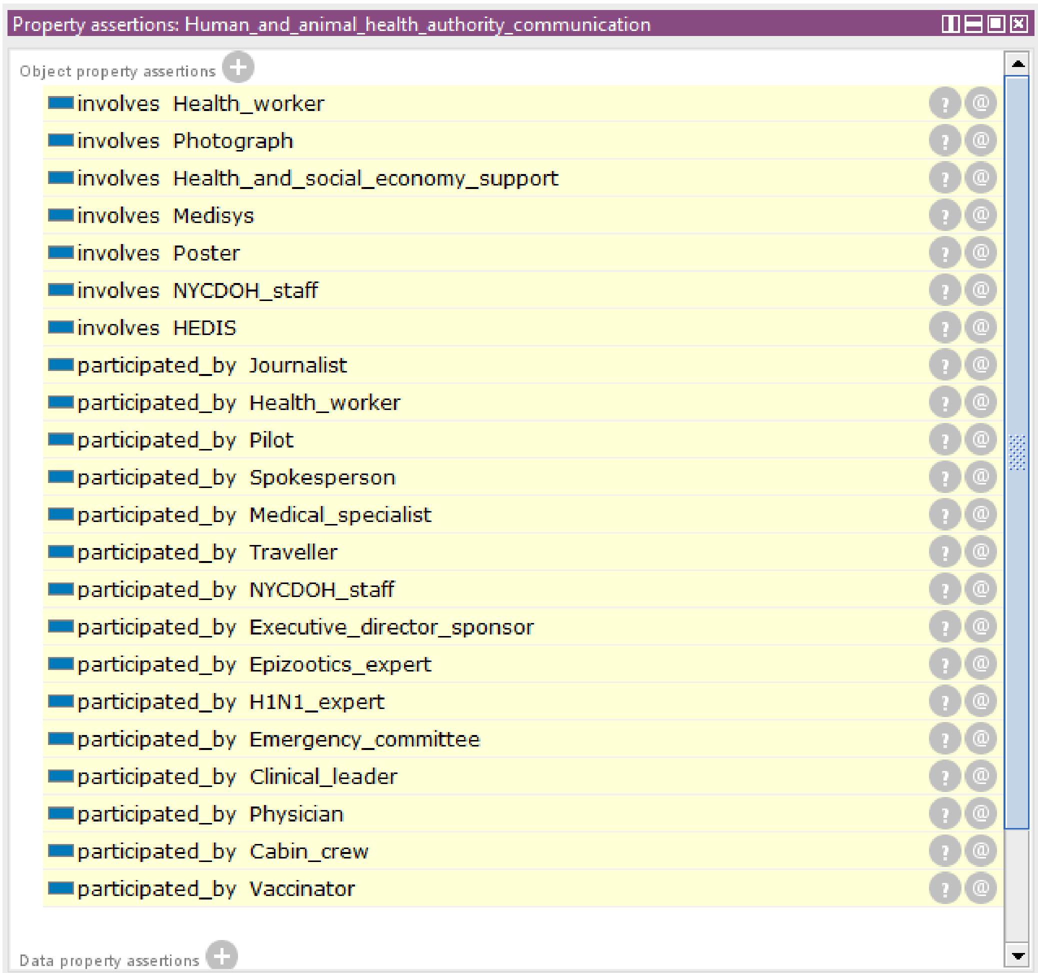


Figure B.11: Reasoning results for "Human_and_animal_health_authority_communication"

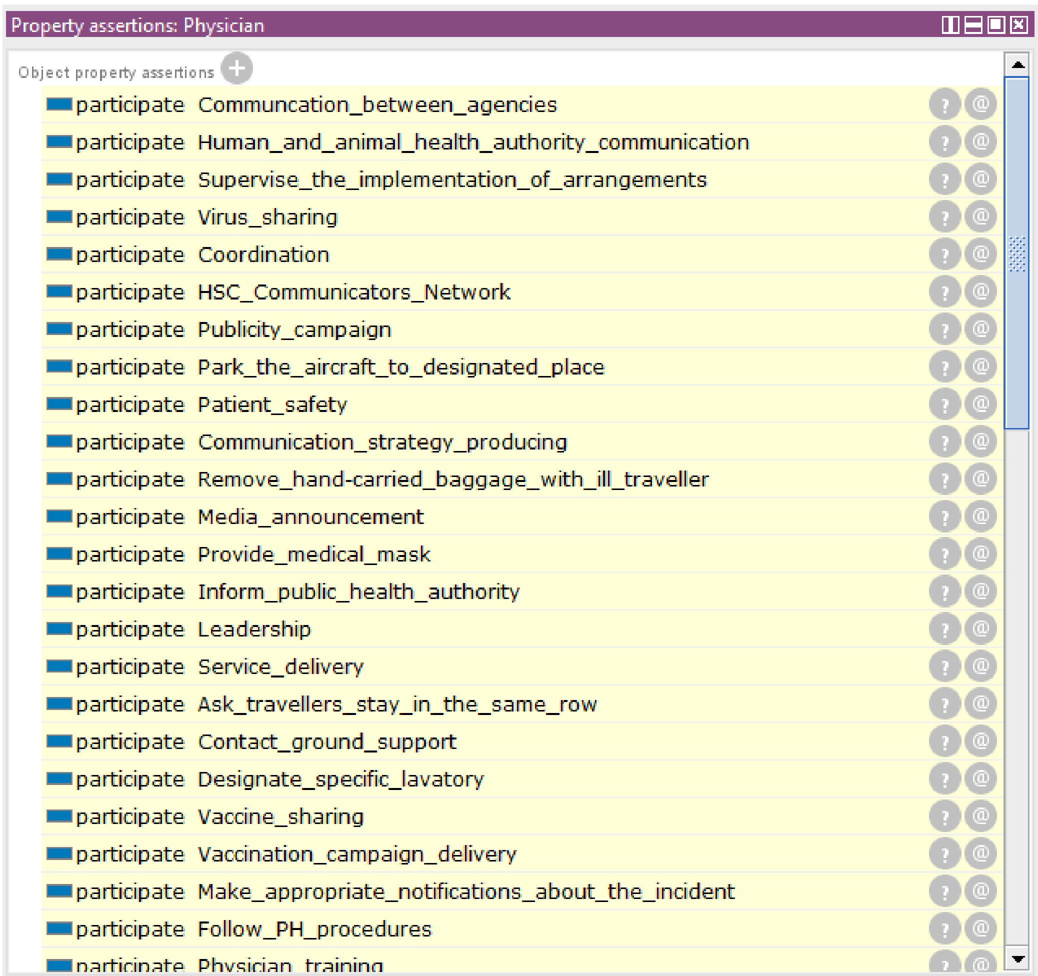


Figure B.12: Reasoning results for “Physician”

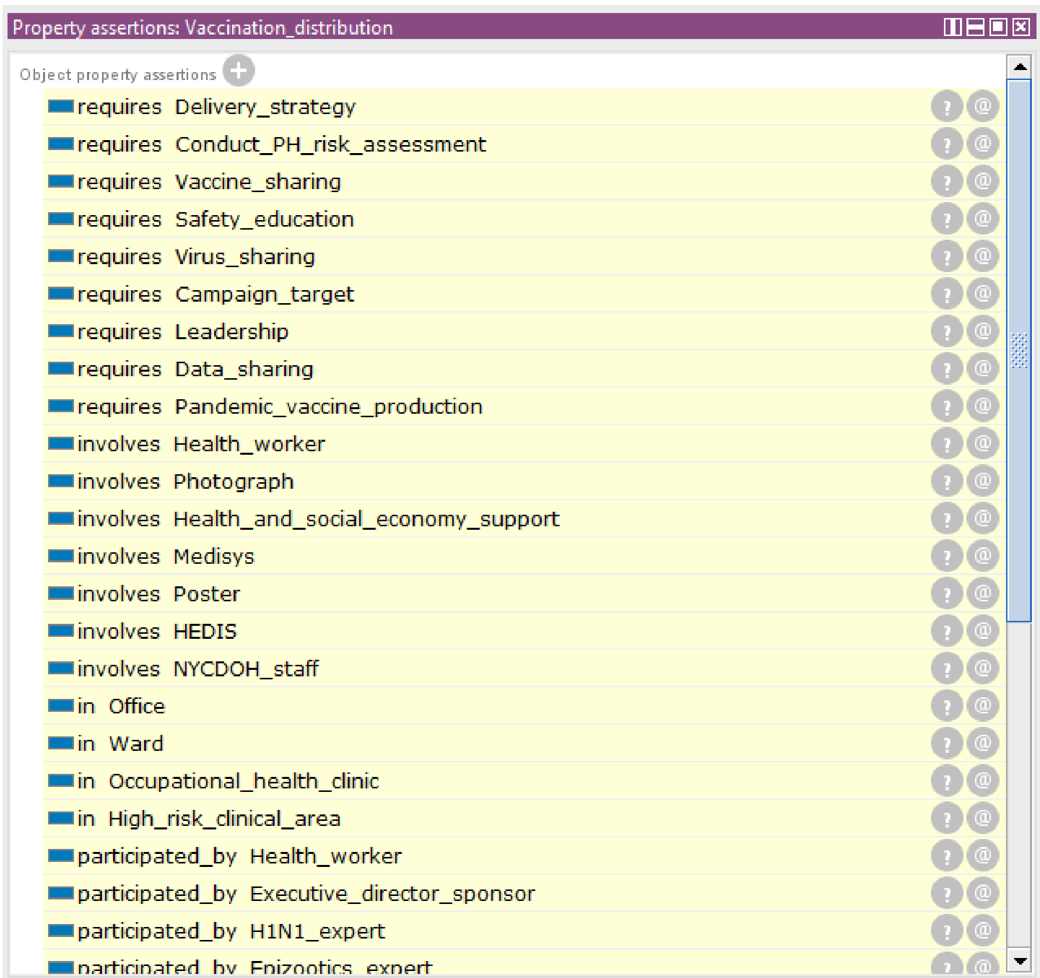


Figure B.13: Reasoning results for "Vaccination distribution"

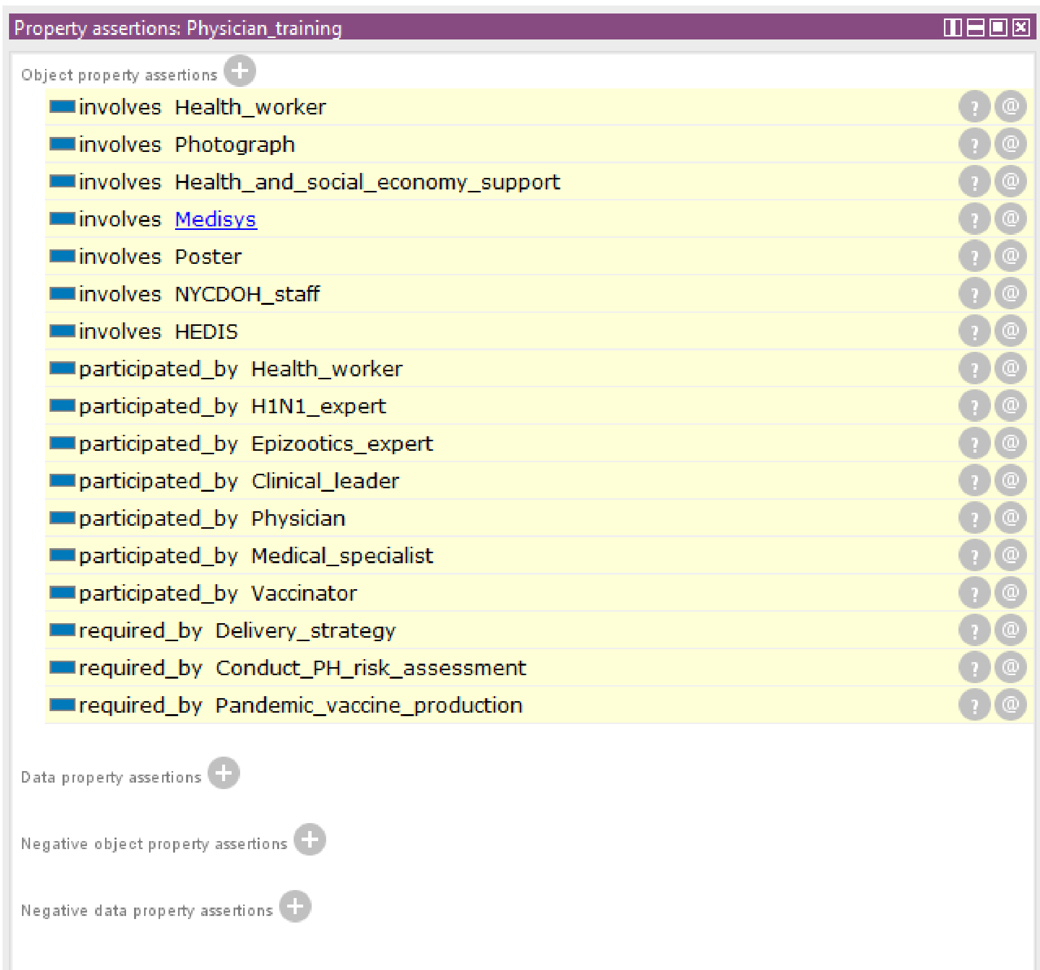


Figure B.14: Reasoning results for "Physician training"

Appendix C

OntoPH SWRL Rules

C.1 SWRL Rules for H1N1 Lessons

C.1.1 Rule 1.1

This rule explains events management during the flight, required by "Case management H1N1 AirTransport guidance" [Organization, 2009b]. Specifically, it extends the expression "Management of event during the flight."

Listing C.1: OntoPH SWRL rule 1.1

```
Guideline(Case_management_H1N1_AirTransport_guidance),
Assertion(Management_of_event_during_the_flight)
-> asserts(Case_management_H1N1_AirTransport_guidance,
Management_of_event_during_the_flight)

Non-health_sector(Cabin_crew), Reporting(?reporting),
asserts(Case_management_H1N1_AirTransport_guidance,
Management_of_event_during_the_flight)
-> participate(Cabin_crew, ?reporting)

Non-health_sector(Cabin_crew), Management(Designate_cabin_crew),
asserts(Case_management_H1N1_AirTransport_guidance,
Management_of_event_during_the_flight)
-> participate(Cabin_crew, Designate_cabin_crew)

Non-health_sector(Cabin_crew), Management(Designate_specific_lavatory),
asserts(Case_management_H1N1_AirTransport_guidance,
Management_of_event_during_the_flight)
-> participate(Cabin_crew, Designate_specific_lavatory)

Non-health_sector(Cabin_crew), Prevention(Provide_medical_mask),
asserts(Case_management_H1N1_AirTransport_guidance,
Management_of_event_during_the_flight)
-> participate(Cabin_crew, Provide_medical_mask)

Non-health_sector(Cabin_crew), Isolation(?isolation),
asserts(Case_management_H1N1_AirTransport_guidance,
Management_of_event_during_the_flight)
-> participate(Cabin_crew, ?isolation)

Non-health_sector(Cabin_crew), Detection(Identify_ill_traveller),
asserts(Case_management_H1N1_AirTransport_guidance,
Management_of_event_during_the_flight)
-> participate(Cabin_crew,Identify_ill_traveller)
```

C.1.2 Rule 1.2

This rule explains pilot in command actions, required by "Case management H1N1 Air-Transport guidance" [Organization, 2009b]. Specifically, it extends the expression "Pilot in command actions."

Listing C.2: OntoPH SWRL rule 1.2

```
Guideline(Case_management_H1N1_AirTransport_guidance),
Knowledge(Pilot_in_command_actions)
-> contains(Case_management_H1N1_AirTransport_guidance,
Pilot_in_command_actions)

Non-health_sector(Pilot), Reporting(?reporting),
contains(Case_management_H1N1_AirTransport_guidance,
Pilot_in_command_actions) -> participate(Pilot, ?reporting)

Legal_role(PH_authority),
Interactive_network(Communication_between_agencies),
contains(Case_management_H1N1_AirTransport_guidance,
Pilot_in_command_actions) -> participate(PH_authority,
Communication_between_agencies)
```

C.1.3 Rule 1.3

This rule describes arrival procedures at airport, required by "Case management H1N1 Air-Transport guidance" [Organization, 2009b]. Specifically, it extends the expression "Arrival airport procedures."

Listing C.3: OntoPH SWRL rule 1.3

```
Guideline(Case_management_H1N1_AirTransport_guidance),
Knowledge(Arrival_airport_procedures)
-> contains(Case_management_H1N1_AirTransport_guidance,
Arrival_airport_procedures)

Non-health_sector(Pilot),
Management(Park_the_aircraft_to_designated_place),
contains(Case_management_H1N1_AirTransport_guidance,
Arrival_airport_procedures) -> participate(Pilot,
Park_the_aircraft_to_designated_place)

Non-health_sector(Traveler), Management(Follow_PH_procedures),
contains(Case_management_H1N1_AirTransport_guidance,
Arrival_airport_procedures) -> participate(Traveler, Follow_PH_procedures)

Non-health_sector(Traveler), Symptom(?symptom),
has_symptom(Traveler, ?symptom),
Reporting(Inform_public_health_authority),
contains(Case_management_H1N1_AirTransport_guidance,
Arrival_airport_procedures) -> participate(Traveler,
Inform_public_health_authority)

Non-health_sector(Cabin_crew), Management(Follow_PH_procedures),
contains(Case_management_H1N1_AirTransport_guidance,
Arrival_airport_procedures) ->
participate(Cabin_crew, Follow_PH_procedures)
```

C.1.4 Rule 1.4

This rule describes public health authority actions at arrival airport, required by "Case management H1N1 AirTransport guidance" [Organization, 2009b]. Specifically, this rule extends the expression "PH authority actions at arrival airport."

Listing C.4: OntoPH SWRL rule 1.4

```
Guideline(Case_management_H1N1_AirTransport_guidance),
Knowledge(PH_authority_actions_at_arrival_airport)
-> contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)

Legal_role(PH_authority),
Intra(Coordinate_with_the_airport_authority),
contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)
-> participate(PH_authority,
Coordinate_with_the_airport_authority)

Legal_role(PH_authority),
Announce(Make_appropriate_notifications_about_the_incident),
contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)
-> participate(PH_authority,
Make_appropriate_notifications_about_the_incident)

Legal_role(PH_authority),
Management(Supervise_the_implementation_of_arrangements),
contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)
-> participate(PH_authority,
Supervise_the_implementation_of_arrangements)

Legal_role(PH_authority),
Management(Ensure_availability_of_appropriate_transport),
contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)
-> participate(PH_authority,
Ensure_availability_of_appropriate_transport)

Legal_role(PH_authority), Strategy(Conduct_PH_risk_assessment),
contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)
-> participate(PH_authority, Conduct_PH_risk_assessment)

Legal_role(PH_authority), Intra(Communication_between_agencies),
contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)
-> participate(PH_authority, Communication_between_agencies)

Legal_role(PH_authority),
Broadcast(Inform_travellers_of_the_health_measures_recommended_by_WHO),
contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)
-> participate(PH_authority,
Inform_travellers_of_the_health_measures_recommended_by_WHO)

Legal_role(PH_authority),
Training(Border_agency_representative_training),
contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)
-> participate(PH_authority,
Border_agency_representative_training)

Legal_role(PH_authority), Detection(Identify_ill_traveller),
contains(Case_management_H1N1_AirTransport_guidance,
PH_authority_actions_at_arrival_airport)
-> participate(PH_authority, Identify_ill_traveller)
```

C.1.5 Rule 2.1

This rule explains vaccination campaign in the U.K., required by "DOH vaccination campaign best practice guidance" [UKDOH, 2010]. Specifically, it extends the expression "Take the vaccination to staff."

Listing C.5: OntoPH SWRL rule 2.1

```
Guideline(DOH_vaccination_campaign_best_practice_guidance),
Assertion(Take_the_vaccination_to_staff)
-> asserts(DOH_vaccination_campaign_best_practice_guidance,
Take_the_vaccination_to_staff)

Social_role(Health_worker), Vaccination(?vaccination),
asserts(DOH_vaccination_campaign_best_practice_guidance,
Take_the_vaccination_to_staff)
-> participate(Health_worker, ?vaccination)
```

C.1.6 Rule 2.2

This rule explains vaccination campaign in the U.K., required by "DOH vaccination campaign best practice guidance" [UKDOH, 2010]. Different from Rule 2.1, it extends the expression "Involve individual sites" and "Establish communication network."

Listing C.6: OntoPH SWRL rule 2.2

```
Guideline(DOH_vaccination_campaign_best_practice_guidance),
Assertion(Involve_individual_sites)
-> asserts(DOH_vaccination_campaign_best_practice_guidance,
Involve_individual_sites)

Guideline(DOH_vaccination_campaign_best_practice_guidance),
Intention(Establish_communication_network)
-> intends(DOH_vaccination_campaign_best_practice_guidance,
Establish_communication_network)

Vaccination(?vaccination), Workplace(?workplace),
asserts(DOH_vaccination_campaign_best_practice_guidance,
Involve_individual_sites)
-> in(?vaccination, ?workplace)

Vaccination(?vaccination), Sharing(?sharing),
intends(DOH_vaccination_campaign_best_practice_guidance,
Establish_communication_network)
-> requires(?vaccination, ?sharing)

Sharing(?sharing), Vaccination(?vaccination),
Workplace(?workplace), in(?vaccination, ?workplace),
requires(?vaccination, ?sharing) -> in(?sharing, ?workplace)
```

C.1.7 Rule 2.3

This rule describes vaccination campaign in the U.K., required by "DOH vaccination campaign best practice guidance" [UKDOH, 2010]. Different from the previous rules, this rule extends the expression "IHR creates a pool of vaccinators."

Listing C.7: OntoPH SWRL rule 2.3

```
Guideline(DOH_vaccination_campaign_best_practice_guidance),
Intention(IHR_creates_a_pool_of_vaccinators)
-> intends(DOH_vaccination_campaign_best_practice_guidance,
IHR_creates_a_pool_of_vaccinators)

Social_role(Vaccinator), Vaccination(?vaccination),
intends(DOH_vaccination_campaign_best_practice_guidance,
IHR_creates_a_pool_of_vaccinators)
-> participate(Vaccinator, ?vaccination)
w
Social_role(Vaccinator), Planning(?planning),
participate(Vaccinator, ?vaccination)
-> participate(Vaccinator, ?planning)

Social_role(Vaccinator), Delivery(?delivery),
participate(Vaccinator, ?vaccination)
-> participate(Vaccinator, ?delivery)

Social_role(Vaccinator), Training(?training),
participate(Vaccinator, ?vaccination)
-> participate(Vaccinator, ?training)
```

C.1.8 Rule 2.4

This rule describes vaccination campaign in the U.K., required by "DOH vaccination campaign best practice guidance" [UKDOH, 2010]. Specifically, this rule extends the expression "Corporate visible and active leadership."

Listing C.8: OntoPH SWRL rule 2.4

```
Guideline(DOH_vaccination_campaign_best_practice_guidance),
Knowledge(Corporate_visible_and_active_leadership)
-> contains(DOH_vaccination_campaign_best_practice_guidance,
Corporate_visible_and_active_leadership)

Vaccination(?vaccination), Management(Leadership),
contains(DOH_vaccination_campaign_best_practice_guidance,
Corporate_visible_and_active_leadership)
-> requires(?vaccination, Leadership)

Leader(?leader), Vaccination(?vaccination),
Management(Leadership), requires(?vaccination, Leadership)
-> participate(?leader, ?vaccination)

Broadcast(?broadcast), Management(Leadership),
Vaccination(?vaccination),
requires(?vaccination, Leadership) ->
requires(Leadership, ?broadcast)

Safety_protection(?safetyprotection), Management(Leadership),
Vaccination(?vaccination), requires(?vaccination, Leadership)
-> requires(Leadership, ?safetyprotection)

Delivery(?delivery), Management(Leadership),
Vaccination(?vaccination),
requires(?vaccination, Leadership) ->
requires(Leadership, ?delivery)
```

C.1.9 Rule 2.5

This rule describes vaccination campaign in the U.K., required by "DOH vaccination campaign best practice guidance" [UKDOH, 2010]. Specifically, it extends the expression "Develop comprehensive strategy."

Listing C.9: OntoPH SWRL rule 2.5

```
Guideline(DOH_vaccination_campaign_best_practice_guidance),
Intention(Develop_comprehensive_strategy)
-> intends(DOH_vaccination_campaign_best_practice_guidance,
Develop_comprehensive_strategy)

Vaccination(?vaccination), Strategy(?strategy),
intends(DOH_vaccination_campaign_best_practice_guidance,
Develop_comprehensive_strategy)
-> requires(?vaccination, ?strategy)

Vaccination(?vaccination), Strategy(?strategy),
Education(Safety_education),
requires(?vaccination, ?strategy) ->
requires(?vaccination, Safety_education)

Strategy(?strategy), Department(?department)
-> performs(?department, ?strategy)

Strategy(?strategy), Periodic(?periodic),
Department(?department),
performs(?department, ?strategy) -> before(?strategy, ?periodic)
```

C.1.10 Rule 2.6

This rule describes vaccination campaign in the U.K., required by "DOH vaccination campaign best practice guidance" [UKDOH, 2010]. Specifically, this rule extends the expression "Element of targeting."

Listing C.10: OntoPH SWRL rule 2.6

```
Guideline(DOH_vaccination_campaign_best_practice_guidance),
Knowledge(Element_of_targeting)
-> contains(DOH_vaccination_campaign_best_practice_guidance,
Element_of_targeting)

Targeting(?targeting), Vaccination(?vaccination),
contains(DOH_vaccination_campaign_best_practice_guidance,
Element_of_targeting)
-> requires(?vaccination, ?targeting)

Targeting(?targeting), Static_site(?staticsite) ->
in(?targeting, ?staticsite)

Vaccination(?vaccination), Targeting(?targeting),
Static_site(?staticsite),
requires(?vaccination, ?targeting), in(?targeting, ?staticsite)
-> in(?vaccination, ?staticsite)
```

C.1.11 Rule 2.7

This rule explains project management, required by "DOH vaccination campaign best practice guidance" [UKDOH, 2010]. Specifically, this rule extends the expression "Good project management."

Listing C.11: OntoPH SWRL rule 2.7

```
Guideline(DOH_vaccination_campaign_best_practice_guidance),
Evaluative_Proposition(Good_project_management)
-> bears(DOH_vaccination_campaign_best_practice_guidance,
Good_project_management)

Strategy(?strategy), Implementation(?implementation),
bears(DOH_vaccination_campaign_best_practice_guidance,
Good_project_management)
-> requires(?strategy, ?implementation)

Strategy(?strategy), Department(?department)
-> performs(?department, ?strategy)

Department(?department), Strategy(?strategy),
Management(Project_management),
requires(?strategy, Project_management),
performs(?department, ?strategy)
-> performs(?department, Project_management)
```

C.1.12 Rule 2.8

This rule demonstrates expectation setting, required by "DOH vaccination campaign best practice guidance" [UKDOH, 2010]. Specifically, this rule extends the expression "Set out expectation message."

Listing C.12: OntoPH SWRL rule 2.8

```
Guideline(DOH_vaccination_campaign_best_practice_guidance),
Expectation(Expectation_message)
-> promises(DOH_vaccination_campaign_best_practice_guidance,
Expectation_message)

Agency(?agency), Guideline(?guideline),
Expectation(Expectation_message),
promises(DOH_vaccination_campaign_best_practice_guidance,
Expectation_message) -> set(?agency, Expectation_message)
```

C.2 SWRL Rules for WHO Pandemic Preparedness Guide

C.2.1 Rule 3.1

This rule describes the role of government, and government leadership in pandemic preparedness and response, required by chapter 3 of "WHO pandemic preparedness response guidance" [Organization, 2009a]. Specifically, this rule extends the expression "WHO expects government leadership."

Listing C.13: OntoPH SWRL rule 3.1

```
Guideline(WHO_pandemic_preparedness_response_guidance),
Expectation(WHO_expects_government_leadership)
-> promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_government_leadership)

Government(?government), Leader(?leader),
promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_government_leadership) ->
plays(?government, ?leader)

Resource(?resource), Government(?government), Leader(?leader),
plays(?government, ?leader) -> allocates(?government, ?resource)

Government(?government), Resource(?resource), Action(?action),
allocates(?government, ?resource) ->
involves(?action, ?resource)
```

C.2.2 Rule 3.2

This rule describes the role of health section, required by chapter 3 of “WHO pandemic preparedness response guidance” [Organization, 2009a]. Specifically, this rule extends the expression “WHO expects health sector guidance.”

Listing C.14: OntoPH SWRL rule 3.2

```
Guideline(WHO_pandemic_preparedness_response_guidance),
Expectation(WHO_expects_health_sector_guidance)
-> promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_health_sector_guidance)

Health_sector(?health_sector), Communication(?communication),
promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_health_sector_guidance)
-> participate(?health_sector, ?communication)

Health_sector(?health_sector), Control(?control),
promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_health_sector_guidance)
-> participate(?health_sector, ?control)

Health_sector(?health_sector), Implementation(?implementation),
promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_health_sector_guidance)
-> participate(?health_sector, ?implementation)
```

C.2.3 Rule 3.3

This rule describes the role of non-health sector, required by chapter 3 of "WHO pandemic preparedness response guidance" [Organization, 2009a]. Specifically, this rule extends the expression "WHO expects non-health sector cooperation."

Listing C.15: OntoPH SWRL rule 3.3

```
Guideline(WHO_pandemic_preparedness_response_guidance),
Expectation(WHO_expects_non-health_sector_cooperation)
-> promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_non-health_sector_cooperation)

Non-health_sector(?nonhealth_sector), Planning(?planning),
promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_non-health_sector_cooperation)
-> participate(?nonhealth_sector, ?planning)

Planning(?planning), Non-health_sector(?nonhealth_sector),
Pandemic(?pandemic), participate(?nonhealth_sector, ?planning)
-> involves(?nonhealth_sector, ?pandemic)

Resource(?resource), Non-health_sector(?nonhealth_sector),
promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_non-health_sector_cooperation)
-> allocates(?nonhealth_sector, ?resource)

Non-health_sector(?nonhealth_sector),
Communication(?communication),
promises(WHO_pandemic_preparedness_response_guidance,
WHO_expects_non-health_sector_cooperation)
-> participate(?nonhealth_sector, ?communication)
```

C.2.4 Rule 3.4

This rule describes the role of WHO, required by chapter 3 of "WHO pandemic preparedness response guidance" [Organization, 2009a]. Specifically, this rule extends the expression "WHO responsibility."

Listing C.16: OntoPH SWRL rule 3.4

```
Guideline(WHO_pandemic_preparedness_response_guidance),
Assertion(WHO_responsibility)
-> asserts(WHO_pandemic_preparedness_response_guidance,
WHO_responsibility)

Intergovernmental_organization(WHO), Interactive(Coordination),
asserts(WHO_pandemic_preparedness_response_guidance,
WHO_responsibility)
-> performs(WHO, Coordination)

Interactive(Coordination), Intergovernmental_organization(WHO),
Treaty(International_health_regulations),
performs(WHO, Coordination) -> requires(Coordination,
International_health_regulations)

Intergovernmental_organization(WHO), Planning(?planning),
asserts(WHO_pandemic_preparedness_response_guidance,
WHO_responsibility)
-> performs(WHO, ?planning)
```

Appendix D

Construct QDE for Level Control Tank System

D.1 Construct QDE

Adapting the linear level control tank example discussed in Section 5.5, we can construct the QDE using QSIM algorithm.

The quantity space is described as follows with landmark values:

$$(h \quad (0 \;\; \text{FULL} \;\; \infty)),$$
$$(h_s \quad (0 \;\; \text{SP} \;\; \infty)),$$
$$(e \quad (-\infty \;\; 0 \;\; \infty)),$$
$$(p \quad (-\infty \;\; 0 \;\; \infty)),$$
$$(q_1 \quad (0 \;\; \infty)),$$
$$(q_2 \quad (0 \;\; \text{IF}_2 \;\; \infty)),$$
$$(f_{out} \quad (0 \;\; \text{OF}_{\text{FULL}} \;\; \infty)),$$
$$(f_{in} \quad (0 \;\; \infty)),$$
$$(f_{net} \quad (-\infty \;\; 0 \;\; \infty)).$$

Then, we can write the qualitative constraints of this system,

$$((- \;\; h_s \;\; h \;\; e) \quad (0 \;\; 0 \;\; 0) \quad (\text{SP} \;\; \text{FULL} \;\; (-\infty \;\; 0 \;\; \infty)) \quad (\infty \;\; \infty \;\; 0)),$$
$$((M^+ \;\; e \;\; p) \quad (-\infty \;\; -\infty) \quad (0 \;\; 0) \quad (-\infty \;\; \infty)),$$
$$((M^+ \;\; p \;\; q_2) \quad (-\infty \;\; 0) \quad (0 \;\; \text{IF}_2) \quad (\infty \;\; \infty)),$$
$$((M^- \;\; h \;\; f_{out}) \quad (0\;0) \quad (\text{FULL} \;\; \text{OF}_{\text{FULL}}) \quad (\infty \;\; \infty)),$$
$$((+ \;\; q_1 \;\; q_2 \;\; f_{in})),$$
$$((- \;\; f_{in} \;\; f_{out} \;\; f_{net})),$$
$$(\frac{d}{dt} \;\; h \;\; f_{net}),$$
$$(\text{constant} \;\; q_1),$$
$$(\text{constant} \;\; h_s).$$

The transition is indicated by the following equation,

$$((h \quad (\text{FULL} \quad inc)) \quad \rightarrow \quad \text{overflow}).$$

D.2 Propagation from Initial State: Scenario I

To understand what is the current state of the system, we propagate the initial state through the system to obtain the system behavior. Assume h_s is at set point SP, q_1 is at IF_1^*, and if initial value of h is smaller than h_s (INIT < SP), we have the quantity space

$$(h \quad (0 \;\; \text{INIT} \;\; \text{SP} \;\; \text{FULL} \;\; \infty)),$$
$$(h_s \quad (0 \;\; \text{SP} \;\; \infty)),$$
$$(e \quad (-\infty \;\; \text{E}_{\text{FULL}} \;\; 0 \;\; \text{E}_{\text{INIT}} \;\; \infty)),$$
$$(p \quad (-\infty \;\; \text{P}_{\text{FULL}} \;\; 0 \;\; \text{P}_{\text{INIT}} \;\; \infty)),$$
$$(q_1 \quad (0 \;\; \text{IF}_1 \;\; \infty)),$$
$$(q_2 \quad (0 \;\; \text{IF}_{\text{FULL}} \;\; \text{IF}_2 \;\; \text{IF}_{\text{INIT}} \;\; \infty)),$$
$$(f_{out} \quad (0 \;\; \text{OF}_{\text{INIT}} \;\; \text{OF}_{\text{SP}} \;\; \text{OF}_{\text{FULL}} \;\; \infty)),$$
$$(f_{in} \quad (\text{IF}_1 \;\; \text{IF}_{\text{FULL}} \;\; \text{IF} \;\; \text{IF}_{\text{INIT}} \;\; \infty)),$$
$$(f_{net} \quad (-\infty \;\; \text{NF}_{\text{FULL}} \;\; 0 \;\; \text{NF}_{\text{INIT}} \;\; \infty)).$$

The initial state t_0 is,

$$(h \quad (\text{INIT}) \quad ?).$$

Propagating through the constraints, we have

1. $h = (\text{INIT}) \quad \rightarrow \quad e = (\text{E}_{\text{INIT}})$,
2. $e = (\text{E}_{\text{INIT}}) \quad \rightarrow \quad p = (\text{P}_{\text{INIT}})$,
3. $p = (\text{P}_{\text{INIT}}) \quad \rightarrow \quad q_2 = (\text{IF}_{\text{INIT}})$,
4. $q_2 = (\text{IF}_{\text{INIT}}) \quad \rightarrow \quad f_{in} = (\text{IF}_{\text{INIT}})$,
5. $h = (\text{H}_{\text{INIT}}) \quad \rightarrow \quad f_{out} = (\text{OF}_{\text{INIT}})$,
6. $f_{in},\ f_{out} \quad \rightarrow \quad f_{net} = (\text{NF}_{\text{INIT}})$,
7. $f_{net} = (\text{NF}_{\text{INIT}}) \quad \rightarrow \quad \frac{dh}{dt} > 0 \quad \rightarrow \quad \text{dir}_h = \text{inc}.$

So the complete initial state is

$$
\begin{array}{ll}
(h \quad (\text{INIT}) \quad \text{inc}), & (q_2 \quad (\text{IF}_{\text{INIT}}) \quad \text{dec}), \\
(h_s \quad (\text{SP}) \quad \text{std}), & (f_{out} \quad (\text{OF}_{\text{INIT}}) \quad \text{inc}), \\
(e \quad (\text{E}_{\text{INIT}}) \quad \text{dec}), & (f_{in} \quad (\text{IF}_{\text{INIT}}) \quad \text{dec}), \\
(p \quad (\text{P}_{\text{INIT}}) \quad \text{dec}), & (f_{net} \quad (\text{NF}_{\text{INIT}}) \quad \text{dec}), \\
(q_1 \quad (\text{IF}_1)\ \text{std}), & (\frac{dh}{dt} \quad (\text{NF}_{\text{INIT}}) \quad \text{dec}).
\end{array}
$$

Move to the time point (t_0, t_1), the current state is

$$
\begin{array}{ll}
(h \quad (\text{INIT} \;\; \text{FULL}) \quad \text{inc}), & (q_2 \quad (\text{IF}_2 \;\; \text{IF}_{\text{INIT}}) \quad \text{dec}), \\
(h_s \quad (\text{SP}) \quad \text{std}), & (f_{out} \quad (\text{OF}_{\text{INIT}} \;\; \text{OF}_{\text{SP}}) \quad \text{inc}), \\
(e \quad (0 \;\; \text{E}_{\text{INIT}}) \quad \text{dec}), & (f_{in} \quad (\text{IF} \;\; \text{IF}_{\text{INIT}}) \quad \text{dec}), \\
(p \quad (0 \;\; \text{P}_{\text{INIT}}) \quad \text{dec}), & (f_{net} \quad (0 \;\; \text{NF}_{\text{INIT}}) \quad \text{dec}), \\
(q_1 \quad (\text{IF}_1)\ \text{std}), & (\frac{dh}{dt} \quad (0 \;\; \text{NF}_{\text{INIT}}) \quad \text{dec}).
\end{array}
$$

At t_1, we have the final state as following

$$
\begin{array}{ll}
(h \quad (\text{SP}) \quad \text{std}), & (q_2 \quad (\text{IF}_2) \quad \text{std}), \\
(h_s \quad (\text{SP}) \quad \text{std}), & (f_{out} \quad (\text{OF}_{\text{SP}}) \quad \text{std}), \\
(e \quad (0) \quad \text{std}), & (f_{in} \quad (\text{IF}) \quad \text{std}), \\
(p \quad (0) \quad \text{std}), & (f_{net} \quad (0) \quad \text{std}), \\
(q_1 \quad (\text{IF}_1)\ \text{std}), & (\frac{dh}{dt} \quad (0) \quad \text{std}).
\end{array}
$$

D.3 Propagation from Initial State: Scenario II

What if INIT > SP? We have a different initial state, but it turns out that the steady state is the same as we propagating the initial state through the constraints. The quantity space in this case is,

$(h \quad (0 \;\; \text{SP} \;\; \text{INIT} \;\; \text{FULL} \;\; \infty))$,
$(h_s \quad (0 \;\; \text{SP} \;\; \infty))$,
$(e \quad (-\infty \;\; \text{E}_{\text{FULL}} \;\; \text{E}_{\text{INIT}} \;\; 0 \;\; \infty))$,
$(p \quad (-\infty \;\; \text{P}_{\text{FULL}} \;\; \text{P}_{\text{INIT}} \;\; 0 \;\; \infty))$,
$(q_1 \quad (0 \;\; \text{IF}_1 \;\; \infty))$,
$(q_2 \quad (0 \;\; \text{IF}_{\text{FULL}} \;\; \text{IF}_{\text{INIT}} \;\; \text{IF}_2 \;\; \infty))$,
$(f_{out} \quad (0 \;\; \text{OF}_{\text{INIT}} \;\; \text{OF}_{\text{SP}} \;\; \text{OF}_{\text{FULL}} \;\; \infty))$,
$(f_{in} \quad (\text{IF}_1 \;\; \text{IF}_{\text{FULL}} \;\; \text{IF}_{\text{INIT}} \;\; \text{IF} \;\; \infty))$,
$(f_{net} \quad (-\infty \;\; \text{NF}_{\text{FULL}} \;\; \text{NF}_{\text{INIT}} \;\; 0 \;\; \infty))$.

The initial state t_0 is,

$$(h \quad (\text{INIT}) \quad ?).$$

By propagating the initial state through the constraints, we have

1. $h = (\text{INIT}) \quad \rightarrow \quad e = (\text{E}_{\text{INIT}})$,
2. $e = (\text{E}_{\text{INIT}}) \quad \rightarrow \quad p = (\text{P}_{\text{INIT}})$,
3. $p = (\text{P}_{\text{INIT}}) \quad \rightarrow \quad q_2 = (\text{IF}_{\text{INIT}})$,
4. $q_2 = (\text{IF}_{\text{INIT}}) \quad \rightarrow \quad f_{in} = (\text{IF}_{\text{INIT}})$,
5. $h = (\text{H}_{\text{INIT}}) \quad \rightarrow \quad f_{out} = (\text{OF}_{\text{INIT}})$,
6. $f_{in},\ f_{out} \quad \rightarrow \quad f_{net} = (\text{NF}_{\text{INIT}})$,
7. $f_{net} = (\text{NF}_{\text{INIT}}) \quad \rightarrow \quad \frac{dh}{dt} < 0 \quad \rightarrow \quad \text{dir}_h = \text{dec}$.

So the complete initial state is

$$\begin{array}{ll}
(h \quad (\text{INIT}) \quad \text{dec}), & (q_2 \quad (\text{IF}_{\text{INIT}}) \quad \text{inc}), \\
(h_s \quad (\text{SP}) \quad \text{std}), & (f_{out} \quad (\text{OF}_{\text{INIT}}) \quad \text{dec}), \\
(e \quad (\text{E}_{\text{INIT}}) \quad \text{inc}), & (f_{in} \quad (\text{IF}_{\text{INIT}}) \quad \text{inc}), \\
(p \quad (\text{P}_{\text{INIT}}) \quad \text{inc}), & (f_{net} \quad (\text{NF}_{\text{INIT}}) \quad \text{inc}), \\
(q_1 \quad (\text{IF}_1)\ \text{std}), & (\dfrac{dh}{dt} \quad (\text{NF}_{\text{INIT}}) \quad \text{inc}).
\end{array}$$

At (t_0, t_1), the state is

$$
\begin{array}{ll}
(h \quad (0 \ \ \mathrm{INIT}) \quad \mathrm{dec}), & (q_2 \quad (\mathrm{IF_{INIT}} \ \ \mathrm{IF_2}) \quad \mathrm{inc}), \\
(h_s \quad (\mathrm{SP}) \quad \mathrm{std}), & (f_{out} \quad (\mathrm{OF_{SP}} \ \ \mathrm{OF_{INIT}}) \quad \mathrm{dec}), \\
(e \quad (\mathrm{E_{INIT}} \ \ 0) \quad \mathrm{inc}), & (f_{in} \quad (\mathrm{IF_{INIT}} \ \ \mathrm{IF}) \quad \mathrm{inc}), \\
(p \quad (\mathrm{P_{INIT}} \ \ 0) \quad \mathrm{inc}), & (f_{net} \quad (\mathrm{NF_{INIT}} \ \ 0) \quad \mathrm{inc}), \\
(q_1 \quad (\mathrm{IF_1}) \ \mathrm{std}), & (\frac{dh}{dt} \quad (\mathrm{NF_{INIT}} \ \ 0) \quad \mathrm{inc}).
\end{array}
$$

Finally, at t_1, the final state obtained is

$$
\begin{array}{ll}
(h \quad (\mathrm{SP}) \quad \mathrm{std}), & (q_2 \quad (\mathrm{IF_2}) \quad \mathrm{std}), \\
(h_s \quad (\mathrm{SP}) \quad \mathrm{std}), & (f_{out} \quad (\mathrm{OF_{SP}}) \quad \mathrm{std}), \\
(e \quad (0) \quad \mathrm{std}), & (f_{in} \quad (\mathrm{IF}) \quad \mathrm{std}), \\
(p \quad (0) \quad \mathrm{std}), & (f_{net} \quad (0) \quad \mathrm{std}), \\
(q_1 \quad (\mathrm{IF_1}) \ \mathrm{std}), & (\frac{dh}{dt} \quad (0) \quad \mathrm{std}).
\end{array}
$$