STAMP Applied to Fukushima Daiichi Nuclear Disaster and the Safety of Nuclear Power Plants in Japan

by

Daisuke Uesako

M.E., Environmental & Ocean Engineering, University of Tokyo, 2007
B.E., Systems Innovation, University of Tokyo, 2005

Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

June 2016

© 2016 Daisuke Uesako. All rights reserved.

The author hereby grants to MIT permission to reproduce
and to distribute publicly paper and electronic
copies of this thesis document in whole or in part
in any medium now known or hereafter created.

Signature of Author: _____

Daisuke Uesako
System Design and Management Program
May 6, 2016

Certified by: _____

Nancy Leveson
Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: _____

Patrick Hale
Director
System Design and Management Program

[Page intentionally left blank]

STAMP applied to Fukushima Daiichi nuclear disaster and the safety of nuclear power plants in Japan

by

Daisuke Uesako

Submitted to the System Design and Management Program
on May 6, 2016 in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

ABSTRACT

On March 11, 2011, a huge tsunami generated after the Great East Japan Earthquake triggered an extremely severe nuclear accident at the Fukushima Daiichi Nuclear Power Plant. This thesis analyzes why the stakeholders could not prevent the Fukushima Daiichi nuclear disaster, and, with regard to the future nuclear safety in Japan, what the potentially hazardous control actions could be. Because of the complex sociotechnical nature of nuclear power plants, System-Theoretic Accident Model and Processes (STAMP)—specifically, Causal Analysis based on STAMP (CAST) and System-Theoretic Process Analysis (STPA)—is used for these analyses.

The CAST process reveals the whole picture of the unsafe control actions by multiple stakeholders, as well as their flawed communication and coordination, which significantly damped the overall control structure for the Fukushima Daiichi Nuclear Power Plant. It becomes clear that all the stakeholders were inadequate to fulfill their safety requirements regarding the safety design, safety management and emergency response. The shared notion of the "Safety Myth," which emerged as an "explanation on safety" for the purpose of promoting the use of nuclear power and was enhanced, among others, by administrative issues such as lack of leadership on nuclear safety, flawed safety culture, lack of resources at the regulatory bodies and bureaucracy, restricted the efforts by the stakeholders to ensure the actual safety against severe accidents or compound nuclear disasters.

The STPA process identifies a number of unsafe control actions in the control structure for the safety of nuclear power plants in Japan, the causal scenarios by which these unsafe control actions could occur, and possible safety requirements to prevent these causal scenarios. It is demonstrated that, despite extensive improvements by the stakeholders after the Fukushima Daiichi nuclear disaster including the establishment of a new regulatory body, the "Safety Myth" or administrative issues might still come into play as causal factors, while investment for safety and sound safety culture can be possible safety requirements that subdue these causal factors.

Finally, recommendations to strengthen the current safety control structure are developed for some key stakeholders, based on the findings of these analyses.

Thesis Supervisor: Nancy Leveson
Title: Professor of Aeronautics and Astronautics

[Page intentionally left blank]

ACKNOWLEDGMENTS

I would first like to thank my thesis advisor Professor Nancy Leveson of the Department of the Aeronautics and Astronautics at Massachusetts Institute of Technology (MIT). She showed me a new way to look at system safety, and when I asked her to become my thesis advisor, she gladly accepted my request, stating her passion for my research interest. She consistently allowed this paper to be my own work, but steered me in the right direction.

I would also like to thank Doctor Bryan Moser of the System Design and Management (SDM) Program at MIT, who gave me valuable insights in the conceptual stage of my research, and Professor John Carroll, the Gordon Kaufman Professor of Management at MIT, who taught me the managerial aspects of nuclear safety and gave me the name of a professor specifically working on those of the Fukushima Daiichi. Without their passionate participation and input, this research could not have been successfully formed or conducted.

I would also like to acknowledge Doctor Masaru Nagura, an SDM fellow, who willingly shared with me his work experience at the Nuclear Regulation Authority (NRA), Japan, and I am gratefully indebted to him for his valuable inputs on NRA.

Finally, I must express my very profound gratitude to my employer—the Ministry of the Environment, Japan—, my friends, and especially my parents for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Daisuke Uesako
Cambridge, Massachusetts
May 2016

Contents

Chapter 1. Introduction 9

1.1 The Nuclear Disaster 9
1.2 History of Nuclear Industry in Japan 11
1.3 TEPCO and Fukushima Daiichi Nuclear Power Plant 14
1.4 Systemic Complexity 15
1.5 STAMP—Accident Model Based on Systems Theory 16
1.5.1 CAST 17
1.5.2 STPA 18
1.6 Purpose of the Analysis 20
1.7 References 21

Chapter 2. Accident Analysis Using the CAST Process 23

2.1 Stakeholders and Safety Constraints 23
2.1.1 Tokyo Electric Power Company (TEPCO) 24
2.1.2 Nuclear and Industrial Safety Agency (NISA) 25
2.1.3 Off-site Center (Local NERHQ) 26
2.1.4 Nuclear Safety Commission (NSC) 26
2.1.5 Prime Minister's Office (NERHQ) 27
2.1.6 Ministry of Education, Culture, Sports, Science and Technology (MEXT) 27
2.1.7 Fukushima Prefectural Government and Municipal Governments 28
2.1.8 General Electric 29
2.1.9 Other stakeholders 29
2.2 Safety Control Structure 31
2.3 Unsafe Control Actions 33
2.3.1 Tokyo Electric Power Company (TEPCO) 33
2.3.2 Nuclear and Industrial Safety Agency (NISA) 39
2.3.3 Off-site Center (Local NERHQ) 44
2.3.4 Nuclear Safety Commission (NSC) 45
2.3.5 Prime Minister's Office (NERHQ) 47
2.3.6 Ministry of Education, Culture, Sports, Science and Technology (MEXT) 49
2.3.7 Fukushima Prefectural Government and Municipal Governments 50
2.3.8 General Electric 51

2.3.9 Other stakeholders 52
2.4 Flawed Communication and Coordination 54
2.5 "Safety Myth" and its Consequences 55
2.5.1 "Safety Myth" 56
2.5.2 Overemphasis on design-basis accidents (deterministic approach) 57
2.5.3 Inefficacy of severe accident management (probabilistic approach) 59
2.5.4 Lack of preparedness against compound nuclear disasters 62
2.6 Administrative Issues 64
2.6.1 Lack of expertise and leadership of TEPCO top management on nuclear safety 64
2.6.2 TEPCO's safety culture 65
2.6.3 Complex administrative framework of promotion and regulation 67
2.6.4 Detrimental effects of bureaucracy 69
2.7 Summary and Findings 70
2.8 References 76

Chapter 3. Hazard Analysis using the STPA Process 79

3.1 Improvements by Stakeholders 79
3.1.1 "Nuclear Reform" by TEPCO 80
3.1.2 Actions by Other Nuclear Operators 82
3.1.3 Establishment of Nuclear Regulation Authority 84
3.1.4 Improvement of Safety Regulations 85
3.1.5 Improvement of Emergency Response 87
3.2 Safety Constraints and Control Structure 88
3.2.1 System Level Accidents, Hazards and Safety Constraints 88
3.2.2 Safety Control Structure 89
3.3 Step 1—Identifying Unsafe Control Actions 92
3.3.1 Unsafe Control Actions in Peacetime 92
3.3.2 Unsafe Control Actions in an Emergency 94
3.4 Step 2—Identifying the Causes of Unsafe Control Actions 96
3.4.1 Causal Factors of Unsafe Control Actions in Peacetime 96
3.4.2 Causal Factors of Unsafe Control Actions in an Emergency 105
3.5 Summary and Findings 114
3.6 References 116

Chapter 4. Conclusion 117

4.1 Overall Summary 117

4.2 Recommendations 118

4.2.1 Nuclear operators 118

4.2.2 Nuclear Regulation Authority 119

4.2.3 Cabinet Office 120

4.2.4 Scientists and IAEA 120

4.3 Future Works 121

Chapter 1. Introduction

The Fukushima Daiichi nuclear disaster triggered by the tsunami of the Great East Japan Earthquake on March 11, 2011, was the largest nuclear disaster since the Chernobyl disaster in 1986. In spite of the limited information we have so far owing to the ongoing aftermath of the accident, many have attempted to identify why this accident happened. However, it is not easy to decide the "root causes" of the accident, given that various aspects of this complex sociotechnical system, which intricately intertwines with each other, have contributed to the accident. Nor is it easy to identify what could trigger a hazard leading to another accident in the future. For this reason, it is useful to analyze the system safety using a new type of accident model based on systems theory.

1.1 The Nuclear Disaster

On March 11, 2011, a magnitude-9 earthquake, which would be named the Great East Japan Earthquake, shook northeastern Japan, unleashing a savage tsunami. It triggered an extremely severe nuclear accident at the Fukushima Daiichi Nuclear Power Plant, owned and operated by Tokyo Electric Power Company (TEPCO). This devastating accident was ultimately declared a Level 7 ("Severe Accident") by the International Nuclear Event Scale (INES).

Kurokawa *et al.* (2012, pp. 12-14) summarize the severe accident, which ultimately emitted an enormous amount of radioactive material into the environment, as follows. [1]

> When the earthquake occurred, Unit 1 of the Fukushima Daiichi plant was in normal operation at the rated electricity output according to its specifications; Units 2 and 3 were in operation within the rated heat parameters of their specifications; and Units 4 to 6 were undergoing periodical inspections. The emergency shut-down feature, or SCRAM, went into operation at Units 1, 2 and 3 immediately

after the commencement of the seismic activity.

The seismic tremors damaged electricity transmission facilities between the TEPCO Shinfukushima Transformer Substations and the Fukushima Daiichi Nuclear Power Plant, resulting in a total loss of off-site electricity. 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.

The tsunami caused by the earthquake flooded and totally destroyed the emergency diesel generators, the seawater cooling pumps, the electric wiring system and the DC power supply for Units 1, 2 and 4, resulting in loss of all power—except for an external supply to Unit 6 from an air-cooled emergency diesel generator. In short, Units 1, 2 and 4 lost all power; Unit 3 lost all AC power, and later lost DC before dawn of March 13, 2012[1]. Unit 5 lost all AC power.

The tsunami did not damage only the power supply. The tsunami also destroyed or washed away vehicles, heavy machinery, oil tanks, and gravel. It destroyed buildings, equipment installations and other machinery. Seawater from the tsunami inundated the entire building area and even reached the extremely high pressure operating sections of Units 3 and 4, and a supplemental operation common facility (Common Pool Building). After the water retreated, debris from the flooding was scattered all over the plant site, hindering movement. Manhole and ditch covers had disappeared, leaving gaping holes in the ground. In addition, the earthquake lifted, sank, and collapsed building interiors and pathways, and access to and within the plant site became extremely difficult. Recovery tasks were further interrupted as workers reacted to the intermittent and significant aftershocks and tsunami.

The loss of electricity resulted in the sudden loss of monitoring equipment such as scales, meters and the control functions in the central control room. Lighting and communications were also affected.

[1] "March 13, 2012" should be read "March 13, 2011."

The decisions and responses to the accident had to be made on the spot by operational staff at the site, absent valid tools and manuals. The loss of electricity made it very difficult to effectively cool down the reactors in a timely manner. Cooling the reactors and observing the results were heavily dependent on electricity for high-pressure water injection, depressurizing the reactor, low pressure water injection, the cooling and depressurizing of the reactor containers and removal of decay heat at the final heat-sink. The lack of access, as previously mentioned, obstructed the delivery of necessities such as alternative water injection using fire trucks, the recovery of electricity supply, the line configuration of the vent and its intermittent operation.

As a result, this severe accident ultimately emitted an enormous amount of radioactive substances into the environment, and forced approximately 150,000 residents to evacuate. [1]

1.2 History of Nuclear Industry in Japan

The development of nuclear power in Japan was forcibly started due to political agendas. In 1953, future Prime Minister Yasuhiro Nakasone, who was a supporter of nuclear power and then a young politician studying at Harvard University, learned from politically connected professors that the United States was about to allow the knowledge and technology that built atomic bombs to be exported for the peaceful use of nuclear power. As soon as President Dwight D. Eisenhower of the United States announced his “Atoms for Peace” initiative, Nakasone led efforts in the Diet in late 1953 and early 1954 to draw up Japan’s first-ever budget for nuclear power research. [2][3]

Without significant fossil fuel reserves of its own, it made sense that Japan chose to increase its energy independence. The Atomic Energy Basic Act was enacted in 1955 to “secure energy resources in the future, achieve scientific and technological progress, and promote industry by encouraging the research,

development and utilization of nuclear energy, thereby contributing to the improvement of the welfare of human society and of the national living standard (Article 1).” [4]

Nakasone also assembled a group of like-minded allies in and out of government to help convince the public of the necessity to invest in this new technology. One of the most influential was Matsutaro Shoriki, head of the Yomiuri Shimbun, a major newspaper company in Japan, and head of the newly created Nippon TV. Under his guidance, the Yomiuri led the way in selling nuclear power to the public as a safe, reliable and peaceful energy source. He was elected to the Diet in 1955, and became the first head of Atomic Energy Commission and the Director General of Science and Technology Agency in 1956. [3]

In this political context, the research on nuclear energy for practical use was rapidly conducted. Japan Atomic Energy Research Institute (JAERI) was established in the same year, and its first research reactor JRR-1 reached first criticality in 1957. Electricity was generated for the first time by its Power Demonstration Reactor (JPDR) in 1963.

The first commercial reactor was developed at Tokai Power Station by the Japan Atomic Power Company, which had been established in 1957 at the initiative of the government. It first reached criticality in 1965 and started operation in the following year. Although this first one was a graphite-moderated, carbon dioxide gas-cooled reactor (GCR) introduced from the United Kingdom, the private power companies were planning to build light-water reactors developed in the United States, either boiling water reactors (BWRs) or pressurized water reactors (PWRs), since they were considered to be more compact, constructed with fewer costs and more evolvable than GCRs. Kansai Electric Power Company started the commercial operation at the Mihama Nuclear Power Plant (Unit 1 – PWR) in 1970, and TEPCO at the Fukushima Daiichi Nuclear Power Plant (Unit 1 – BWR) in the following year. [5]

The national government remained firmly committed to a large scale nuclear power program despite sustained resistance from local communities, to reduce the oil dependence after the 1973 oil crisis. As the

approval of the prefectural governor (e.g. Governor of Fukushima Prefecture in case of the Fukushima Daiichi Nuclear Power Plant) is a de facto prerequisite to build nuclear power plants, the government instituted tactics to smooth the path for its nation-wide energy agenda undertaken in cooperation with private utilities. Its largest tools were the so-called "*Dengen Sanpo* (Three Power Source Development Laws)" established in 1974, when Nakasone was head of the Ministry of International Trade and Industry, the ministry promoting nuclear energy for commercial use, and they have collectively provided enormous subsidies for communities hosting nuclear power plants. [6]

As a result, capacity of nuclear power plants grew rapidly to nearly 50GW in total, as shown in Figure 1-1. Early in 2011, nuclear energy accounted for almost 30% of the country's total electricity production (29% in 2009). [7][8]

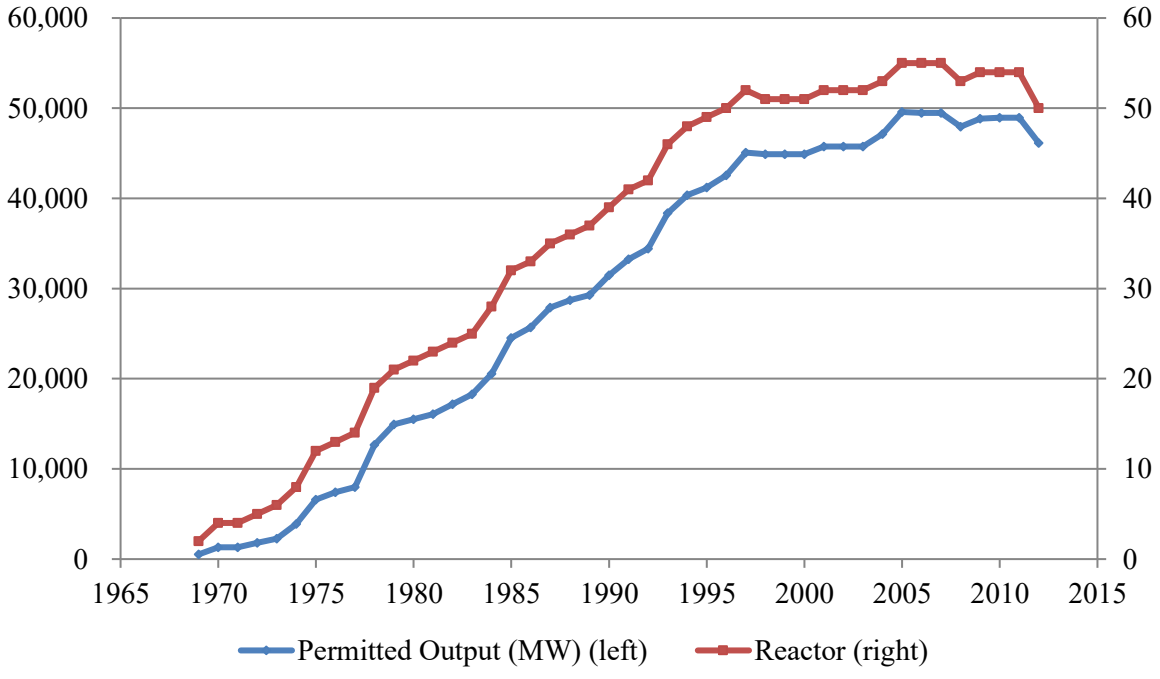


Figure 1-1: Capacity of Nuclear Power Plants in Japan [7]

1.3 TEPCO and Fukushima Daiichi Nuclear Power Plant

Tokyo Electric Power Company (TEPCO), an electric utility established in 1951, has been effectively allowed by Electricity Business Act (Act No. 170 of 1964) franchise monopoly within the Greater Tokyo Area (Tokyo, Kanagawa, Saitama, Chiba, Tochigi, Gunma, Ibaraki, Yamanashi and east Shizuoka). It is one of the world's largest electric utility companies, serving nearly 30 million customers with 190 power plants that primarily utilize thermal, nuclear and hydroelectric power sources. [9][10]

As of March 2010, TEPCO owned 17 nuclear reactors, 6 in Fukushima Daiichi, 4 in Fukushima Daini, and 7 in Niigata Kashiwazaki-Kariwa (note: all of them were located outside TEPCO’s service area) and the total capacity was 17,308 MW. Nuclear power accounted for approximately 40% of TEPCO's total electricity output. [11]

The Fukushima Daiichi Nuclear Power Plant is located in the towns of Futaba and Ohkuma, 250 km north of Tokyo. It was the first nuclear plant to be constructed and operated entirely by TEPCO, with the first unit of the nuclear station commissioned in 1971.

As shown in Table 1-1, the total installed capacity of the six boiling water reactor units is 4,696 MW. Unit 1 has an installed capacity of 460 MW, Units 2, 3, 4 and 5 each have 784 MW capacity and Unit 6 is rated at 1,100 MW. Units 1 to 5 are Mark I type while Unit 6 is a Mark II built with containment structures.

Table 1-1: Reactors in the Fukushima Daiichi Nuclear Power Plant [1]

		Unit No. 1	Unit No. 2	Unit No. 3	Unit No. 4	Unit No. 5	Unit No. 6
Reactor type		BWR3	BWR4	BWR4	BWR4	BWR4	BWR5
Containment type		MARK 1	MARK 1	MARK 1	MARK 1	MARK 1	MARK II
Electrical output (10,000 KW)		46.0	78.4	78.4	78.4	78.4	110.0
Thermal output (10,000 KW)		138.0	238.1	238.1	238.1	238.1	329.3
Application for reactor installment license		July 1, 1966	September 18, 1967	July 1, 1969	August 5, 1971	February 22, 1971	December 21, 1971
Reactor installment license granted		December 1, 1966	March 29, 1968	January 23, 1970	January 13, 1972	September 23, 1971	December 12, 1972
Start of construction		September 29, 1967	May 27,1969	October 17, 1970	May 8, 1972	December 22, 1971	March 16, 1973
Criticality		October 10, 1970	May 10, 1973	September 6, 1974	January 28, 1978	August 26, 1977	March 9, 1979
Start of operations		March 26, 1971	July 18, 1974	March 27, 1976	October 12, 1978	April 18, 1978	October 24, 1979
Main contractor		GE	GE/Toshiba	Toshiba	Hitachi	Toshiba	GE/Toshiba
Architect, engineer		EBASCO	EBASCO	Toshiba	Hitachi	Toshiba	EBASCO
Suppliers	Reactor system	GE/GETSCO	GE/Toshiba	Toshiba	Hitachi	Toshiba	GE/Toshiba
	Pressure vessel system	GE/GETSCO/ Toshiba/IHI	GE/GETSCO/ Toshiba/IHI	Toshiba/IHI	Hitachi/Bab-cock-Hitachi	Toshiba/IHI	GE/GETSCO/ Toshiba/IHI
	Reactor core	GE/GETSCO	GE	Toshiba	Hitachi	Toshiba	GE
	Fuel	GNF-J/NFI	GNF-J/NFI	GNF-J	NFI	NFI/AREVA NP	NFI
	Steam system	GE/GETSCO	GE/Toshiba/ GETSCO	Toshiba	Hitachi	Toshiba	GE/Toshiba/ GETSCO
	Turbine	GE/GETSCO	GE/Toshiba/ GETSCO	Toshiba	Hitachi	Toshiba	GE/GETSCO
	Construction work	Tobishima/ PENTA-OCEAN/ Hazama/Maeda/ Kumagai/GE	Kajima/ Kumagai	Kumagai/ Kajima	Kajima/PENTA-OCEAN /Haza-ma/Maeda/ Kumagai	Kajima/Kum-agai/PENTA-OCEAN	Kajima/Kumagai/ Hazama/Maeda/ PENTA-OCEAN

The six reactors were designed by General Electric, which also supplied Units 1, 2 and 6. Units 3 and 5 were supplied by Toshiba and Unit 4 by Hitachi. The nuclear complex was constructed by Kajima, a Japanese construction company.

The emergency core cooling system of each reactor was designed to run on electricity, which could be supplied from the nation's power grid or from on-site diesel generators.

1.4 Systemic Complexity

Since the Fukushima Daiichi nuclear disaster, several accident investigation reports, as well as a large

number of articles, have been published in an effort to identify the causes, not only from technical but also managerial points of view. In the official report published by the National Diet, Kurokawa *et al.* (2012, p.16) conclude that the accident was the result of collusion between the government, the regulators and TEPCO, and the lack of governance by said parties. [1]

While this official report provides good insights into the core contributors to the accident, it focuses on blaming TEPCO and the regulator, with relatively few descriptions of other factors. In fact, it is safe to say that the whole picture surrounding the accident is much more complex when we consider the variety of stakeholders involved in nuclear safety and the contexts that affected the decision making of each party, because of the sociotechnical complexity that a nuclear power plant has.

Guntzburger *et al.* (2014) highlight that a complex network of legal, cultural and technological paradigms, as well as the defense mechanisms of personal and organizational moral disengagement, have structured the context of this crisis, allowing for an event to turn into this disaster. They then argue that a reform of traditional risk and crisis management is needed, embracing a more complex and systemic approach, integrating the historical, socio-cultural and ethical dimensions. [12]

1.5 STAMP—Accident Model Based on Systems Theory

To address the aforementioned challenges, it is beneficial to use a new type of accident model based on systems theory, which can be extended to these social factors. System-Theoretic Accident Model and Processes (STAMP) captures more types of accident causal factors including social and organizational structures, new kinds of human error, design and requirements flaws, and dysfunctional interactions among non-failed components. Specifically, STAMP focuses particular attention on the role of constraints in safety management, and accidents are seen as resulting from inadequate control or enforcement of

constraints on safety-related behavior at each level of the system development and system operations control structures, an example of which is shown in Figure 1-2. [13][14]

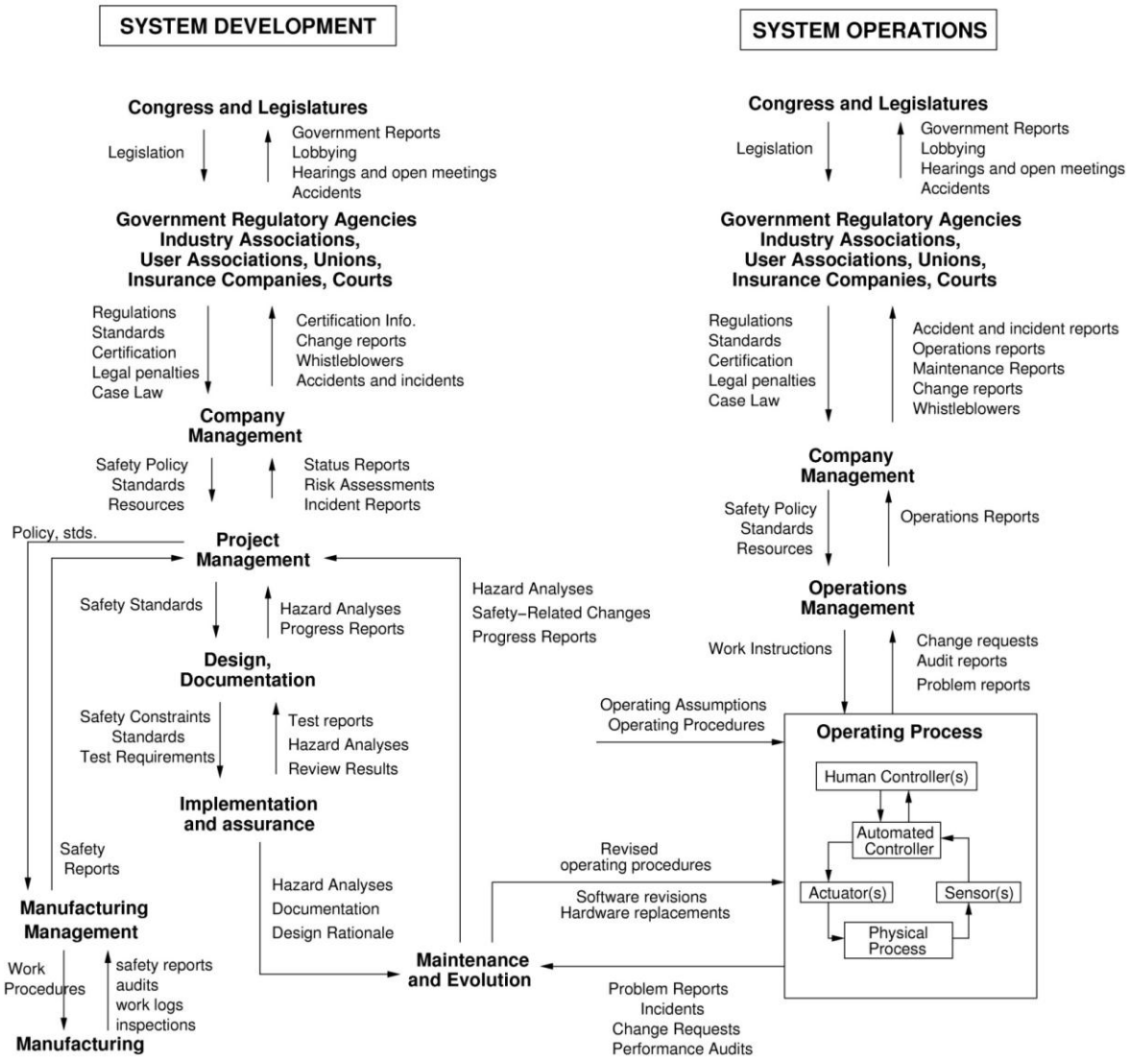


Figure 1-2: General Form of a Model of Sociotechnical Control [13]

1.5.1 CAST

CAST (Causal Analysis based on STAMP) is an accident analysis technique based on STAMP, providing a framework to assist in understanding the entire accident process and identifying the most important

systemic causal factors involved, to see why the accident occurred and how to prevent similar losses in the future.

Specifically, the use of CAST, by identifying the unsafe control actions by each component of the system (or stakeholders) as well as reasons for these actions, provides the ability to examine the entire sociotechnical system design to identify the weaknesses in the existing safety control structure and to identify changes that will not simply eliminate symptoms but potentially all the causal factors, including the systemic ones. [13]

1.5.2 STPA

STPA (System-Theoretic Process Analysis) is an approach to hazard analysis based on the STAMP causality model, using a functional control diagram and the requirements, system hazards, and safety constraints or requirements for the components of the system. It is used to identify accident scenarios that encompass the entire accident process, some of which cannot be identified with conventional hazard analysis techniques such as Fault Tree Analysis and Failure Modes and Effects Analysis (FMEA). [13]

STPA has two main steps: [13]

1. Identify the potential for inadequate control of the system that could lead to a hazardous state.
   Hazardous states result from inadequate control or enforcement of the safety constraints, which can occur because:

   (a) A control action required for safety is not provided or not followed;

   (b) An unsafe control action is provided;

   (c) A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequences;

(d) A control action required for safety is stopped too soon or applied too long.

2. Determine how each potentially hazardous control action identified in Step 1 could occur.

(a) For each unsafe control action, examine the parts of the control loop to see if they could cause it. For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems (Figure 1-3).

(b) Consider how the designed controls could degrade over time and build in protection.

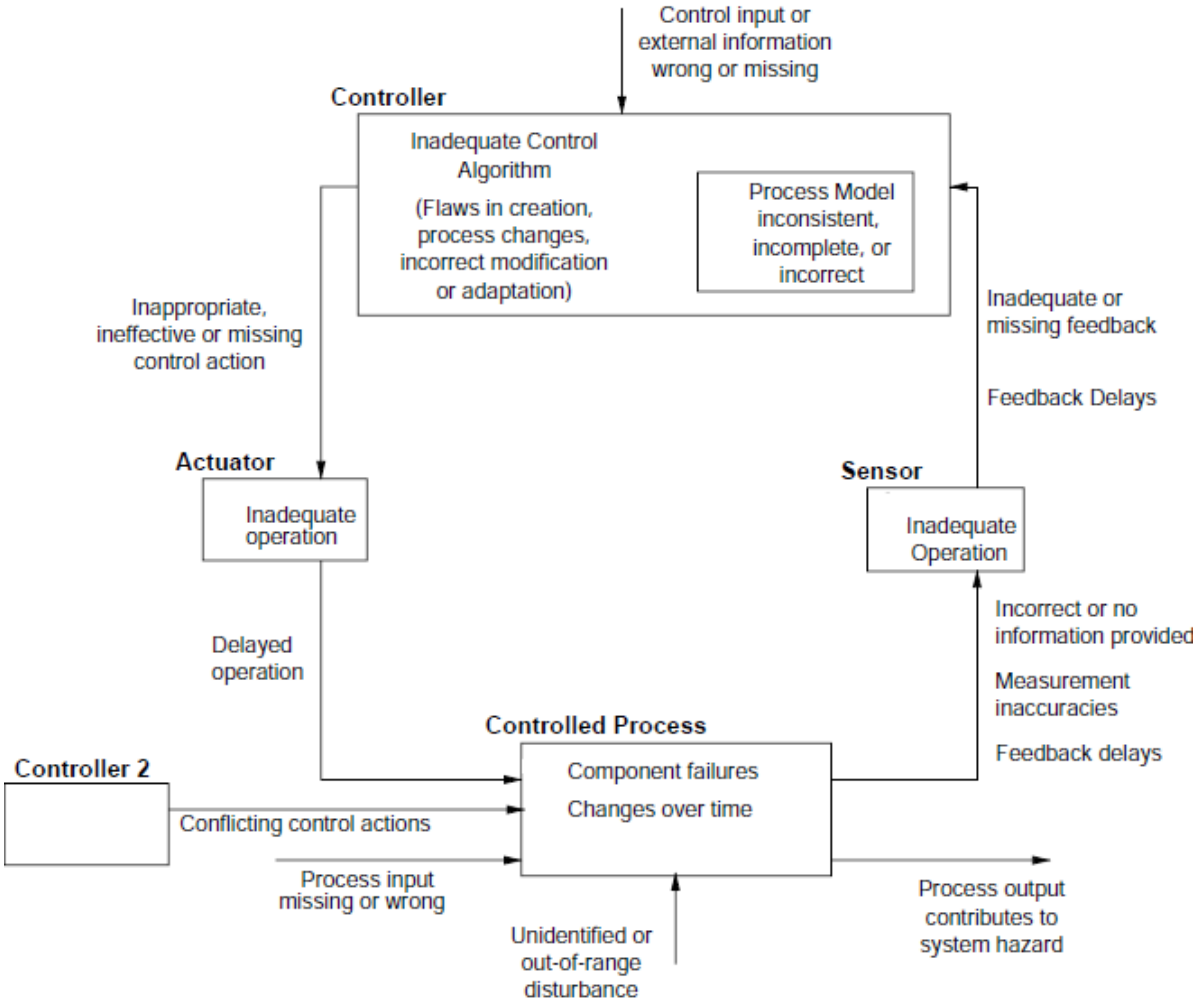


Figure 1-3: Causal Factors to Be Considered in a Control Loop [13]

1.6 Purpose of the Analysis

This thesis takes a systemic approach—STAMP methodology—to identify why the Fukushima Daiichi nuclear disaster occurred and what should be done to establish nuclear safety in Japan, by analyzing the responsibility of each stakeholder, the overall control structure, unsafe control actions and contributing factors, as well as coordination and communication issues. It also identifies what managerial aspects should be changed and maintained to eliminate, reduce or at least mitigate such kinds of severe nuclear disasters in the future. The rest of the thesis is organized as follows.

In Chapter 2, the Fukushima Daiichi nuclear disaster is analyzed using the CAST process, in order to understand why the safety control structure as a whole was inadequate both in preventing the disaster and in managing the crisis. This accident analysis, focusing on social and *inter*-organizational structures rather than technical or *intra*-organizational aspects, is based mainly on accident investigation reports, as well as media items both in Japan and in other countries, and personal comments of those close to the nuclear industry.

In Chapter 3, the potential risks with regard to the safety control of nuclear energy in Japan are identified performing an STPA, taking into account the analysis in Chapter 2 and the recent changes made after the Fukushima Daiichi nuclear disaster. This analysis also depicts possible migrations towards a state of increasing risk over time, as well as the methods to control them.

Finally, conclusions and recommendations are made and future works are proposed in Chapter 4 for ensuring the safety of nuclear power plants in Japan.

1.7 References

[1] Kurokawa, K., Ishibashi, K., Oshima, K., Sakiyama, H., Sakurai, M., Tanaka, K. and Yokoyama, Y. (2012), "The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission (Executive Summary)", The National Diet of Japan, Tokyo, available at: http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/en/report/

[2] 延近充研究会 (2012). 「原子力発電について ― 内在する本質的問題と日本における利用の展望と課題 ―」(Japanese). Retrieved September 27, 2015, from http://keizemi-keio.com/wordpress/wp-content/uploads/%E5%BB%B6%E8%BF%91%E7%A0%94%E7%A9%B6%E4%BC%9A.pdf

[3] The Japan Times (2011). "Key players got nuclear ball rolling". Retrieved September 27, 2015, from http://www.japantimes.co.jp/news/2011/07/16/national/key-players-got-nuclear-ball-rolling/

[4] The Independent Investigation on the Fukushima Nuclear Accident (2014), "The Fukushima Daiichi Nuclear Power Station Disaster: Investigating the Myth and Reality", Routledge.

[5] 日本の原子力発電開発の歴史 (16-03-04-01) - ATOMICA - (n.d.) (Japanese). Retrieved September 27, 2015, from http://www.rist.or.jp/atomica/data/dat_detail.php?Title_No=16-03-04-01

[6] Aldrich, D. P. (2005). Japan's Nuclear Power Plant Siting: Quelling Resistance. Retrieved from http://japanfocus.org/-Daniel_P_-Aldrich/2047/article.html

[7] Japan Nuclear Energy Safety Organization (2013). 原子力施設運転管理年報 平成 25 年版 (Japanese). Retrieved September 28, 2015, from http://www.inaco.co.jp/isaac/shiryo/pdf/genpatu/jnes_25.pdf

[8] Nuclear Power in Japan | Japanese Nuclear Energy (n.d.). Retrieved October 11, 2015, from http://www.world-nuclear.org/info/Country-Profiles/Countries-G-N/Japan/

[9] Get to Know Tepco: Japan's Biggest Power Company (n.d.). Retrieved October 10, 2015, from http://www.pbs.org/newshour/rundown/get-to-know-tepco-japans-biggest-power-company/

[10] TEPCO: Corporate Information (n.d.). Retrieved October 10, 2015, from http://www.tepco.co.jp/en/corpinfo/overview/p-glance-e.html

[11] TEPCO : Challenges of TEPCO | Nuclear / TEPCO-Power Plants (n.d.). Retrieved October 11, 2015, from http://www.tepco.co.jp/en/challenge/energy/nuclear/plants-e.html

[12] Guntzburger, Y. and Pauchant, T. C. (2014),"Complexity and ethical crisis management", Journal of Organizational Effectiveness: People and Performance, Vol. 1 Iss 4 pp. 378-401

[13] Leveson, N. (2012). “Engineering a safer world: systems thinking applied to safety”. Engineering systems. Cambridge, Massachusetts: MIT Press.

[14] Thomas, J. (2013). “Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis” (Doctoral dissertation, Massachusetts Institute of Technology).

Chapter 2. Accident Analysis Using the CAST Process

The previous chapter showed how the tsunami triggered by the Great East Japan Earthquake on March 11, 2011, caused the catastrophe at the Fukushima Daiichi Nuclear Power Plant. However, the disaster might have been prevented if the power plant had been properly prepared against such severe accidents. In fact, the Onagawa Nuclear Power Plant owned and operated by Tohoku Electric Power Company, which was closer to the epicenter and experienced higher tsunami, was able to shut down safely, and the Fukushima Daini Nuclear Power Plant of TEPCO, approximately 12 km to the south of the Fukushima Daiichi, managed to escape the fate as its sister plant.

In this chapter, the CAST process reveals why the overall safety control structure for the Fukushima Daiichi Nuclear Power Plant went wrong, by identifying the multiple stakeholders of this accident, their safety constraints and unsafe control actions on one another, as well as communication and coordination issues. In addition, some important beliefs and contexts that were underlying these problems are analyzed. Note that the focus of this analysis is not technical details of the power plant but a high-level and organizational set of constraints and actions.

2.1 Stakeholders and Safety Constraints

In this section, the roles of stakeholders involved in the safety of the Fukushima Daiichi Nuclear Power Plant, that is, safety design, safety management and emergency response, are analyzed. Note that the names of organizations and their safety constraints are based on what they were at the time of the accident.

2.1.1 Tokyo Electric Power Company (TEPCO)

As discussed in Chapter 1, Tokyo Electric Power Company (TEPCO) was a power company that provided electricity in the Greater Tokyo Area. TEPCO owned and operated six reactors at the Fukushima Daiichi Nuclear Power Plant.

The Fundamental Safety Principles of IAEA Safety Standards (IAEA, 2006) states that "the prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risks." Specifically, TEPCO was responsible for: [1]

- Establishing and maintaining the necessary competences;
- Providing adequate training and information;
- Establishing procedures and arrangements to maintain safety under all conditions;
- Verifying appropriate design and the adequate quality of facilities and activities and of their associated equipment;
- Ensuring the safe control of all radioactive material that is used, produced, stored or transported.

In case of an emergency, it was required for TEPCO to report it immediately to the national and local governments, and to ensure that the nuclear reactors—the controlled processes—retained the following three capabilities at all costs: the ability to control the nuclear reactions occurring inside the reactor (to *stop* the reaction); the ability to remove heat from inside the reactor (to *cool* the reactor); and the ability to prevent the spread of radioactive substances outside the reactor (to *contain* the radioactive substances). It was also necessary for TEPCO to provide adequate information for neighborhood residents who might be affected. [2]

2.1.2 Nuclear and Industrial Safety Agency (NISA)

As a result of the reorganization of the central government in January 2001, the Ministry of Economy, Trade and Industry (METI) —the former Ministry of International Trade and Industry (MITI) —took charge of all safety regulations on nuclear power as an energy source. In this process, the Nuclear and Industrial Safety Agency (NISA) was established as a "special agency" inside the Agency for Natural Resources and Energy (ANRE), an extra-ministerial bureau, to take charge of ensuring energy safety and industrial safety. [3]

NISA, as a regulatory body, had a responsibility in establishing standards and the regulatory framework for protecting people and the environment against radiation risks. (Note: as discussed in 2.1.6, nuclear safeguards and radiation protection was the responsibility of the Ministry of Education, Culture, Sports, Science and Technology.) To this end, according to the Fundamental Safety Principles of IAEA Safety Standards (IAEA, 2006), NISA ought to have: [1]

- Had adequate legal authority, technical and managerial competence, and human and financial resources to fulfill its responsibilities;
- Been effectively independent of the licensee and of any other body, so that it was free from any undue pressure from interested parties;
- Set up appropriate means of informing parties in the vicinity, the public and other interested parties, and the information media about the safety aspects (including health and environmental aspects) of facilities and activities and about regulatory processes;
- Consulted parties in the vicinity, the public and other interested parties, as appropriate, in an open and inclusive process.

NISA was also responsible for nuclear emergency response. It was charged with disaster prevention and damage mitigation in the event of an accident as the secretariat of the Nuclear Emergency Response

Headquarters (NERHQ), and was expected to perform the functions of planning and coordinating responses to the accident being undertaken by the NERHQ, the Local NERHQ, and other relevant organizations. More specifically, the secretariat was responsible for the collection of information on nuclear plants, the forecasts, monitoring results and other information of the dispersion of radioactive substances, and for the planning of protective measures for residents (including evacuation orders) and the coordination, etc. of emergency transportation of supplies, on the basis of such information. [4]

2.1.3 Off-site Center (Local NERHQ)

An Off-site Center was designated for each nuclear facility as a base for responding to a nuclear disaster, and was positioned to act as the base of the national nuclear emergency preparedness system. In the event of the issuance of the Nuclear Emergency Declaration, the Local NERHQ was established at the Off-site Center and organized the Joint Council for Nuclear Emergency Response (Joint Council) with the prefectural/municipal headquarters for disaster control of the nuclear facility location, for purposes of information exchange and mutual cooperation. [4]

2.1.4 Nuclear Safety Commission (NSC)

In response to the rise of the antinuclear movement in the 1970s, the Nuclear Safety Commission (NSC) separated from the Atomic Energy Commission in 1978 with the objective of improving safety regulations. NSC, the commissioners of which were appointed by the Prime Minister on Diet approval, was granted the function to double check safety regulations and to deliberate and decide regulation policies. In addition, they had the right to issue recommendations through the Prime Minister to regulatory bodies. [4]

In the case of nuclear emergency, NSC was to provide technical advice based on requests made by the

Prime Minister, director-general of NERHQ. Specifically, NSC was to set up a headquarters organization called an Emergency Technical Advisory Body within its secretariat, and a local body of the Emergency Technical Advisory Body at the Off-site Center to which it would dispatch, among others, the NSC commissioners and the advisors for emergency responses. In turn, NSC was to collect information and perform investigations and analyses, as well as prepare technical advice. [4]

2.1.5 Prime Minister's Office (NERHQ)

In response to the notification made by a nuclear operator, the Prime Minister should issue a Nuclear Emergency Declaration, and should establish the Nuclear Emergency Response Headquarters (NERHQ), of which he would serve as the director-general, for the promotion of emergency response measures and the comprehensive coordination among relevant organizations. [4]

Specifically, NERHQ, with the support of NISA serving as its secretariat, was to play a pivotal role in the government's emergency response measures such as taking protective action on behalf of the residents, including their evacuation. To this end, it was also expected, in terms of public relations in an emergency, to provide relevant information to the public via local governments, promptly, accurately, and in an easily understandable, clear-cut manner. [3][4]

2.1.6 Ministry of Education, Culture, Sports, Science and Technology (MEXT)

The Ministry of Education, Culture, Sports, Science and Technology (MEXT) was formed in 2001, with the former Ministry of Education merged with the former Science and Technology Agency (STA), which was established in 1956 originally to take on a central role in Japan's administration of nuclear energy. [2]

MEXT served as the authority for radiation protection, including monitoring and radiation survey. The Nuclear Emergency Response Support Headquarters was established within the ministry in the case of a nuclear emergency, which existed mainly to provide advice for monitoring conducted by the radiation squad at the Off-site Center, to analyze monitoring data, and to dispatch disaster medical assistance teams to the site. [2][4]

2.1.7 Fukushima Prefectural Government and Municipal Governments

Local governments, although they were responsible for the protection of their residents, did not have authority to give an order to nuclear operators, since the national government was considered to comprehensively supervise their activities such as designing, building, operating and maintaining the nuclear facilities. Instead, it became customary for utilities to gain the consent of the local governments (prefectural and municipal governments) in the 1970s by concluding non-binding "safety agreements" with them. These safety agreements, including one about the Fukushima Daiichi Nuclear Power Plant, effectively allowed the local governments to play their role to protect its residents, including: [5][6][7]

- Measurement and evaluation of radioactivity in the environment;
- Judgement on the installation and extension of facilities;
- Safety confirmation of facilities;
- Planning for nuclear emergency response.

The Regional Disaster Prevention Plan stipulated that Fukushima prefectural government, when they received a report on abnormality, should establish a Prefectural Headquarters for Disaster Control, send their officials to the Off-site Center for coordination of disaster control measures with the national government, and provide assistance for municipal governments for resident evacuation. They also made

provisions to take swift countermeasures to implement emergency monitoring, which included the need to work out a radiation monitoring strategy, prepare and maintain radiation monitoring facilities and equipment, secure all required radiation monitoring personnel, and ensure cooperation among relevant organizations. [4][8]

2.1.8 General Electric

As Japan was not capable of designing its own nuclear power plants in the 1960s, TEPCO imported nuclear technology wholesale from General Electric. As mentioned in Chapter 1, all the reactors of Fukushima Daiichi Nuclear Power Plant were based on the designs by General Electric, and Units 1 to 5 were Mark I type containment structure. [9]

Generally speaking, while the operator had overall responsibility for safety, the design organization of a nuclear power plant was expected to play an essential role in establishing the basis for nuclear safety, as the International Atomic Energy Agency (IAEA, 2000)[2] stated that "The design organization shall ensure that the installation is designed to meet the requirements of the operating organization, including any standardized utility requirements; that it takes account of the current state of the art for safety; that it is in accordance with the design specifications and safety analysis; that it satisfies national regulatory requirements; that it fulfils the requirements of an effective quality assurance programme; and that the safety of any design change is properly considered." [10]

2.1.9 Other stakeholders

In addition to the stakeholders discussed above, who were primarily responsible for safety design, safety

[2] This description is excerpted from the publication amended following the accident in the Fukushima Daiichi nuclear power plant and renumbered as IAEA Safety Standards Series No. SSR-2/1 (Rev. 1). However, IAEA states that "The review revealed no significant areas of weakness and resulted in just a small set of amendments to strengthen the requirements and facilitate their implementation."

management and emergency response, there were other stakeholders that indirectly contributed to the safety of Fukushima Daiichi Nuclear Power Plant, as follows:

(a) Scientists

One of the roles that scientists play in society, in general, is to provide scientific knowledge and advice to decision makers and, if necessary, to make policy recommendations based on their expertise.

Specifically, they were expected to offer their expertise in nuclear science and technology or in disaster prevention, to TEPCO and the governmental organizations. NSC, in particular, consisted of members from academia.

(b) Radiation Emergency Medicine Network

Radiation emergency medicine refers to medical treatment provided in the event of contamination and radiation exposure as a result of radiation accidents and nuclear disasters. The medical institutions that provide special treatment to patients suffering from radiation contamination or exposure are known as radiation emergency medical institutions.

Several of the medical institutions located in prefectures where nuclear power plants were situated, including Fukushima Prefecture, had been designated as radiation emergency medical institutions and, together with the National Institute of Radiological Sciences, made up the radiation emergency medicine network. [4]

The radiation emergency medicine network was built under the initiative of MEXT, the authority for radiation protection (See 2.1.6), in accordance with the basic principles underlying “The Shape of

Radiation Emergency Medicine" agreement drawn up by NSC. [4]

2.2 Safety Control Structure

Figure 2-1 shows the system control structure for the safety design and safety management of the Fukushima Daiichi Nuclear Power Plant and the emergency response in case of an accident, according to the safety constraints of stakeholders discussed in the previous section.

TEPCO was charged with the direct safety management of the nuclear power plant, which had been originally designed by General Electric. NISA provided supervision over the operator, and their safety regulations were checked by NSC. Scientists provided knowledge and expertise for stakeholders such as TEPCO, NISA and NSC.

In case of an emergency, operators were to control the nuclear power plant with the help of TEPCO head office. The Prime Minister's Office was to take the initiative in emergency response with the support of NISA as its secretariat, and the Off-site Center located near the nuclear power plant was to organize a joint council with the local governments. Residents would be given monitoring information and be instructed about evacuation by the national or the prefectural government, and radiation emergency hospitals would provide special treatment to patients suffering from radiation contamination or exposure.

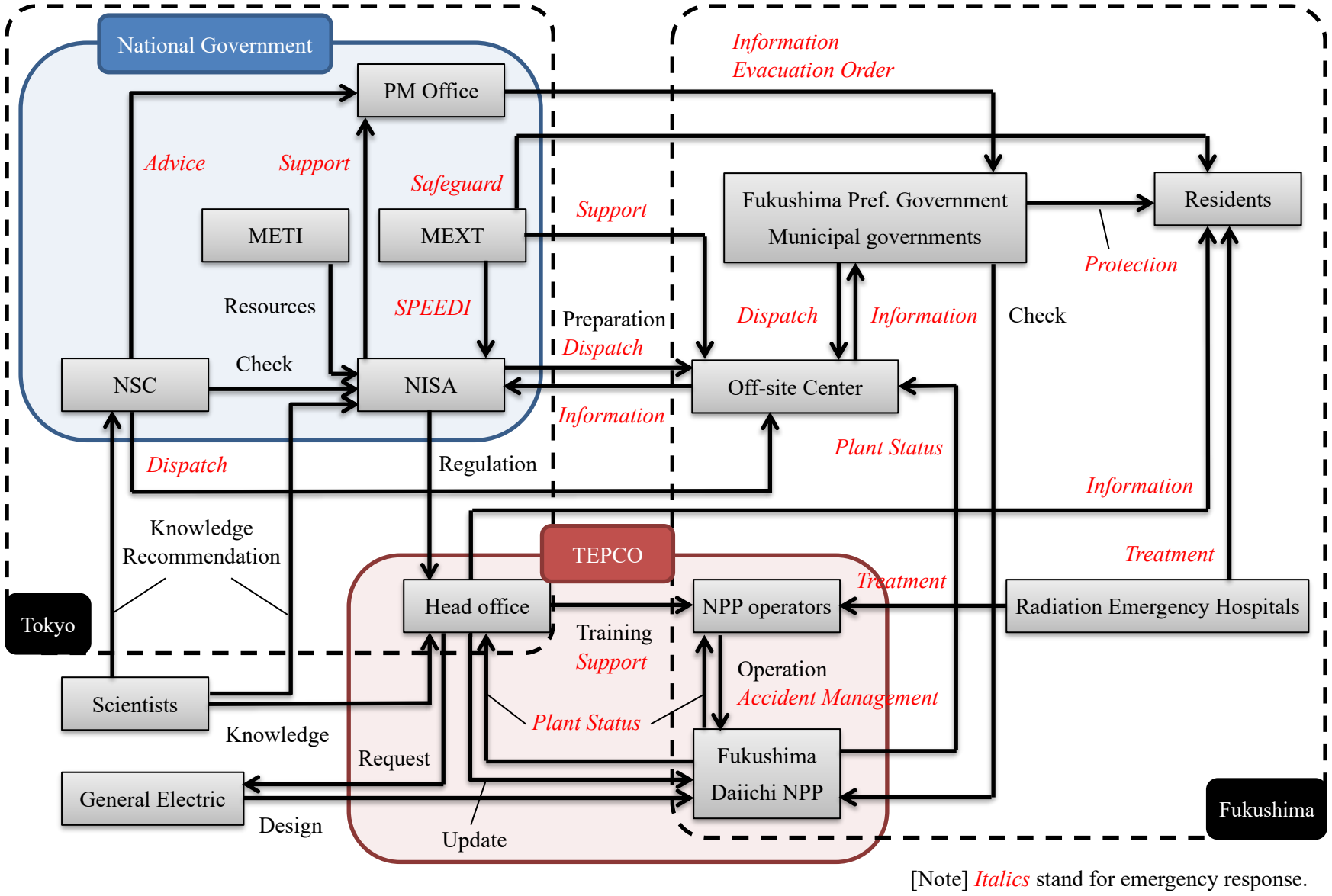


Figure 2-1: Planned System Control Structure for the Safety of the Fukushima Daiichi Nuclear Power Plant

2.3 Unsafe Control Actions

In this section, the unsafe control actions of each stakeholder are analyzed as well as their mental model flaws and the contexts behind these actions.

2.3.1 Tokyo Electric Power Company (TEPCO)

(a) Nuclear reactors at the Fukushima Daiichi Nuclear Power Plant (physical process)

Unsafe Control Action #1: Inability to "*stop, cool and contain*" in response to an external event

On March 11, 2011, the emergency shut-down feature, or SCRAM, went into operation at Units 1, 2 and 3 immediately after the commencement of the seismic activity. However, the tsunami inundated the plant and destroyed the electrical systems, and as a consequence, station blackout led to the inability to cool the reactors, which is believed to have caused core meltdown. The power plant also failed to contain the radioactive substances, releasing them into the environment at a large scale.

(Contexts)

As discussed in 2.3.8, the system design by General Electric was susceptible to an accident. TEPCO was advised at least 20 years before the accident to make design improvement such as the diversification of power and cooling systems and the reinforcement of reactor containers and reactor buildings, but the advice was not taken seriously. [11]

(b) Fukushima Daiichi NPP operators

Unsafe Control Action #1: Inadequate control of severe accidents

Fukushima Daiichi Nuclear Power Plant (NPP) operators were overwhelmed and “lost for words” at the ongoing unpredictable and devastated state that far exceeded any expected major accident, after they received information that the nuclear reactors were successively losing their power sources. [8]

Despite their great efforts, NPP operators failed to control the overheating reactors after many of the functions to effectively cool down the reactors had been lost. Their ability to think about and confront the situation for themselves proved to be limited, and there was a lack in flexible and proactive thinking, which is necessary in responding to a crisis. [3]

Miscommunication within the site also seems to have blocked the prompt emergency response. Information such as the operation status of emergency equipment was not accurately communicated from the shift team to the NPP Emergency Response Center, which was situated in the Emergency Response Office on the second floor of a seismic isolation building of the Fukushima Daiichi NPP, and there was a discrepancy in awareness between the two parties. [8]

(Mental Model Flaws)

The NPP Emergency Response Center did not accurately recognize the status of the plant. For example, they mistakenly believed for a while that the isolation condenser (IC) system of Unit 1 to transfer residual and decay heat was operating normally, leading to no further actions. [8]

(Contexts)

It is clear that the loss of the main control room function, lighting and communication systems inhibited or delayed on-site emergency response to a great extent. The operators had to work in the yard where there were rubble and debris, worrying about the aftershock or the recurrence of tsunami as well as the safety of their families. The working environment further deteriorated with time due to an increase in radiation level and hydrogen gas explosions in the reactor buildings. [4][8]

The Safety Parameter Display System, by which both the Fukushima Daiichi NPP operators and the head office would have been able to instantly grasp and monitor the operational status of all units, was not available because it had lost its power supply after the tsunami. In addition, most of the main control rooms, which would have been the only source of information on the plant status, became incapable of providing the plant parameters for the same reason. [8]

There were organizational issues as well including a lack of planning and implementation of adequate operator training in response to severe accidents, and the lack of staff experience in activating emergency equipment during the normal operation or periodical inspection. Basic procedures to take on the occasion of a serious accident were not adequately shared among the operators at the whole site, as opposed to those at the Fukushima Daini Nuclear Power Plant. [3][4]

Furthermore, the operational structure of the assignment of lead engineers for the nuclear reactors and the work schedule of plant operators was not sufficient to respond to multiple nuclear accidents occurring at the same time. The Nuclear Reactor Regulation Act (Act No. 166 of 1957) required operators to assign a lead engineer for each nuclear reactor to oversee the safe operations, but in reality one engineer was made responsible for several reactors; at the Fukushima Daiichi Nuclear Power Plant, only two engineers were in charge of six reactors. In addition, the lead engineers had not received special training or education to prepare them for disastrous accidents. [4]

(c) TEPCO head office

Unsafe Control Action #1: Lack of protection against huge tsunamis and mitigation of severe accidents

The elevation of the area where major buildings for Units 1 through 4 were located was 10 meters above sea level, while the inundation height of the tsunami reached a level between about 11.5 meters and 15.5

meters, and the emergency diesel generators were poorly protected. [8][9]

In addition, severe accident countermeasures that postulated external events such as earthquakes and tsunamis had not been considered in Japan until recently. At the beginning of 2009, in response to discussions on the move toward regulatory requirements for severe accident countermeasures, operators finally began to review schedules for the probabilistic safety analysis of external events. However, according to the roadmap created by the Federation of Electric Power Companies of Japan (FEPC), the evaluation of tsunamis would not be started until 2015. [4]

TEPCO did start to discuss, after launching a "Working Group on Tsunami in Fukushima" in August 2010, the contents of countermeasure constructions that might become necessary as tsunami countermeasures. However, it was regarded difficult to realize countermeasures such as watertight motors for seawater pumps and the installation of a building to contain pumps, both due to technical challenges.

As a result, no sufficient countermeasures against tsunamis had been taken before the accident. [8]

(Mental Model Flaws)

After the Niigata-ken Chuetsu-oki Earthquake occurred in July 2007, TEPCO was busy preparing for the restart of operation of their Kashiwazaki-Kariwa Nuclear Power Plant and they were highly conscious of the importance of countermeasures against seismic motions, but the awareness of their accompanying events such as tsunamis was low. [8]

Sakae Muto, Executive Vice President of TEPCO's Nuclear Power & Plant Siting Division, and others, believed that huge tsunamis would not occur in the near future. He explained, "It was judged that natural disaster countermeasures had no urgency because such disasters occur less than once every 100 years. The lifespan of the reactor is shorter." [4]

(Contexts)

In the late 1960s at the time of the application for an establishment license of these reactor units, simulation technologies to estimate tsunami heights were not generalized yet. The license was granted with the wave height for providing tsunami countermeasures as the highest tide level observed at a port near the site when the Chile Tsunami hit the port in 1960. In fact, it was not until 1970 that the Atomic Energy Commission—NSC did not exist at that time—introduced guidelines for regulatory safety reviews, bringing natural phenomena, including tsunamis, into the conversation; there had been no clear standards regarding tsunami risks prior to this. [2][8]

In 2006, however, when NISA and the Japan Nuclear Energy Safety Organization (JNES) set up the Study Group on Flooding, TEPCO became aware that no basis existed for assuming that the probability of a tsunami hitting the Fukushima Daiichi Nuclear Power Plant was extremely low, and that if such a tsunami hit the power plant, there was the possibility of a station blackout. [4]

Unsafe Control Action #2: Inadequate education, training and instruction to cope with severe accidents

Although TEPCO had been conducting legally required education and training for relevant personnel of nuclear power plants prior to the accident, and every operator in the nuclear sector showed abundant knowledge, their response to the accident was insufficient, and the functional teams established to manage the accident failed to coordinate with each other, as discussed in 2.3.1 (b). This can be considered to stem from a consequence of inadequate education and training that would give a view to an extreme situation such as the complete and simultaneous loss of AC power at multiple nuclear reactor units. [3]

Their manuals on emergency operating procedures proved to be unusable. They assumed an ability to monitor the nuclear reactors, and were not designed to cope with the loss of all electric power for a long period of time, which is what actually happened. [4]

(Mental Model Flaws)

As discussed in Section 2.5, the “Safety Myth”—the notion that serious severe accidents could never occur in nuclear power plants in Japan—existed among the stakeholders, which resulted in the inability to capture such crises as a reality. [3]

Unsafe Control Action #3: Ineffective emergency response and information disclosure

The TEPCO head office lacked the awareness and organization to support the operators at the front line of the accident site, and failed to provide technical assistance for them. For example, Masao Yoshida, Site Superintendent of the Fukushima Daiichi Nuclear Power Plant, asked TEPCO Representative Director and Executive Vice President Sakae Muto for technical advice when the situation at Unit 2 became serious, but Muto was unable to respond, as he was on the way from the Off-site Center. [4]

Furthermore, neither the chairman nor the president of TEPCO was at the head office at the time of the accident. The absence of the two top executives resulted in an extra burden on the communication and consultation flow at a time when serious decisions were urgently required. It is possible that the absence of the executives hampered the promptness of the initial response to the accident. [4]

TEPCO also failed to disclose facts about the accident’s progression to local residents, Japanese citizens, and stakeholders across the world in a timely and appropriate manner, and the information disclosed was not always sufficient. If TEPCO had proactively published an alert with regard to the anomalies of reactors, for example, they could have reduced the impact of radioactive substances on local citizens. [4]

(Contexts)

As discussed in 2.3.1 (b), the head office was not able to instantly grasp and monitor the operational status

of the reactors since the Safety Parameter Display System was not available. The head office also had to respond simultaneously to the crisis at the Fukushima Daini Nuclear Power Plant, the reactors of which were also in danger of meltdown by the aftermath of the tsunami.

TEPCO's information disclosure policy included the following characteristics: While it discloses what is required by laws or what has been confirmed, it does not disclose information other than those above, especially detrimental information. [4]

2.3.2 Nuclear and Industrial Safety Agency (NISA)

(a) Nuclear and Industrial Safety Agency

Unsafe Control Action #1: Inability to give the industry appropriate supervision

NISA, as a part of METI, had to play a role in protecting the framework for promoting nuclear power for the sake of its parent organization, compromising its position as the guardian of nuclear safety. For example, from the early stages of the development and revision of regulations, NISA and NSC effectively invited the operators to participate in the process, and established plausible standards that could be achieved without decommissioning any existing reactors, which allowed the postponement of countermeasures against tsunamis and station blackout. [4]

They also failed to take appropriate actions to improve their organization and the regulatory framework. In 2007, Japan received an Integrated Regulatory Review Service (IRRS) of IAEA, a peer review that evaluated legal systems and regulatory organizations, and NISA, in particular, received several recommendations and suggestions, such as "NISA should continue to develop its efforts to address the impacts of human and organizational factors on safety in operation," and "NISA should develop a strategic human resources management plan to face future challenges." Nevertheless, NISA did not take any

concrete measures in response. [4][12]

(Mental Model Flaws)

NISA believed that the probability of severe accidents was so small that, from an engineering perspective, severe accidents could be said never to happen in reality since the safety of Japan's reactor facilities was sufficiently ensured. [2]

Furthermore, officials at NISA were substantially dependent on precedent in making decisions; as discussed in 2.6.4, they believed that decisions made in the past should be appropriate. This belief, in turn, gave them little motivation to review and update the regulation.

(Contexts)

TEPCO, which was supposed to be subject to nuclear safety regulatory supervision, strongly pressured regulatory authorities for postponement of regulations and softening of regulatory criteria, taking advantage of its information superiority and its close relationship with NISA's parent organization METI, which was the supervising authority for the electric power business and was promoting nuclear power policies. [4]

There were some organizational issues with NISA. First, NISA was not an agency dedicated to nuclear regulations; it was also in charge of industrial safety. Therefore, if accidents occurred such as petrochemical complex accident or gas water heater accident in the field of industrial safety, NISA executive officials such as the Director-General and the Deputy Director-General were forced to handle these accidents, instead of focusing on nuclear safety regulations. [3]

Second, NISA was not independent in terms of personnel management. Administrative and engineering officials of NISA were employed as those for the entire Ministry of Economy, Trade and Industry. As discussed in 2.3.2 (b), periodic personnel transfers for these staff members made it difficult to develop

specialized technical ability and therefore to commit themselves to their duties that required sufficient expertise and experience with nuclear regulations. [3]

Third, NISA did not have an organizational and personnel arrangement capable of addressing mid- to long-term challenges. NISA had been occupied with the handling of various incidents since its establishment in January 2001, and therefore NISA had no choice but to prioritize the handling of such short-term administrative issues. Although NISA recognized the necessity of reviewing mid- and long-term issues, it was not feasible to maintain a sufficient amount of human resources for these issues. [3]

Unsafe Control Action #2: Ineffective preparation for the occurrence of serious accidents

NISA could not develop effective hardware or software to cope with serious accidents.

For instance, NISA developed and maintained Off-site Centers as a base for responding to a nuclear disaster, as discussed in 2.1.3, but they were found not to function as intended in case of serious accidents in which radioactive substances were released into the environment at a large scale.

Specifically, the Off-site Center for both the Fukushima Daiichi NPP and the Fukushima Daini NPP was located only about 5 km from the Fukushima Daiichi NPP, and was not equipped with air cleaning filters to insulate it from radioactive substances. Those factors ultimately forced the Off-site Center to relocate its functions, as discussed in 2.3.3. [8]

Furthermore, NISA was taking initiative of the comprehensive nuclear emergency preparedness drills conducted annually by the national government, but the drills did not anticipate severe accidents or complex disasters at all. It was virtually useless as a measure to increase preparedness for nuclear accidents. [4]

(Mental Model Flaws)

As with TEPCO, NISA believed that serious accidents could never occur in nuclear power plants in Japan —the "Safety Myth," as discussed in Section 2.5. [3]

(Contexts)

Off-site Centers were required by law to be established within 20 km from nuclear power plants.

Participants in the comprehensive nuclear emergency preparedness drills changed every year due to frequent personnel transfers and changes of administration in the government. The various organizations in charge of the drills were required to brief participants from scratch every time the drill was conducted. The time available to brief participants from the government, including politicians (Cabinet members etc.) as well as bureaucrats, was very limited. With the huge amount of time required for preparation, in practice the drills were only conducted in line with a predetermined scenario. [4]

Unsafe Control Action #3: Ineffective emergency response in the face of a compound nuclear disaster

NISA, the secretariat of NERHQ, failed in the function of collecting and sharing information concerning the progression of the accident and the progress of the response, and could not provide NERHQ with appropriate and organized advice as experts. [4]

NISA also expended an inordinate amount of time on reviewing the scope of evacuation, and was unable to draft a proposal for the specific designation of evacuation areas in a prompt manner. Moreover, NISA, as well as other institutions, fell into a so-called "elite panic," in which they refused to pass on critical pieces of information, in the fear of inciting panic among the general public; for instance, NISA failed to publish immediately most of the results of the monitoring conducted during the period from March 11 to

15 and sent from the Off-site Center. [2][4][8]

(Mental Model Flaws)

They were not well prepared since they believed that, as rigorous nuclear safety regulations were in place in Japan, it was not necessary to anticipate an accident that would release enough radioactive material to actually require protective actions. [4]

One of the reasons why it took a long time to review the evacuation areas was that they did not use the qualitative, likely atmospheric dispersion of radioactive materials calculated by SPEEDI (discussed in 2.3.6) developed to predict the dispersion of radioactive materials in case of a nuclear emergency. NISA thought that, with no information within the reactor available for SPEEDI owing to the malfunction of data transmission, the qualitative calculations based on an assumed unit release rate were useless, although they were still useful in making judgment on which direction people should be evacuated. [3]

(Contexts)

While the Off-site Center was expected to collect information locally and report it to NISA, it could not function properly due to reasons such as the defunct communication means. [8]

(b) Ministry of Economy, Trade and Industry (METI)

Unsafe Control Action #1: Not offering NISA institutional independence or sufficient expertise

As discussed in 2.1.2, NISA, when it was established in 2001, was put under the jurisdiction of METI, which was in charge of promoting nuclear power; hence, METI controlled NISA's budgetary and personnel management. Career bureaucrats, who took charge of NISA's administrative positions, had not necessarily been educated or trained as nuclear technology experts, and were compelled to shuttle back

and forth between the agency and METI every two or three years under the personnel rotation system. [2][4]

By relying on its traditional personnel management system based on rotation, METI failed to offer NISA institutional independence and sufficient expertise, which were necessary for it to work as a regulatory body.

(Mental Model Flaws)

The government contended that the necessary level of independence with regard to NISA was safeguarded, because the level of independence became higher than before the establishment of NISA, and because NISA came under the supervision of NSC. [4]

(Contexts)

As a national policy, periodic personnel transfers are recommended for purposes such as “development of administrative processing system which is able to respond appropriately to various administrative issues and changing work load.” (Basic Policy of Employment and Promotion) [3]

2.3.3 Off-site Center (Local NERHQ)

Unsafe Control Action #1: Inability to take the initiative in the on-site response

The establishment of the Local NERHQ, which needed to be set up at the Off-site Center for this accident, required a lot of time due to the delays and cancellations of the arrivals of necessary personnel as well as the loss of power supply. Even after the establishment of the Local NERHQ, ground communication lines remained disconnected, causing serious problems with the sharing of information, liaison and coordination with relevant organizations, as discussed in Section 2.4. [4]

Furthermore, as the accident became more serious, radiation doses within the building increased in tandem with the rises in radiation doses in surrounding areas, raising concerns about the impact on the health of personnel there. Under these circumstances, the Local NERHQ decided to relocate the functions of the Off-site Center to the Fukushima prefectural government building. [4]

(Contexts)

The government's preparedness system in the event of a nuclear disaster had been built on the assumption that the infrastructure, including communication and transportation networks, would function and operate as in ordinary times; the loss of the functions of this infrastructure was not amply anticipated and countermeasures for such a situation had not been adequately taken in advance. [4]

The Off-Site Center, in particular, did not have sufficient logistical and personnel support in place, and was not equipped with air filters to block the penetration of radioactive materials. [4]

2.3.4 Nuclear Safety Commission (NSC)

Unsafe Control Action #1: Inability to check safety regulations and to decide effective regulation policies

NSC also lacked independence from administrative institutions promoting nuclear power and did not play its expected role of checking regulations administered by NISA. On the contrary, in some cases they received instructions from NISA, an organization that they were supposed to supervise, illustrating the fact that NSC was seriously ignored as far as actual operations were concerned. [4]

NSC almost never exercised its authority to issue recommendations through the Prime Minister to regulatory bodies in spite of a number of nuclear accidents and incidents, and avoided any regulation that appeared to be an obstacle to the promotion and utilization of nuclear power. [4]

(Contexts)

The staff members of NSC's secretariat were dominated by people from organizations such as MEXT and METI. The decision making processes were also affected by the industry. [4]

Furthermore, NSC had no right to investigate the regulatory bodies and operators, nor was authorized to punish these entities. As they did not personally confront nuclear operators, detect problems in their operations, or set safety standards for necessary repairs, the commission tended to consider nuclear plant safety from a rational and theoretical basis, regardless of on-site circumstances. [2][4]

Finally, NSC, like NISA, had no organizational capacities to deal with mid- and long-term issues properly. While NISA was preoccupied with responses to various incidents at nuclear facilities, NSC was also forced to check NISA's short-term regulatory activities. It was not until in December 2010 that NSC identified their mid- and long-term tasks, such as the documentation of the fundamental principles for nuclear safety and improvement of severe accident measures. [3]

Unsafe Control Action #2: Inability to provide appropriate advice at the time of disaster

NSC used a group e-mail system for mobile phones to summon the advisors for emergency responses, and attempted to establish an Emergency Technical Advisory Body. However, the group e-mail was not delivered to some advisors for emergency responses, and disruptions in public transportation and telecommunications meant that nearly all of the advisors for emergency responses that were summoned failed to convene on March 11. [4]

While NSC Chairman Madarame individually joined the discussion at the Prime Minister's Office, NSC was not able to organizationally provide technical support for him. Nor did NSC take a proactive stance from the perspective of protecting the public, such as providing advice of their own accord. [4]

2.3.5 Prime Minister's Office (NERHQ)

Unsafe Control Action #1: Causing confusion by decision making processes different from that in drills

The core group for the emergency response was not NERHQ, but the Prime Minister and a limited number of other concerned parties who assembled in the rooms on the fifth floor at the Prime Minister's Office. As the situation of the events evolved so fast, there was no time for discussion at these meetings of NERHQ, and thus "the fifth floor" directly collected opinions and views from TEPCO, NISA, the members of NSC and other parties concerned, and made decisions based on them. [4]

However, at a time when the government should have been using all its resources in an integrated fashion to respond to the situation, the content and context of deliberations on the fifth floor were not completely understood by the representatives from relevant ministries and agencies assembled in the Crisis Management Center located belowground in the Prime Minister's Office. As a result, NERHQ failed to serve its function as a whole. [8]

Furthermore, the direct intervention by the Prime Minister's Office to TEPCO, including the site visit to the Fukushima Daiichi Nuclear Power Plant by the Prime Minister himself, led to disruption in the chain of command, formulating a route for transmitting information that was at odds with the planned route, and gave rise to confusion at the scene of the accident. [4]

(Contexts)

From the very beginning of this accident, the crisis, which was going on simultaneously at multiple reactors, unfolded with unexpected speed. The scale, complexity, and speed of the progress of the accident had never been assumed in past nuclear emergency preparedness drills. Moreover, the government was also facing the huge task of responding to the tremendous damage that had been wrought by the

earthquake and tsunami on an extremely large scale, and ended up having to carry out difficult responses on two fronts. [4]

Owing to information security concerns, mobile phones could not ordinarily be used in the Prime Minister's Office's basement, where the relevant government officials assembled. With other communication means not adequately available, it was difficult for these officials to gather information on the accident rapidly. To Prime Minister Kan, it seemed that officials of relevant ministries and agencies did not provide information in a timely manner or make a convincing explanation regarding the response to the nuclear accident. [3][8]

Unsafe Control Action #2: Not providing the residents with accurate information on evacuation

Many residents did not receive accurate information along with the evacuation orders issued by NERHQ, including news about the seriousness of the accident or the expected term of their evacuation.

Unaware of the severity of the accident, they thought that they would be away from their homes for only a few days. They headed to the evacuation shelters literally with "just the clothes on their backs." Ultimately, however, they have been subjected to a long-term evacuation. In addition, the residents were forced to relocate to other evacuation shelters whenever the evacuation zone changed, increasing their stress. Some evacuees unknowingly evacuated to areas that were later found to have high doses of radiation. [4]

(Contexts)

Although it was essential for the government to ensure that information was disclosed promptly and appropriately in times of emergency, there was no such policy to determine what information should be released and how it should be released. [4]

2.3.6 Ministry of Education, Culture, Sports, Science and Technology (MEXT)

Unsafe Control Action #1: Failure to safeguard the residents against radioactivity

It was impossible to obtain almost any emergency monitoring results during the initial response stage of this accident because the monitoring posts, which were overly concentrated along the Fukushima Prefectural coastline, became unusable in the wake of the earthquake and tsunami. MEXT also dispatched monitoring cars, but it was not until March 13 that their professional support members arrived at the Off-site Center. Furthermore, initial monitoring activities did not work out as intended due to a host of reasons including hazardous road conditions from earthquake damage and fuel shortages. [4][8]

MEXT developed and deployed a system that predicts and computes the situation of the dispersion of radioactive materials into the atmosphere, called SPEEDI (System for Prediction of Environmental Emergency Dose Information), in order to support the consideration of protective action for residents when a nuclear emergency occurs. However, the calculation results from SPEEDI were not helpful for those making decisions on evacuation orders in the earliest stages because the progression of events during this accident was so swift and the information on sources of release (*i.e.* the nuclide types of radioactive material and the hourly amount of release) was not available. [4]

(Contexts)

There were some people involved in nuclear emergency preparedness who recognized, before the accident, the limitations of the prediction systems. However, a review of the existing framework in which evacuation orders would rely on the calculation results of the prediction systems was not held. Moreover, no systematic study was performed of measures that could compensate for the limitations of SPEEDI or of ways to utilize the calculations' predictions. [4]

2.3.7 Fukushima Prefectural Government and Municipal Governments

Unsafe Control Action #1: Insufficient emergency preparedness to protect the residents

Fukushima Prefectural Government and municipal governments that hosted the nuclear facility could not sufficiently involve the residents in evacuation drills. A survey of local residents showed that the ratio of local residents who had actually participated in evacuation drills was only around 10 to 15 percent, and virtually no one claimed that past emergency preparedness drills helped them weather this accident. [4]

(Contexts)

The comprehensive nuclear emergency preparedness drill conducted by the national government in cooperation with local governments, was superficial in nature as it was aimed primarily at not worrying or confusing local residents, and therefore lacked effectiveness in response to actual accidents. [4]

Unsafe Control Action #2: Inability to establish an initial response structure

The number of personnel available to respond to the nuclear disaster was significantly limited, making it impossible to implement the structure as planned. Most of the towns that hosted the nuclear facility could not dispatch personnel to the Off-site Center, and those who were hastily assigned to the nuclear disaster response were forced to respond single-handedly without any clearly defined scope of operations. [4]

Fukushima Prefecture was also unable to implement prompt emergency monitoring because it lacked the necessary equipment. For instance, since most of their monitoring posts were either washed away in the tsunami or with communication lines broken by the earthquake, only one of the 24 monitoring posts was functioning properly following the disaster. [4]

(Mental Model Flaws)

The nuclear emergency preparedness system of Fukushima Prefecture was not based on the assumption that a nuclear disaster, an earthquake and a tsunami could occur simultaneously. Their Regional Disaster Prevention Plan noted that an earthquake was not assumed to cause a nuclear emergency since the national government had confirmed the seismic safety of the nuclear power plants. [4]

In addition, Fukushima Prefecture officials were under the impression that the response to the nuclear disaster was mainly to be carried out at the Off-site Center, and the ineffectiveness of the Off-site Center thus pushed the prefecture's response to the disaster into a state of confusion. [4]

(Contexts)

When the nuclear accident happened, a large number of personnel both in the Fukushima Prefecture and in the municipalities were tied up with their response to the earthquake and tsunami disasters. [4]

2.3.8 General Electric

Unsafe Control Action #1: Providing system design susceptible to an accident

The emergency diesel generators for Units 1 through 5 were located in the basement in the poorly protected turbine buildings, as opposed to the Unit 6 whose diesel generators and cooling systems were protected by the fortified reactor building. As a result, the diesel generators for these reactors were submerged under seawater by the tsunami, and the plant eventually lost its emergency power supply for cooling the reactors. [2][9]

The cooling systems were designed to be heavily dependent on electricity for high-pressure water injection, depressurizing the reactor, low pressure water injection, the cooling and depressurizing of the

reactor containers and removal of decay heat at the final heat-sink. [4]

Furthermore, it had occasionally been pointed out that the Mark I containment system used in Units 1 through 5 was vulnerable to the dynamic loads that could be experienced with a loss of coolant. [13]

(Contexts)

The Fukushima Nuclear Power Plant was built based on turnkey agreements, by which the overseas manufacturer undertook all operations from plant design to materials procurement, construction, and trial operation, delivering to the customer a plant in a fully operational state. Unit 1 was originally designed to withstand a tornado, which is why the diesel generators were located in the basement. The reactor buildings were designed to be small to keep the reactor compact and economical. Nevertheless, the Japanese user was excluded from the reactor-design process, which implies there was little or no input from the operator. [2][9]

Furthermore, the Act on Compensation for Nuclear Damage (Act No. 147 of 1961) stipulated that the manufacturers, including General Electric, were exempted from product liability (*i.e.* the nuclear operators were solely liable for nuclear damage) according to the demand from the United States in return for technology licensing on nuclear power. [14]

2.3.9 Other stakeholders

(a) Scientists

Unsafe Control Action #1: Delay in research on nuclear safety

Safety research entered a period of decline in the second half of the 1990s, and its scope gradually diminished. Particularly tsunami research, until recently, consisted largely of efforts by a small number of

general researchers operating with limited resources, and could barely deliver clear answers to the sort of questions required to assess the safety of nuclear power plants—questions such as “How tall will the one-in-every-10,000-years tsunami be?” [2]

(Mental Model Flaws)

According to a survey conducted by the Atomic Energy Society of Japan to its members, the trend among the nuclear scientists was that the light water reactor was such a proven technology that it was no longer the target of research. [15]

(Contexts)

Power companies did not welcome research on nuclear safety for fear that the public might think there were some safety issues on nuclear reactors. [15]

Unsafe Control Action #2: Lack of communication within scientists and with different stakeholders

The fields of research were compartmentalized, but they lacked the communication between these fields to integrate the knowledge and expertise on the safety of the whole system. The failures of communication among nuclear safety experts and tsunami researchers, for instance, contributed to the inadequacy of preparedness against a huge tsunami. [2][15]

Nuclear researchers also failed to communicate with different stakeholders involved in nuclear safety, such as the operators and the regulatory bodies, and to offer effective policy recommendations to the government. [15]

(Mental Model Flaws)

Nuclear researchers believed that they were not influential enough to change the attitude of the operators

and the regulatory bodies, and that ensuring the safety of operational nuclear power plants was beyond their responsibility. [15]

(b) Radiation Emergency Medicine Network

Unsafe Control Action #1: Inability to cope with large-scale nuclear accidents

The emergency radiation medical system was unable to deal with accidents that involve the release of large amounts of radioactive substances over a wide area for the following reasons: inappropriate locations of primary radiation emergency hospitals as the hospitals themselves had to be evacuated; inability of these hospitals to treat any patients; lack of decontamination facilities; and finally, inadequate or almost non-existent radiation training of the hospital staff. [4]

Thus some of those who were injured at the Fukushima Daiichi Nuclear Power Plant did not have their injuries treated for three days. [3]

2.4 Flawed Communication and Coordination

As discussed in 2.6.3 in detail, the complex administrative framework of the national government had blurred the responsibilities of each stakeholder involved in safety regulations, such as NISA, NSC and MEXT, which generated coordination issues between them.

At the time of the emergency response, the fact that the earthquake severely damaged the communication measures, and the malfunction of the Off-site Center as discussed in 2.3.3, greatly hampered the smooth communication between the stakeholders, which they had not anticipated and prepared for. This caused not only the inadequate emergency response by each stakeholder, but also the lack of coordination

between them.

One of the consequences was the conflicting evacuation orders to the residents. The Fukushima Prefectural Government and the national government did not coordinate with each other's respective efforts. With a growing sense of crisis, Fukushima Prefecture made a decision to order residents within a 2 km radius of the Fukushima Daiichi Nuclear Power Plant to evacuate, but failed to communicate it to the national government. Just 30 minutes later, the national government, unaware of the instruction by Fukushima Prefecture, issued another evacuation order for residents within a 3 km radius of the nuclear power plant. The prefectural government tried to notify residents of the evacuation order, which proved to be tremendously difficult in the confusion after the earthquake and tsunami. [4]

2.5 "Safety Myth" and its Consequences

Not only the nuclear operators, but also many other players in the Japanese nuclear power industry including the regulators, the nuclear experts and even the local governments that obtained subsidies for hosting nuclear power plants, relied on the continued operation of the existing reactors, creating a situation where they were "all in same boat." The frequently used term "Nuclear Village" illustrated the fundamentally close, insular, conservative and interconnected nature of these players. [2][4]

It became the unspoken understanding in the "Nuclear Village" that the "risk of shutting down existing reactors in order to avoid any potential risk of accidents" outweighed the "risk of accidents occurring as the result of inaction," and accordingly, the stakeholders shared the "Safety Myth," an abstract notion that nothing could go wrong in Japan's nuclear sector. [4]

As discussed in 2.5.1 through 2.5.4 in detail, the "Safety Myth" emerged as an "explanation on safety" and was enhanced by strengthening the micromanagement of hardware by the regulatory bodies, but this in

turn restricted the efforts by the stakeholders to ensure the nuclear safety as a system. As a consequence, preparations for severe accidents and for compound nuclear disasters remained inadequate (Figure 2-2).

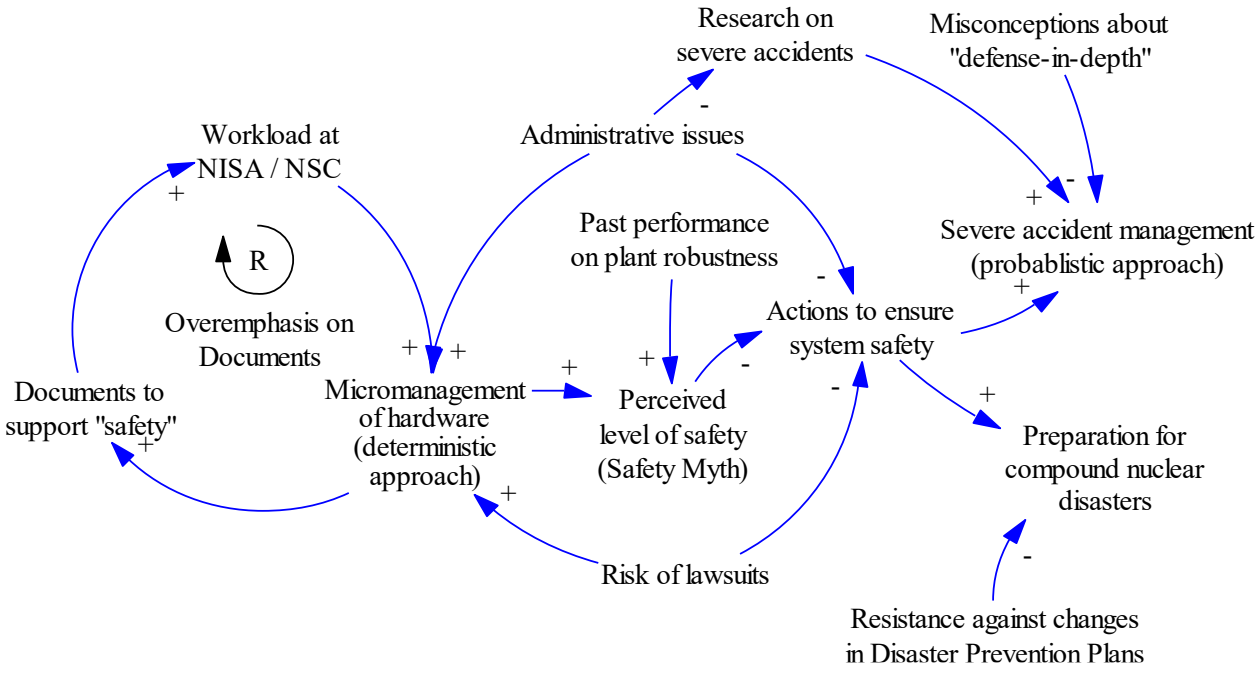


Figure 2-2: Causal Loop Diagram on “Safety Myth” and its Consequences

2.5.1 “Safety Myth”

The “Safety Myth” has played a significant role in affecting attitudes and societal acceptance of nuclear power technology, as well as in determining the administrative framework of safety regulations. [2]

There is a historical context: For a nation poor in energy resources, promotion of nuclear power came first in importance, but it was found that an “explanation on safety” to local governments, communities near the site, and the citizens, was needed. One reason behind this was Japan’s own experience as a target of nuclear bomb attacks over Hiroshima and Nagasaki during World War II and the entrenched antinuclear sentiment it engendered. [2][4]

As discussed in Chapter 1, the government took the initiative to introduce nuclear power since the 1950s, and some local governments manifested interest in hosting nuclear power plants in the hope of obtaining subsidies as well as a major source of employment. But as the local governments and the national governmental organs responsible for nuclear energy advancement scouted Japan's countryside to site future nuclear power plants, they found that people lived close to many of the sites. Assuming they could not convince residents to move, they inspired trust that the plants were indeed safe. [2]

In reality, however, there were not many discussions on safety at the national level until the 1970s, since they believed that nuclear energy safety could be assured by maintaining the safety standards established in other countries, from which the nuclear energy technology was being imported. It is reported that, between 1973 and 1974, Kinji Moriyama, then the Japan Atomic Energy Commission's chairman, said that it was only necessary for the commission to consider the construction of nuclear power plants, with no need for input on safety from academics—no need to question or doubt that nuclear reactors were completely safe. [2]

As the "Safety Myth" became prevalent, power companies and regulatory bodies were constrained by the "explanation on safety" they themselves had made in the past, and it became increasingly difficult for them to recognize and discuss the potential risks of accidents. One of the consequences was the obsession with a deterministic approach rather than a probabilistic approach, as discussed below.

2.5.2 Overemphasis on design-basis accidents (deterministic approach)

A design-basis accident is a postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to ensure public health and safety. By considering a wide variety of design-basis accidents and ensuring that existing safety

precautions are sufficiently conservative to all hypothetical events, governments and the nuclear industry can reasonably expect to ensure adequate capacity for handling most accident sequences that might occur in practice. [2][16]

When a lawsuit concerning the safety of the Ikata Nuclear Power Plant, operated by Shikoku Electric Power Company, brought to trial in 1978, the government produced various types of written documents to support its argument of the plant's safety. As the court considered these documents as well as mandatory inspections as concrete evidence of its safety, nuclear regulators eventually shifted to document-based inspections performed in a bureaucratic manner to show every aspect of hardware was designed and maintained to be safe. [2]

This explains why it was difficult for the government to take the probabilistic approach as regulatory requirements. During the lawsuit, the Government had explained the deterministic approach regarding design-basis accidents and the reasoning behind that approach, and had argued that existing regulations ensured satisfactory safety levels. This historic background created concern that, if regulatory oversight were to be required for severe accident preparedness, it would logically follow that the existing regulations had been inadequate and their application had been deficient. Moreover, the fact that the regulator substantially increased the number of items covered in inspections, lengthened the time needed to complete inspections, and increased the time and labor to produce and process the review documents, seems to have spurred their shortsighted approaches as they themselves became occupied with the handling of various accidents that had occurred at nuclear facilities. [2][8]

The nuclear operators were also bound in the same mindset. When asked in the fifth Tsunami Evaluation Subcommittee of the Japan Society of Civil Engineers (July 28, 2000), a member of the secretariat from the electric power industry answered that it was difficult for them to say "a tsunami larger than expected might possibly occur, and we therefore should also consider how to address it in case it occurs" because

nuclear power plants were laid with a hardware requirement never to release radioactivity to the outside. [8]

However, such deterministic approach is not sufficient from the perspective of defense-in-depth as discussed below. It should also be noted that, while the nuclear site licenses were issued on the basis of a facility's design, that would not ensure the facility's overall safety; the operational aspects including whether a nuclear emergency preparedness system is established, are also essential.

2.5.3 Inefficacy of severe accident management (probabilistic approach)

A severe accident, as opposed to a design-basis accident, is a type of accident that may challenge safety systems at a level much higher than expected. During these events, the response methods anticipated by design safety evaluations are unable to provide adequate reactor cooling capacity or to control the rate of reactions, resulting in severe damage to a reactor core, as shown in Figure 2-3. [2][16]

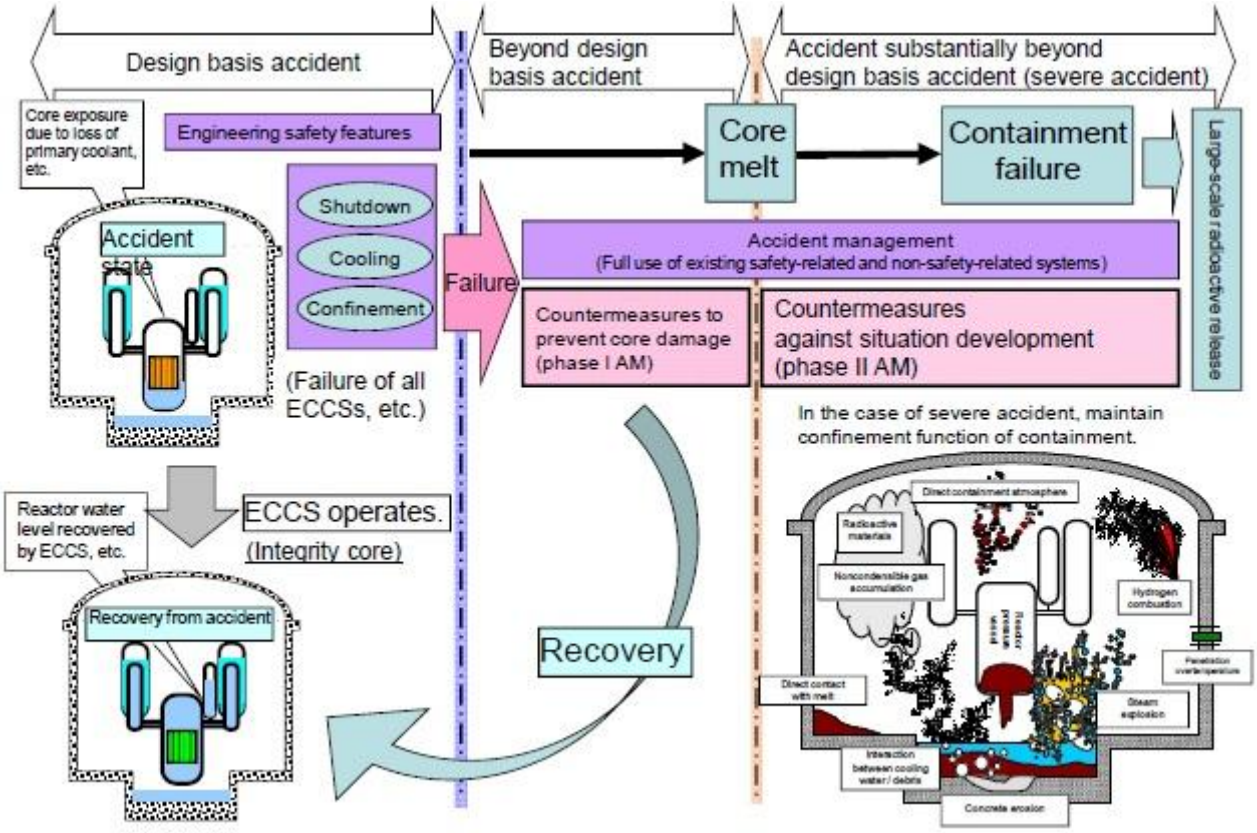


Figure 2-3: Severe Accident and its Management (Accident Management) [8]

After the Chernobyl disaster in 1986, the Nuclear Safety Commission established a group to study severe-accident measures. However, assuming that the safety of Japan's reactor facilities was sufficiently ensured by the philosophy of defense-in-depth—which was not true as described below—, the commission recommended in 1992 that nuclear operators "voluntarily" prepare effective severe accident management programs and ensure that they would be able to implement them properly in an emergency. [2]

(Misconceptions about defense-in-depth) Defense-in-depth is an approach to designing and operating nuclear facilities that prevents and mitigates

accidents that release radiation or hazardous materials, by creating multiple independent and redundant layers of defense, as follows, to compensate for potential human and mechanical failures. [16][17]

1) to prevent deviations from normal operation, and to prevent system failures

2) to detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions

3) to control their consequences and to achieve stable and acceptable plant states following such events by providing inherent safety features, fail-safe design, additional equipment and procedures (design basis)

4) to address severe accidents in which the design basis may be exceeded and to ensure that radioactive releases are kept as low as practicable

5) to mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions

Although the basic idea is that no single layer, no matter how robust, should be exclusively relied upon, the widespread misconception was that the emergency response set out in the fourth and fifth levels of defense-in-depth were not necessary when the safety provisions of the first three levels were adequate. [2]

In fact, Kobayashi (2012), who worked for Japan Airlines as an aeronautical engineer for a long time, observes that nuclear power plants, as opposed to aircraft, may be deficient in preparation for rare events in which they should fail since they are believed to have been designed with robustness. [18]

By the early 2000s, plant operators had assessed the efficacy of severe accident management of each plant, but the measures that they studied and implemented were limited to consideration of internally, not

externally, triggered events, although policy promises had been made that power companies and regulatory bodies would continue research with the eventual goal of expanding the scope of severe accident management to cover external events. [2]

One of the reasons why they failed to expand the scope was that, besides the excessive emphasis on the deterministic approach, research on severe accidents was conducted separately and uncoordinatedly by two organizations—the Nuclear Power Engineering Corporation (the predecessor of the Japan Nuclear Energy Safety Organization) affiliated with the Agency for Natural Resources and Energy, and the Japan Atomic Energy Research Institute affiliated to the Japan Science and Technology Agency. [2]

NISA was aware of the delays and passive attitude toward the regulation of severe-accident countermeasures. In February 2010, NISA published a document titled "Summary of Challenges in Nuclear Safety Regulation," which stated that it would be the right action for Japan to review the definition and treatment of severe accident management within its regulatory and legal frameworks. However, research on severe accident management for tsunami was still incomplete in March 2011; research conducted at JNES, for example, was still in the stage of test analysis. In addition, power companies and NISA felt that, in communicating with locals, it was extremely difficult to explain that there was a risk based on the results of probabilistic assessments. [3][8]

2.5.4 Lack of preparedness against compound nuclear disasters

It must be remembered that the Fukushima Daiichi nuclear disaster was a "compound nuclear disaster," a nuclear disaster triggered and accompanied by a natural disaster. When such a compound nuclear disaster occurs, a number of predicaments arise at the same time, creating a situation different from a single accident or a single disaster; to name a few, the national and local governments were faced with a situation

requiring simultaneous response to multiple disasters. Confusion reigned at many levels, response actions were delayed, and the earthquake and power outage paralyzed telecommunications infrastructure. In the midst of these difficulties the Off-site Center, the keystone in accident response, ceased to function. [8]

The insufficient preparedness on the part of both the national government and the local governments (Fukushima Prefectural Government and the municipal governments) in facing a compound nuclear disaster resulted in an unprecedented expansion in damage caused by this accident. [4]

The Niigata-ken Chuetsu-oki Earthquake, which occurred on July 16, 2007, triggered multiple troubles and failures, including a transformer fire and a leakage of water containing radioactive substances at the Kashiwazaki-Kariwa Nuclear Power Plant owned and operated by TEPCO. In response to these outcomes, many pundits requested nuclear power plants to put emergency preparedness measures in place to address compound nuclear disasters. NISA, although it assumed that compound nuclear disasters were not likely to occur, set out to establish the preparedness against them. [4]

Some national government agencies and local governments, however, harshly objected to NISA's proposal on compound nuclear disasters. This was partly because the assumption that there might be a situation in which a nuclear disaster and a natural disaster should occur simultaneously would drastically impact their Regional Disaster Prevention Plans, which defined how local governments should deal with nuclear disasters, and would thus incur large costs to fix these plans. NISA also felt that assuming that a large-scale natural disaster could trigger a nuclear disaster was not acceptable, since that assumption, they thought, would contradict their past explanation to local governments that nuclear power plants were designed with extremely stringent safety examinations in mind. [4]

As a result, there was no discussion, at the national level, of any measures for use in response to compound nuclear disasters, nor did the Fukushima Prefecture Disaster Prevention Plan specify measures against them. [4]

2.6 Administrative Issues

In the previous section, it was discussed how the “Safety Myth” emerged and was enhanced among the stakeholders in the “Nuclear Village” to promote the utilization of nuclear power, and how it affected their preparedness for severe accidents and for compound nuclear disasters.

Some of the administrative issues underlying this dynamic—especially those of TEPCO and the national government—deserve special attention.

2.6.1 Lack of expertise and leadership of TEPCO top management on nuclear safety

TEPCO, although it owned as many as 17 nuclear reactors, had never had a CEO whose expertise was rooted in nuclear technology or engineering, and only a limited number of executives could really appreciate the managerial matters of nuclear power business. Past CEOs rose up through administrative departments, which were more valued in TEPCO than technical organizations such as the Nuclear Power Division were. [2]

The top management could not establish effective leadership and management for nuclear safety, which IAEA Fundamental Safety Principles (IAEA, 2006) called for, since they did not understand the details of highly specialized operations of the Nuclear Power Division, and instead entrusted matters, such as safety provisions, to underlings familiar with nuclear power. That may also have caused inadequate sense of responsibility of top management as a nuclear operator, and their weak sense of crisis as described in 2.3.1. [1][2]

The administrative departments were allowed to give orders to each functional division while offering

little or no opportunity for feedback. Under constant pressure to maintain high uptime at nuclear plants, the Nuclear Power Division attempted to make all decisions and implement all necessary responses on its own. [2]

One of the consequences was the lack of company-level, cross-departmental approaches to nuclear safety. For example, TEPCO was aware of the seismic fragility of the Shin-Fukushima Transformer Station transmitting electricity to the Fukushima Daiichi Nuclear Power Plant due to issues related to ground features, but the Engineering Department responsible for strengthening that transformer station focused on the risk of suspended electricity transmission for the general consumers, instead of having rapid measures in place against power loss at the nuclear power plant. [4]

Another consequence of the lack of leadership was the deterioration in TEPCO's safety culture, as discussed in 2.6.2.

2.6.2 TEPCO's safety culture

Safety culture is a subset of organizational culture that reflects the general attitude and approaches to safety and risk management. That affects decision making by the controllers in the safety control structure and determines whether the control structure properly functions. [19]

Leveson (2012) describes two types of dysfunctional safety culture, both of which seem to apply to TEPCO. One is the "culture of denial," in which credible warnings such as whistleblowing are dismissed without appropriate action for improving safety. In 2000, Kei Sugaoka, a Japanese-American nuclear inspector who had done work for General Electric at the Fukushima Daiichi, told the nuclear regulator about a cracked steam dryer that he believed was being concealed, and yet NISA illegally divulged Sugaoka's identity to TEPCO, effectively expelling him from the industry. TEPCO was merely instructed

to inspect its reactors by itself, and was allowed to keep operating its reactors for the next two years even though, an investigation ultimately revealed, its executives had actually hidden other, far more serious problems, including cracks in the shrouds that cover reactor cores. [19][20]

The other type of flawed safety culture is the "paperwork culture," in which employees spend all their time proving the system is safe but little time actually doing the things necessary to make it so. As discussed in 2.5.2, nuclear regulators eventually shifted to document-based inspections to show every aspect of hardware was designed and maintained to be safe, which not only had the consequence of delaying initiatives to assess safety risks such as the possibility of severe accidents, but also tied the hands of workers at nuclear plant sites with a large amount of paperwork. [2][19]

Ryu *et al.* (2014) compare TEPCO's safety culture with that of Tohoku Electric Power Company, which owned and operated the Onagawa Nuclear Power Plant. Tohoku Electric Power Company, being well aware of the risks of tsunamis, had top management strongly advocating safety and had a culture to prioritize safety above all. That safety culture first appeared in their facility design different from that of the Fukushima Daiichi; for example, while historical data noted tsunamis in Tohoku Region to average three meters prior to construction, they themselves conducted surveys and research to determine potential tsunami height, and constructed their plant 14.7 meters above sea level, which was barely above the height of the actual tsunami that they experienced on March 11, 2011. Employees were also prepared for disasters through periodic training sessions against extreme situations, which allowed them to stay poised during the actual disaster and to avoid a catastrophe. [21]

Until the 1980s, however, TEPCO was also active and enthusiastic in its institution of safety provisions. The workers studied safety design philosophy for nuclear power plants and learned the lessons of past accidents, and were trained in an atmosphere of constant initiatives to improve and upgrade things. But as the core focus of work at nuclear power plants shifted to maintenance and operational issues, and as the

pressure to cut costs increased to cope with the partial liberalization of the electricity market, the practical aspects of safety design started to recede into the background, and repairs and inspections of plants were increasingly outsourced to restrain personnel costs, which lessened awareness of the on-site realities of nuclear power plants. [2]

After the accident, TEPCO reviewed their safety culture using the "Degree of Decline in Safety Culture," which appears in the INSAG 13 and 15 reports by the IAEA's International Nuclear Safety Advisory Group (INSAG). They found that, although scandals and other phenomena indicating the decline in their safety culture had surfaced previously, opportunities were missed to improve it with such comments as "There was no inclination[3] toward a decline in the safety culture." [22]

2.6.3 Complex administrative framework of promotion and regulation

Nuclear power generation in Japan has traditionally operated within a framework known as "privately administered government policy"—that is, the government established policy to promote the peaceful use of nuclear power, while the actual business of nuclear power generation was privately administered by power companies. However, this has created ambiguity of responsibility; although TEPCO has the prime responsibility for safety as a nuclear operator (See 2.1.1), they thought and insisted that safety measures such as severe accident management programs should be conducted in accordance with the national policy, instead of doing more than what was required by the government to ensure the safety. [2]

As shown in Figure 2-4, the structure of governmental organizations was also complex. METI (former MITI) was in charge of nuclear power for industrial purposes; ANRE promoted it with its association to the power industry, while NISA regulated it. MEXT (former STA) was in charge of technological

[3] The translated word "inclination" should be read as "tendency."

development and the promotion of nuclear technology, as well as nuclear safeguards and radiation protection. [2]

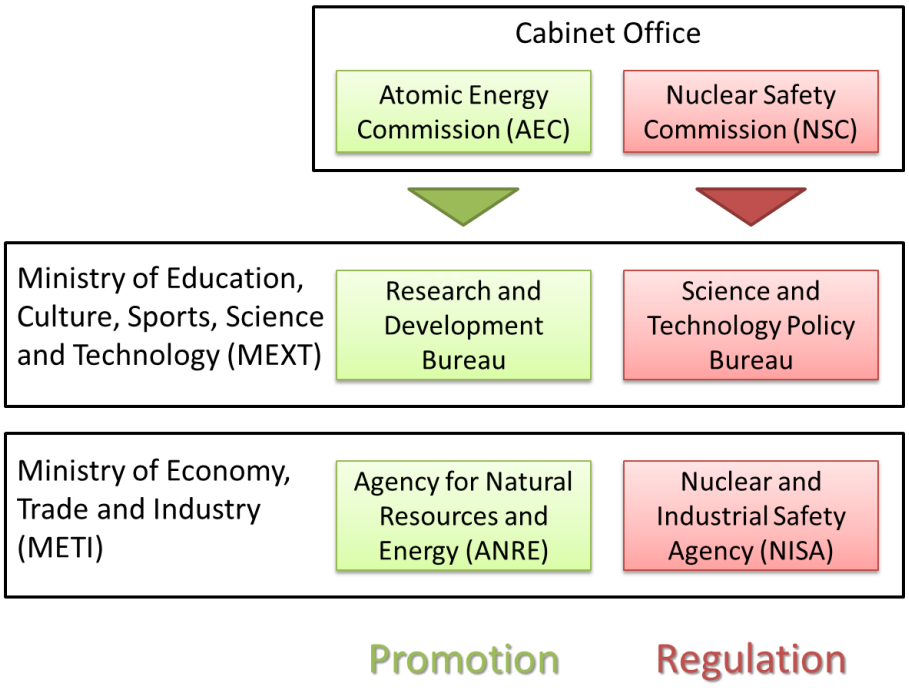


Figure 2-4: Governmental Organization for Promotion and Regulation for Nuclear Energy [23]

This overall administrative complexity resulted not only in overlapping jurisdictions, but also in further blurring the lines of responsibility. Institutional barriers also inhibited two different research institutes, the Japan Nuclear Energy Safety Organization (JNES) and the Japan Atomic Energy Agency (JAEA), from collaborating on safety research, since they were under the control of different ministries.

As Integrated Regulatory Review Service (IRRS) Review Team of IAEA recommended in 2007 that "the role of NISA as the regulatory body and that of NSC, especially in preparing safety guides, should be clarified," the relationship between NISA and NSC was also ambiguous. NISA was expected to take an initiative in safety regulations while its regulatory activities were checked by NSC, but NISA actually waited for NSC to formulate and revise the NSC Regulatory Guides, for fear of taking contradictory

actions. [2][3][12]

This ambiguity of responsibility was especially critical in management. Michael Weightman, the head of an IAEA inspection team that visited Japan in June 2011 in the aftermath of the Fukushima Daiichi nuclear disaster, stated that "the complexity of Japan's systems and organizations might delay decision making in times of crisis." In fact, numerous tasks—including assessing the accident information, giving evacuation orders, utilizing SPEEDI, and communicating risk information—were handled rather clumsily, exposing the weaknesses inherent in the existing structure. [2][4]

2.6.4 Detrimental effects of bureaucracy

One of the characteristics of the Japanese bureaucratic system is the reliance on precedent, putting strong emphasis on what was decided before and has been implemented since. As Kitazawa (2014) describes, once policies are put in place, it is extremely difficult to officially admit that they are wrong and make any amendments. [2]

For example, in the "Safety Design Regulatory Guide of Light Water Nuclear Power Reactor Facilities," which was revised in 1990, Guideline 27 on Design Considerations against Loss of Power stated that "The nuclear reactor facilities shall be so designed that safe shutdown and proper cooling of the reactor after shutting down can be ensured in case of a short-term total AC power loss[4]." The "short-term" had been commonly understood in practice since 1977 to be not more than thirty minutes, and the requirement of the guide was interpreted as a requirement to ensure sufficient battery capacity and others to maintain cooling functions for thirty minutes under a station blackout event.

In general, the provision was considered to be just appropriate. A person involved stated, "[T]he guide had

[4] Emphasis added by the author

been prepared by my seniors who had a good track record in the field and deep technical knowledge as well as good personalities and in whom I did have confidence, [which] convinced me to have no doubt in the guide." There were some people involved who raised concern about the effectiveness of the provision, but it did not lead to a strong question about the review practice or the adequacy of the guide, and the provision stating that a long-term SBO did not have to be considered was never revised. [8]

In addition, in the framework of the periodic personnel rotation discussed in 2.3.2, the safety regulator position was considered anything but a plum career; it was expected that nothing would go wrong, and if anything did, the officials would be blamed. Therefore, although they were charged with the most important government responsibility, which is to protect the nation's people, it was difficult for these officials to be experts with a strong sense of mission. This limitation of resources with technical expertise at NISA accelerated the micromanagement of hardware—in particular, document-based inspections discussed in 2.5.2—instead of taking a holistic approach to ensure the system safety. [2]

It was also found that the key challenge in government crisis management was how quickly the bureaucratic institutions could switch from routine operational mode, in which they prize the values of fairness, efficiency, respect for the law, and a bottom-up approach, to entirely different ways that times of crisis call for—flexibility, dynamic response, clear priorities, redundancy, and a top-down approach to decision making. [2]

2.7 Summary and Findings

As has been discussed in this chapter, multiple stakeholders contributed to the Fukushima Daiichi nuclear disaster. Although the accident was triggered by an external event, the CAST process helped show the whole picture of their unsafe control actions, summarized in Table 2-1, as well as their flawed

communication and coordination, which significantly damped the overall control structure for the Fukushima Daiichi Nuclear Power Plant that otherwise could have ensured its safety against a severe accident.

Table 2-1: Summary of Unsafe Control Actions by Each Stakeholder

Stakeholders	Unsafe Control Actions
TEPCO	
➢ Nuclear reactors	Inability to "*stop, cool and contain*" in response to an external event
➢ NPP operators	Inadequate control of severe accidents
➢ Head office	Lack of protection against huge tsunamis and mitigation of severe accidents Inadequate education, training and instruction to cope with serious accidents Ineffective emergency response and information disclosure
NISA	
➢ NISA	Inability to give the industry appropriate supervision Ineffective preparation for the occurrence of severe accidents Ineffective emergency response in the face of a compound nuclear disaster
➢ METI	Not offering NISA institutional independence or sufficient expertise
Off-site Center	Inability to take the initiative in the on-site response
NSC	Inability to check safety regulations and to decide effective regulation policies Inability to provide appropriate advice at the time of disaster
PM's Office	Causing confusion by decision making processes different from that in drills Not providing the residents with accurate information on evacuation
MEXT	Failure to safeguard the residents against radioactivity
Fukushima Prefecture and Municipalities	Insufficient emergency preparedness to protect the residents Inability to establish an initial response structure
General Electric	Providing system design susceptible to an accident

Scientists	Delay in research on nuclear safety Lack of communication within scientists and with different stakeholders
Radiation Emergency Medicine Network	Inability to cope with large-scale nuclear accidents

Figure 2-5 shows the control structure reflecting the actual state of the control loops before and at the time of the accident. There were, in fact, successful control actions, some of which do not appear in this analysis, such as the immediate report of an emergency from Fukushima Daiichi NPP operators. Nevertheless, it can be said that all the stakeholders—not just TEPCO and the national government—made inadequate or unplanned control actions regarding the safety design, safety management and emergency response, which, in combination, contributed to the accident.

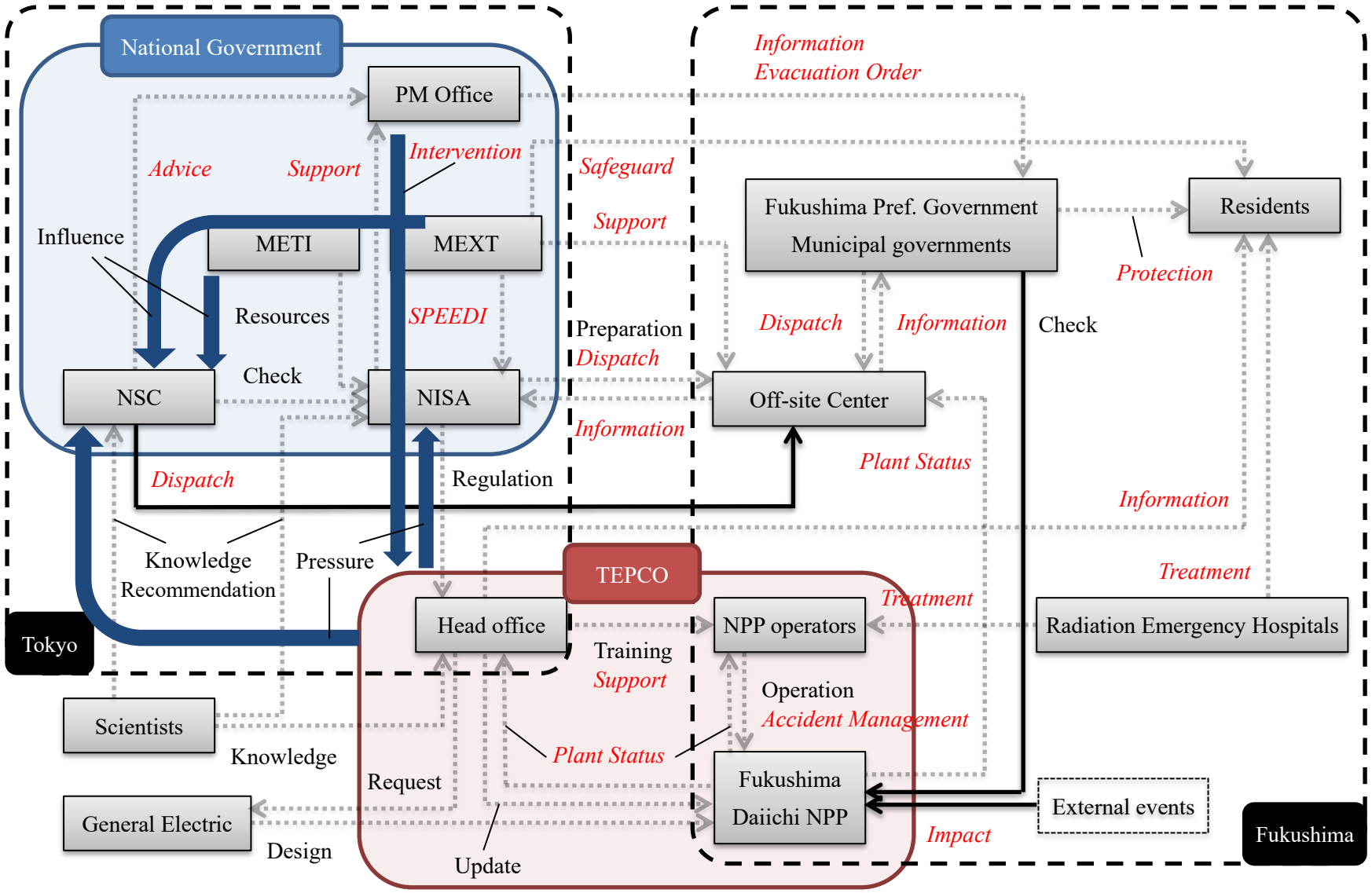


Figure 2-5: Actual System Control Structure for the Safety of the Fukushima Daiichi Nuclear Power Plant

[Note] *Italics*: emergency responses
Faded, dotted arrows: inadequate control actions
Bold arrows: unplanned (and undesirable) actions

Specifically, nuclear reactors at the Fukushima Daiichi Nuclear Power Plant, originally designed by General Electric, were not sufficiently prepared for tsunamis and the subsequent severe accidents. TEPCO, who had the prime responsibility for their safety, failed to take protection and mitigation measures against these events, assuming that it was not urgent. However, NISA lacked the ability to give appropriate supervision over TEPCO, the leader of the nuclear industry, partly because METI did not offer NISA institutional independence or sufficient expertise. NSC could not correct such incomplete regulations or provide effective regulation policies, nor could scientists sound the alarm on the safety of the nuclear power plant.

In addition, almost all of the emergency response actions by the stakeholders were found to be inadequate. Neither tangible nor intangible measures they had prepared were ineffective for severe accidents or compound nuclear disasters, owing to the shared assumption that such accidents could never occur. As a consequence, the infrastructure necessary for emergency response such as the Off-site Center and communication means had remained vulnerable to these accidents, and each organization had not been adequately structured to cope with the accidents swiftly and efficiently. These factors ultimately led not only to the inadequate emergency response by each stakeholder, but also to the lack of coordination between them.

As a causal factor, the “Safety Myth” shared in the “Nuclear Village” explained why the safety management was insufficient and why the stakeholders were not well prepared for the accident. The “Safety Myth” emerged as an “explanation on safety” for the purpose of promoting the use of nuclear power, and was enhanced by strengthening the micromanagement of hardware by the regulatory bodies,

which resulted from the risk of lawsuits as well as and administrative issues such as the lack of resources at the regulatory bodies. This “Safety Myth,” however, restricted the efforts by the stakeholders to ensure the actual safety, which, combined with other factors such as misconceptions about defense-in-depth, led to the lack of preparedness against severe accidents and compound nuclear disasters.

As a consequence, the stakeholders were not able to prevent the Fukushima Daiichi nuclear disaster, or to respond to the accident effectively.

.

2.8 References

[1] International Atomic Energy Agency (2006), “Fundamental safety principles : safety fundamentals,” Report, Vienna: IAEA, available at: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1273_web.pdf

[2] The Independent Investigation on the Fukushima Nuclear Accident (2014), “The Fukushima Daiichi Nuclear Power Station Disaster: Investigating the Myth and Reality”, Routledge.

[3] The Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company (2012), “Final Report”, available at: http://www.cas.go.jp/jp/seisaku/icanps/eng/final-report.html

[4] Kurokawa, K., Ishibashi, K., Oshima, K., Sakiyama, H., Sakurai, M., Tanaka, K. and Yokoyama, Y. (2012), “The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission (Main report)”, The National Diet of Japan, Tokyo, available at: http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/en/report/

[5] 自治体と原子力事業所との安全協定 (11-01-05-01) - ATOMICA - (n.d.) (Japanese). Retrieved November 23, 2015, from http://www.rist.or.jp/atomica/data/dat_detail.php?Title_No=16-03-04-01

[6] Asia & Japan Watch by The Asahi Shimbun (2011). More local governments demand safety agreements with nuclear plant operators. Retrieved November 23, 2015, from http://ajw.asahi.com/article/0311disaster/fukushima/AJ201106251998

[7] 東京電力株式会社福島第一原子力発電所周辺地域の安全確保に関する協定書 (1991) (Japanese), available at: http://www.pref.fukushima.lg.jp/download/1/kyoutei_youkou_2.pdf

[8] The Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company (2011), “Interim Report”, available at: http://www.cas.go.jp/jp/seisaku/icanps/eng/interim-report.html

[9] Wall Street Journal (2011), “Design Flaw Fueled Japanese Nuclear Disaster”. Retrieved November 25, 2015, from http://www.wsj.com/articles/SB10001424052702304887904576395580035481822

[10] International Atomic Energy Agency (2000), “Safety of Nuclear Power Plants: Design,” Report, Vienna: IAEA, available at: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1099_scr.pdf

[11] Hit lionhundred (2011), "IAEA 元事務次長「防止策、東電 20 年間放置　人災だ」"(Japanese). Retrieved December 5, 2015, from http://lionhundred.tumblr.com/post/6446056049/

[12] International Atomic Energy Agency (2007), "Integrated Regulatory Review Service to Japan: Report to the Japanese government," Report, Vienna: IAEA, available at: http://www-ns.iaea.org/downloads/actionplan/IRRS%20Mission%20to%20Japan__June_2007.pdf

[13] ABC News (2011), "Fukushima: Mark 1 Nuclear Reactor Design Caused GE Scientist To Quit In Protest". Retrieved December 5, 2015, from http://abcnews.go.com/Blotter/fukushima-mark-nuclear-reactor-design-caused-ge-scientist/story?id=13141287

[14] Dogauchi, M. (2012). "Private International Law Issues on Liability for Transboundary Nuclear Damage" (Japanese). Retrieved April 12, 2016, from http://hdl.handle.net/2065/36188

[15] Atomic Energy Society of Japan (2013), 「東京電力福島第一原子力発電所事故に関する調査委員会　中間報告」(Japanese), available at: http://www.aesj.or.jp/jikocho/interimreport.pdf

[16] NRC: Glossary (n.d.). Retrieved November 18, 2015, from http://www.nrc.gov/reading-rm/basic-ref/glossary.html

[17] International Atomic Energy Agency (2000), "Safety of nuclear power plants : design : safety requirements," Report, Vienna: IAEA, available at: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1099_scr.pdf

[18] Kobayashi, S. (2012), 「航空機事故に学ぶ 危険学の視点」(Japanese)

[19] Leveson, N. (2012). "Engineering a safer world: systems thinking applied to safety". Engineering systems. Cambridge, Massachusetts: MIT Press.

[20] Onishi, N., & Belson, K. (2011). "Culture of Complicity Tied to Stricken Nuclear Plant–New York Times Article (April 2.6.3011)", New York Times, available at: http://hillmanm.ism-online.org/files/2011/10/Culture-of-Complicity-Tied-to-Stricken-Nuclear-Plant-NYT.docx

[21] Ryu, A., Meshkati, D. (2014). "Why You Haven't Heard About Onagawa Nuclear Power Station after the Earthquake and Tsunami of March 11, 2011 – Nuclear Safety Culture in TEPCO and Tohoku Electric Power Company: The root-cause of the different fates of Fukushima Daiichi Nuclear

Power Plant and Onagawa Nuclear Power Station". Fall 2013. Daniel J. Epstein Department of Industrial & Systems Engineering, USC.

[22] Tokyo Electric Power Company, Inc. (2013), "Fukushima Nuclear Accident Summary & Nuclear Safety Reform Plan," available at: http://www.tepco.co.jp/en/press/corp-com/release/betu13_e/images/130329e0801.pdf

[23] MEXT – Our Organization (n.d.). Retrieved November 24, 2015, from http://www.mext.go.jp/english/science_technology/1303802.htm

Chapter 3. Hazard Analysis using the STPA Process

Following the investigation of the Fukushima Daiichi nuclear disaster and the review of why the safety design, safety management and emergency response were incomplete, the stakeholders involved in the nuclear power plants in Japan have made various changes to ensure the nuclear safety. For instance, the nuclear operators, including those other than Tokyo Electric Power Company (TEPCO), have made efforts so that their nuclear power plants can withstand severe accidents, and the national government reorganized the regulatory bodies and established a new agency solely responsible for nuclear safety regulation.

In this chapter, the STPA process, taking into account the accident analysis discussed in the previous chapter and these recent changes made after the Fukushima Daiichi nuclear disaster, reveals the safety constraints of key stakeholders such as power companies and the national and local governments, and identifies the potentially hazardous control actions with regard to the nuclear safety in Japan as well as the methods to control them.

Note that the focus of this analysis, similarly to the CAST process described in Chapter 2, is not technical details of power plants but a high-level and organizational set of constraints and actions.

3.1 Improvements by Stakeholders

In this section, various actions taken by the stakeholders after the Fukushima Daiichi nuclear disaster to improve the safety control structure—particularly with regard to safety management and emergency response—are described.

These improvements—including those not described below—are so extensive that, ideally, they will help overcome the administrative issues and prevent most, if not all, of the unsafe control actions with regard to safety management and emergency response that were discussed in the previous chapter. However, it

remains to be seen whether they will sufficiently bring fundamental changes to the stakeholders, especially TEPCO and other nuclear operators, as well as the government.

It should also be noted that training and raising awareness, listed by some stakeholders as follows, can be helpful but generally less sufficient than the change in the design of the safety control structure or in the safety culture, given that it is impossible to “redesign” humans. [1]

3.1.1 “Nuclear Reform” by TEPCO

In order to overcome the administrative issues that ultimately led to the nuclear accident, as discussed in Section 2.6, TEPCO established in September 2012 the "Nuclear Reform Special Task Force" led by the CEO. The role of the task force includes the reformation of existing safety culture, safety measures, disaster prevention measures, risk/crisis control protocol, information disclosure and risk communication methods from the ground up, in consideration of the lessons learned from the accident. [2]

At the same time, it established the "Nuclear Reform Monitoring Committee," which is an advisory body for TEPCO Board of Directors. It comprises both domestic and international experts, chaired by Dr. Dale Klein, the former Chairman of the US Nuclear Regulatory Commission. The Nuclear Reform Monitoring Committee also conducts external monitoring and supervising the activities of the Nuclear Reform Special Task Force in order to implement its nuclear reform. [3]

In their Nuclear Safety Reform Plan published in March 2013, TEPCO analyzed the dynamics of why the accident preparation was incomplete in the company, and set six measures to “sever the negative spiral,” as follows: [4]

- Measure 1: Reform starting from management

  “Management will undergo training to improve awareness of nuclear power safety, and periodic and

objective evaluations on awareness of nuclear power safety…. In addition, in order to raise the level of safety awareness throughout the entire organization, we will construct mechanisms where cross-sectional and multi-tiered discussions related to safety can be continued."

- Measure 2: Enhancement of oversight and support for management

  "The Nuclear Safety Oversight Office will be established, which is an internal regulatory organization under direct control of the Board of Directors for the purpose of bolstering the Board's management of nuclear safety risks. … The Office will independently and directly evaluate the corporate officers' operations of nuclear power business, and [will report] to the Board of Directors. Corporate officers will be monitored and advised by the Nuclear Safety Oversight Office with respect to nuclear power safety."

- Measure 3: Enhancement of ability to propose defense in depth

  "We will construct a system for developing the technological capability for promptly proposing the enhancement of highly cost-effective measures to improve safety in accordance with defense in depth. Also, we will be conscious that accident[s] and problems which have arisen anywhere around the world may also occur at our power stations, and will construct a system which appropriately applies operational experiences and information including those from other countries and other industries."

- Measure 4: Enhancement of risk communication activities

  "Risk communication will be promoted under the concept 'there is no absolute safety (zero risk) in nuclear' … to proactively announce risks and foster a relationship of trust through communication with siting communities, society and regulatory authorities regarding measures to further reduce risks. To reliably implement this risk communication, we will [set] expert risk communicators, who have had specific training and possess excellent technological knowledge."

- Measure 5: Reform of power station and Head Office emergency response organizations

"The emergency response organization will be reorganized in order to have the following characteristics [such as 'The number of people to be managed under one supervisor will be limited,' 'A clear command system will be created' and 'Roles and responsibilities will be clearly identified'], being modeled after the ICS (Incident Command System), which has been introduced in fire-fighting and other organizations in the United States. Also, training will be repeated so that the safety improvement measures and the emergency response organization itself can actually be utilized effectively."

- Measure 6: Reassessment of non-emergency power station organization and enhancement of capability for direct maintenance work

  "The Nuclear Safety Management Center will be established to bolster the capability to take a comprehensive view of nuclear safety at power stations. … Moreover, in order to develop the applied skills which enable TEPCO personnel to understand the state of damage to important facilities related to stable cooling of the nuclear reactors, to make a quick response regarding such damage and to deal with situations exceeding assumptions, meaningful tasks will be extracted from the maintenance work traditionally performed entirely by contractors and will be carried out by TEPCO personnel themselves to augment technological capabilities."

3.1.2 Actions by Other Nuclear Operators

Other nuclear operators as well as TEPCO suspended all the nuclear power plants in Japan after the Fukushima Daiichi nuclear disaster, and have taken the initiatives to update the safety features of their power plants, including but not limited to the requirements of the new safety regulations stated below, so that the power plants can withstand severe accidents.

For instance, Kansai Electric Power Company, the second largest nuclear operator in Japan following TEPCO, issued a document called “Commitment to Enhancing Nuclear Safety” vowing the following actions, while they prepare their nuclear power plants for extreme events such as massive earthquakes and tsunamis: [5]

- Awareness of the characteristics and risks of nuclear power generation:

  “Every one of us shall always bear in mind that once a severe accident happens due to lack of proper management, it could cause long-term environmental contamination and enormous damage to the people in the plant-hosting communities and the whole country, exerting both economic and social impacts on not only Japan but also worldwide.”

- Continuous removal or reduction of risks:

  “All executives and employees in charge of nuclear power generation shall fully understand the characteristics and risks of nuclear power generation and continually remove or reduce such risks while identifying and evaluating them, never believing at any moment that we have reached the goal of ensuring safety. By practicing these efforts at each level of the Defense-in-Depth, we will thoroughly establish measures to prevent accidents and reinforce countermeasures in a potential case where a nuclear accident could result in core damage.”

- Development of safety culture:

  “Executives shall work harder than ever to take the lead in developing human resources who support nuclear safety, allocating corporate resources and improving organizational and operational structures while all the employees in charge of nuclear power generation shall practice the following in their daily operations: Repeatedly question even in-house rules and common practices. Exchange diverse opinions and discuss issues uninhibitedly regardless of status or position. …”

3.1.3 Establishment of Nuclear Regulation Authority

Having identified the need to "win back public confidence on the government work on nuclear safety and to strengthen its functions," the government decided to create a new regulation authority five months after the accident, in order to separate the nuclear safety regulation body from the Ministry of Economy, Trade and Industry (METI)—the governmental organization advocating the use of nuclear energy—and to further strengthen its functions as a regulatory organization by unifying works related to nuclear safety regulation. [6]

Following the recommendation by the Advisory Committee for Prevention of Nuclear Accident in December 2011, the government drafted the bill of the Act for Establishment of the Nuclear Regulation Authority, which was passed and enacted in the Diet in June 2012.

The Nuclear Regulation Authority (NRA), which was formally established in September 2012 as an external organization of the Ministry of the Environment, is a council-system organization with a high degree of independence, consisting of one chairperson and four commissioners with Diet-approved appointment. The roles and responsibilities of nuclear safety, radiation protection and crisis management, which were formerly shared among several governmental organizations as discussed in Chapter 2, have come under the jurisdiction of NRA, as shown in Figure 3-1. [7]

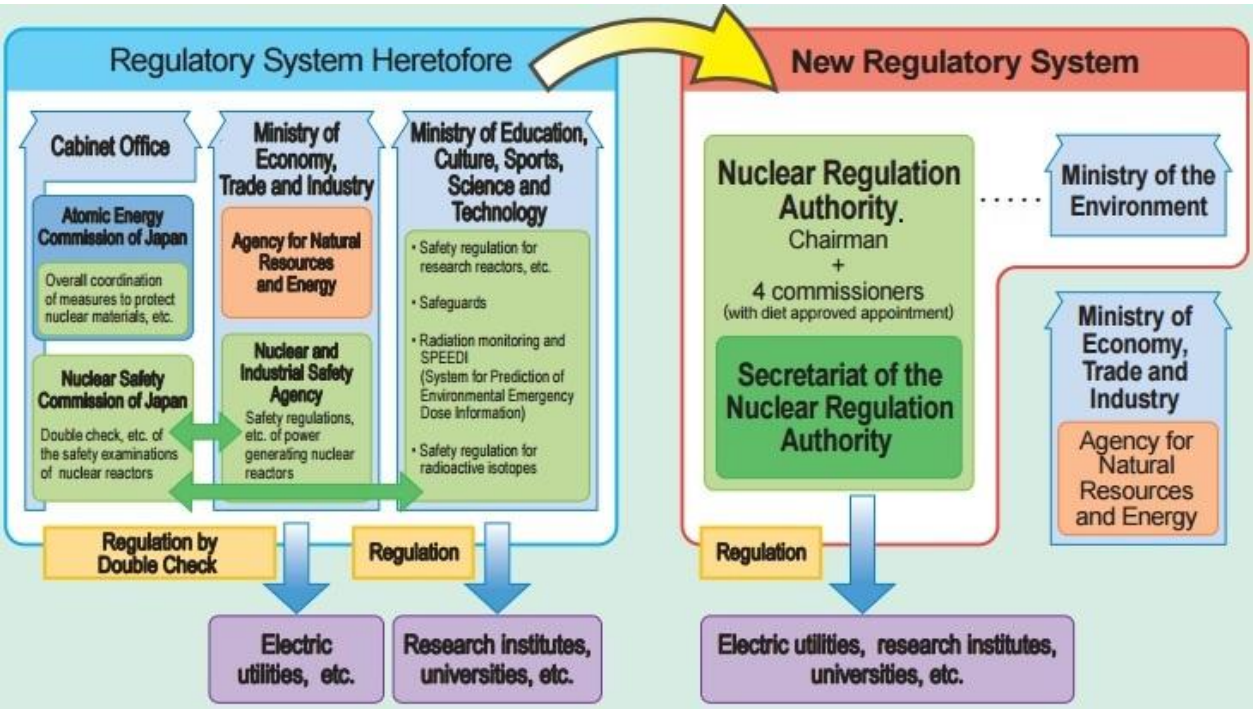


Figure 3-1: Administrative Reformation on Nuclear Safety Regulation [7]

The Secretariat, supporting the fulfillment of NRA's duties, is composed of governmental officials under the "no-return rule" (*i.e.* they cannot be seconded to other governmental organizations charged with the promotion of nuclear energy use). [7]

In January 2016, an Integrated Regulatory Review Service (IRRS) team of the International Atomic Energy Agency (IAEA) stated that Japan's regulatory body for nuclear and radiation safety has demonstrated independence and transparency since it was set up in 2012, while the team also noted that it needs to further strengthen its technical competence in light of upcoming restarts of nuclear facilities. [8]

3.1.4 Improvement of Safety Regulations

In January 2012, the government published the ways to improve nuclear safety regulations. This led to the

amendment of the Nuclear Reactor Regulation Act (Act No. 166 of 1957) so that it can do the following. [7][9]

- Deal with “the unexpected,” taking severe accidents into consideration:

  The previous assumptions on the impact of earthquakes, tsunamis and other external events such as volcanic eruptions, tornadoes and forest fires were reevaluated, and countermeasures for nuclear safety against these external events were decided to be enhanced. Furthermore, it is required to take countermeasures against internal fires and internal flooding, and to enhance the reliability of on-site and off-site power sources to deal with the possibility of station blackout.

  In addition to the above-described enhancement of countermeasures established at design basis, more stringent regulations have been developed with an underlying assumption that severe accidents could occur at any moment. Countermeasures for severe accident response against core damage, containment vessel damage and a diffusion of radioactive materials, enhanced measures for water injection into spent fuel pools, countermeasures against malicious airplane crash, and an installation of emergency response building are also required.

- Regulate based on the latest scientific and technical knowledge being applied on safety issues to existing facilities (back-fitting):

  The new regulations are applied to the existing nuclear power stations. A five-year deferment period from the time of enforcement of the new regulations is given to a realization of some safety measures including filter vents for pressurized water reactors and control rooms for the time of emergency.

- Introduce an operational limit of 40 years, in principle, to ensure the safety of aged power reactors:

  Nuclear power reactors, which are generally limited to 40 years of operation life-time, will be given one-time legal permission to extend it to another 20 years. Operators applying for such an extension are required to implement special inspections to assess whether their facilities meet the latest

technical standards and properly maintain their operation from the viewpoints of any expected wear/tear and deterioration of facilities and equipment in the 20-year time period.

- Specify licensee's responsibility to constantly improve the safety of its facilities:
  It is necessary for the new regulatory requirements and regulations to be constantly reviewed with new findings and scientific technologies that are acknowledged in Japan and overseas with continuous efforts to enhance nuclear safety.

3.1.5 Improvement of Emergency Response

The government also reformed the emergency response by amending the Act on Special Measures Concerning Nuclear Emergency Preparedness (Act No. 156 of 1999) in June 2012, so as to enhance the structure and function of the Nuclear Emergency Response Headquarters (NERHQ) established at the Prime Minister's Office, and to grant NRA authority to establish the Nuclear Emergency Response Guideline (hereinafter referred to simply as the "Guideline").

The Guideline was promulgated in October 2012 by NRA so that various stakeholders involved in the emergency response, including the national government, local governments and nuclear operators, could respond to nuclear disasters smoothly. It also requires updated preparedness against nuclear disasters, such as the improved functions of Off-site Centers and radiation emergency hospitals. [7]

In addition, the Cabinet Office (CAO), a government agency in charge of protection against disasters—formerly other than nuclear disasters—was also assigned to take the responsibility of nuclear emergency preparedness and response under the direction of the Minister of State for Nuclear Emergency Preparedness, a newly created ministerial post. Specifically, CAO supports the local governments to develop their Regional Disaster Prevention Plans, which include but are not limited to plans on nuclear

emergency. In a nuclear emergency, CAO takes the initiative of off-site emergency response and supports the Prime Minister's Office jointly with NRA, which takes charge of on-site emergency response and other technical matters. [7]

3.2 Safety Constraints and Control Structure

In this section, system-level accidents of nuclear power plants in Japan, their high-level system hazards and the system safety constraints to prevent them are identified. Then, the current system control structure for the safety design, safety management and the emergency response is presented.

3.2.1 System Level Accidents, Hazards and Safety Constraints

Although various types of accidents can be considered, including the failure of components dealing with non-radioactive substances, the system level accidents of nuclear power plants are defined here as 1) core meltdown, 2) widespread release of radioactive materials to the environment, and 3) exposure of neighborhood residents to the radioactive materials.

Such accidents can be triggered by such hazards as:

(H1) Failure in decay heat removal inside the reactor

(H2) Unsuccessful containment of radioactive substances

(H3) Failure of the residents to evacuate

In this context, system safety constraints of nuclear power plants are:

(SC1) Decay heat inside the reactor must be sufficiently removed at any time

(SC2) Radioactive substances must be contained even when the reactor fails

(SC3) Neighborhood residents must evacuate quickly before they are exposed to the radioactive materials

Note that, more generally, these safety constraints correspond to defense-in-depth, discussed in 2.5.3 in the previous chapter.

3.2.2 Safety Control Structure

Figure 3-2 shows the system control structure for the safety design and the safety management of nuclear power plants in Japan and the emergency response in case of an accident, according to the safety constraints of stakeholders discussed in the previous Section 3.1. See also Section 2.1 in the previous chapter for the roles of stakeholders that existed before the Fukushima Daiichi nuclear disaster.

For the purpose of this analysis, this control structure model is slightly different from the one represented in the previous chapter (Figure 2-1) in several aspects. First of all, this control structure reflects the reformation of relevant governmental organizations discussed above—NRA established to replace the former regulatory bodies such as the Nuclear and Industrial Safety Agency (NISA) and the Nuclear Safety Commission (NSC), drastically reducing the administrative complexity within the national government described in Chapter 2. Second, the power company listed here can be any nuclear operator in Japan, not just TEPCO, and local bodies (prefectural and municipal governments), Off-site Centers and residents could be those close to any one of the nuclear power plants.

Furthermore, while some actions shown in Figure 2-1 are omitted, other actions are added to the diagram. For instance, NRA gains information on plant status through inspection to see if safety management is properly conducted; if an emergency happens, nuclear power plant (NPP) staff should immediately report to that effect to the national and local governments, as Fukushima Daiichi NPP operators actually did. CAO is added as one of the national government organizations that play important roles for emergency

response, as discussed in 3.1.5.

Note that the manufacturer of the nuclear power plant is still included since, while it is unlikely that new power plants will be planned in the foreseeable future, there may be demands for replacing old power plants, in which case the manufacturers will design new reactors. Scientists—both domestic and international scientists—are more experienced and can provide better advice to manufacturers than in the 1960s, when the manufacturers designed the early nuclear reactors but the scientific communities such as the Atomic Energy Society of Japan, as well as the International Atomic Energy Agency (IAEA), were still fledgling.

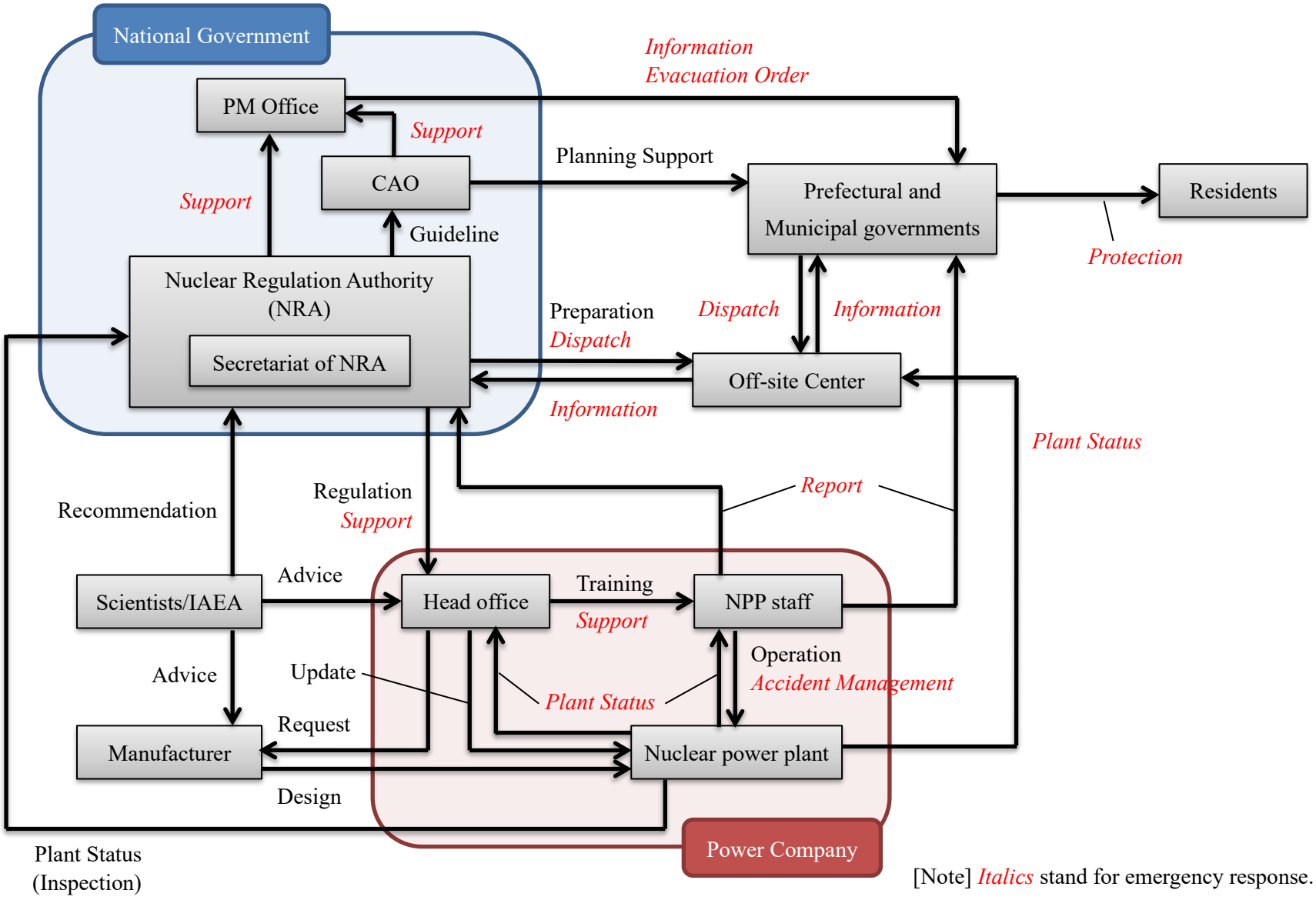


Figure 3-2: System Control Structure for the Safety of Nuclear Power Plants in Japan

3.3 Step 1—Identifying Unsafe Control Actions

The hazards listed in 3.2.1 might be triggered either by ineffective safety design, safety management and emergency preparation, or by inappropriate emergency response. In this section, potentially hazardous control actions are identified by performing STPA Step 1, based on the safety control structure built in the previous section.

Note that some of the unsafe control actions shown below actually happened before and during the Fukushima Daiichi nuclear disaster, as discussed in the previous chapters, while others are imaginary but could take place in the future.

3.3.1 Unsafe Control Actions in Peacetime

Table 3-1 shows the list of unsafe control actions in peacetime (UCA_p with regard to safety design, safety management and emergency preparation, represented in non-italic letters in Figure 3-2).

Table 3-1: STPA Step 1 for Safety Design, Safety Management and Emergency Preparation

Command	Not Providing Causes Hazard	Providing Causes Hazard	Timing / Sequencing Causes Hazard	Stopped Too Soon or Applied Too Long
Manufacturer designs power plant	Manufacturer fails to provide design with necessary safety features. (UCA_p 1-1)	Manufacturer provides design with unsafe features. (UCA_p 1-2)	N/A	N/A

NPP staff operates power plant	NPP staff fails to control power plant properly in abnormal condition. (UCA_p 2-1)	An erroneous action by NPP staff causes abnormality of power plant. (UCA_p 2-2)	NPP staff controls power plant in abnormal condition too late. (UCA_p 2-3)	NPP staff stops controlling the abnormality when it is not solved. (UCA_p 2-4)
Head office updates power plant	Head office fails to update power plant when it is vulnerable. (UCA_p 3-1)	Head office updates power plant improperly and makes it vulnerable. (UCA_p 3-2)	Head office updates power plant too late to avoid an accident. (UCA_p 3-3)	N/A
Head office trains NPP staff	Head office fails to train NPP staff enough to prevent or mitigate accidents. (UCA_p 4-1)	Head office trains NPP staff erroneously and they cause accidents. (UCA_p 4-2)	N/A	Head office stops training NPP staff when they remain untrained. (UCA_p 4-3)
NRA regulates power company	NRA fails to provide effective regulations. (UCA_p 5-1)	NRA provides wrong regulations that make the power plant vulnerable. (UCA_p 5-2)	NRA fails to enforce regulations in time. (UCA_p 5-3)	N/A
NRA prepares Off-site Center	NRA fails to prepare Off-site Center enough to withstand extreme events. (UCA_p 6-1)	NRA improperly prepares Off-site Center and makes it vulnerable. (UCA_p 6-2)	NRA prepares Off-site Center too late. (UCA_p 6-3)	NRA stops preparing Off-site Center when it remains vulnerable to extreme events. (UCA_p 6-4)
NRA provides Guideline for CAO	NRA fails to provide effective Guideline for CAO. (UCA_p 7-1)	NRA provides ineffective Guideline for CAO. (UCA_p 7-2)	NRA provides Guideline for CAO too late. (UCA_p 7-3)	N/A

CAO supports planning of disaster prevention	CAO fails to support planning of disaster prevention by local bodies. (UCA_p 8-1)	CAO impedes sound planning of disaster prevention by local bodies. (UCA_p 8-2)	CAO supports planning of disaster prevention by local bodies too late. (UCA_p 8-3)	CAO stops supporting planning of disaster prevention when local bodies need help. (UCA_p 8-4)
Scientists/ IAEA provide advice to head office/mfr. and rec. to NRA	Scientists/IAEA fail to provide advice to head office/mfr. or recommendation to NRA. (UCA_p 9-1)	Scientists/IAEA provide wrong advice or recommendation that could mislead the head office/mfr. or NRA. (UCA_p 9-2)	Scientists/IAEA provide advice to head office/mfr. or recommendation to NRA too late. (UCA_p 9-3)	Scientists/IAEA stop providing advice or recommendation when they were still necessary. (UCA_p 9-4)

3.3.2 Unsafe Control Actions in an Emergency

Table 3-2 shows the list of unsafe control actions in an emergency (UCA_e with regard to emergency response, represented in *Italic* letters in Figure 3-2).

Table 3-2: STPA Step 1 for Emergency Response

Command	Not Providing Causes Hazard	Providing Causes Hazard	Timing / Sequencing Causes Hazard	Stopped Too Soon or Applied Too Long
Power plant sends plant status to NPP staff etc.	Power plant does not send plant status when emergency happens. (UCA_e 1-1)	N/A	Power plant sends plant status too late after emergency happens. (UCA_e 1-2)	Power plant stops sending plant status when the accident is not solved. (UCA_e 1-3)

NPP staff reports the emergency to NRA and local bodies	NPP staff fails to report the emergency to NRA or local bodies. (UCA_e 2-1)	N/A	NPP staff reports the emergency to NRA or local bodies too late. (UCA_e 2-2)	N/A
NPP staff manages the accident	NPP staff fails to manage the accident properly. (UCA_e 3-1)	An erroneous action by NPP staff exacerbates the accident. (UCA_e 3-2)	NPP staff responds to the accident too late. (UCA_e 3-3)	NPP staff stops managing the accident when it is not solved. (UCA_e 3-4)
Head office support NPP staff	Head office fails to support NPP staff to mitigate the accident. (UCA_e 4-1)	Head office supports NPP staff erroneously and the staff exacerbates the accident. (UCA_e 4-2)	Head office supports NPP staff too late to mitigate the accident. (UCA_e 4-3)	Head office stops supporting NPP staff when they need assistance. (UCA_e 4-4)
NRA supports power company	NRA fails to provide advice to power company. (UCA_e 5-1)	NRA provides wrong advice to power company and the company exacerbates the accident. (UCA_e 5-2)	NRA provides advice to power company too late. (UCA_e 5-3)	NRA stops providing advice to power company when it needs assistance. (UCA_e 5-4)
NRA and CAO support PM Office	NRA or CAO fails to provide advice to PM Office. (UCA_e 6-1)	NRA or CAO provides wrong advice and PM Office exacerbates the accident. (UCA_e 6-2)	NRA or CAO provides advice to PM Office too late. (UCA_e 6-3)	NRA or CAO stops providing advice to PM Office when it needs assistance. (UCA_e 6-4)
NRA and local bodies dispatch personnel to Off-site Center	NRA or local bodies fail to dispatch personnel to Off-site Center. (UCA_e 7-1)	N/A	NRA or local bodies dispatch personnel to Off-site Center too late. (UCA_e 7-2)	NRA or local bodies stop dispatching personnel when emergency continues. (UCA_e 7-3)

Off-site Center sends info. to NRA and local bodies	Off-site Center fails to send information to NRA or local bodies. (UCA$_e$ 8-1)	Off-site Center sends incorrect information to NRA or local bodies. (UCA$_e$ 8-2)	Off-site Center sends information to NRA or local bodies too late. (UCA$_e$ 8-3)	Off-site Center stops sending information when NRA and/or local bodies need it. (UCA$_e$ 8-4)
PM Office provides info. or orders evacuation	PM Office fails to provide information or to order evacuation. (UCA$_e$ 9-1)	PM Office provides wrong information that endangers residents. (UCA$_e$ 9-2)	PM Office provides information or orders evacuation too late. (UCA$_e$ 9-3)	N/A
Local bodies protect residents	Local bodies fail to protect residents. (UCA$_e$ 10-1)	N/A	Local bodies protect residents too late. (UCA$_e$ 10-2)	Local bodies stop protecting residents when they need help. (UCA$_e$ 10-3)

3.4 Step 2—Identifying the Causes of Unsafe Control Actions

In this section, STPA Step 2 identifies causal scenarios leading to the hazardous control actions discussed in the previous section, by examining the safety control structure (Figure 3-2) and its parts. Possible safety requirements (*i.e.* examples of safety requirements) to prevent these causal scenarios from happening are also discussed.

Note that, while it is more precise that each unsafe control action is discussed to identify separate causal scenarios, multiple unsafe control actions are lumped together in this analysis and discussed in a single table for simplicity.

3.4.1 Causal Factors of Unsafe Control Actions in Peacetime

For each stakeholder, the causal scenarios leading to unsafe control actions in peacetime (See 3.3.1),

including possible degradation of designed controls, are shown in Tables 3-3 through 3-8 below. With these scenarios in mind, possible safety requirements of the said stakeholder (and other stakeholders) are also discussed in the same tables.

Table 3-3: UCAs of the Manufacturer in Peacetime, Causal Scenarios and Safety Requirements

UCA_p: Unsafe control actions
(UCA_p 1-1) Manufacturer fails to provide design with necessary safety features. (UCA_p 1-2) Manufacturer provides design with unsafe features.
CS_p: Causal scenarios leading to UCAs
(CS_p 1.a) Manufacturer does not know or misunderstands the use contexts (e.g. natural environment) and associated risks critical for plant safety. (CS_p 1.b) Manufacturer fails to include necessary safety features owing to cost or schedule constraints, or erroneously believes that such safety features are unnecessary. Otherwise, it inadvertently includes other features that could inhibit safety features from working properly. (CS_p 1.c) Manufacturer designs the system properly, but the power plant is constructed improperly.
SR_p: Possible safety requirements
(SR_p 1.a) Manufacturer must listen to the operator to understand the use contexts and associated risks properly, and must identify the factors critical for plant safety. (SR_p 1.b) Manufacturer must ensure that their design team includes necessary safety features in the design and that they work properly—and other features do not inhibit safety features—at any condition in the use contexts. (SR_p 1.c) Manufacturer must accurately and unambiguously communicate the system design to its suppliers and constructors, and must ensure that the power plant is constructed as designed.

Table 3-4: UCAs of NPP Staff in Peacetime, Causal Scenarios and Safety Requirements

UCA_p: Unsafe control actions
(UCA_p 2-1) NPP staff fails to control power plant properly in abnormal condition. (UCA_p 2-2) An erroneous action by NPP staff causes abnormality of power plant. (UCA_p 2-3) NPP staff controls power plant in abnormal condition too late. (UCA_p 2-4) NPP staff stops controlling the abnormality when it is not solved.
CS_p: Causal scenarios leading to UCAs
(CS_p 2.a) Power plant does not signal in a timely manner—or stops signaling—its abnormal condition to NPP staff, or they do not recognize the abnormal condition signaled by the power plant. (CS_p 2.b) NPP staff does not know how to deal with the abnormality, or fails to do so owing to human resource constraints. Otherwise, NPP staff misunderstands the abnormal condition, or erroneously believes no (immediate/further) control actions should be provided. *—See also (CS_p 4.a) through (CS_p 4.e) with regard to the head office offering training to NPP staff.* (CS_p 2.c) NPP staff inadvertently takes an erroneous control action owing to button confusion or mode confusion. (CS_p 2.d) NPP staff chooses correct control actions, but they are not properly processed in a timely manner.
SR_p: Possible safety requirements
(SR_p 2.a) Power plant must be designed and maintained so that any abnormal condition is signaled in a timely manner and is easily recognized by NPP staff. The signals must be accurate and clear-cut, and must be continued unless the abnormality is completely solved. (SR_p 2.b) NPP staff must be provided with enough resources and sufficiently trained to deal with any kind of abnormalities, and must be motivated always to make safer choices. Feedback on control actions must be accurately and continuously gathered from the power plant in a timely manner. *—See also (SR_p 4.a) through (SR_p 4.e) with regard to the head office offering training to NPP staff.* (SR_p 2.c) Button arrangement and operation mode must be simple and intuitive enough (*i.e.* not too complicated) to avoid confusion, and any input—if *and* only if it is potentially hazardous—must be double-checked. (SR_p 2.d) NPP staff must periodically check safety features so that they work properly in a timely manner at any condition.

Table 3-5: UCAs of the Head Office in Peacetime, Causal Scenarios and Safety Requirements

UCA_p: Unsafe control actions (1/2)
(UCA_p 3-1) Head office fails to update power plant when it is vulnerable. (UCA_p 3-2) Head office updates power plant improperly and makes it vulnerable. (UCA_p 3-3) Head office updates power plant too late to avoid an accident.
CS_p: Causal scenarios leading to UCAs (1/2)
(CS_p 3.a) Head office does not know or misunderstands the plant status, use contexts and associated risks critical for plant safety. (CS_p 3.b) Head office erroneously believes that such safety features are unnecessary or have no urgency. Otherwise, it inadvertently adds features that could inhibit safety features from working properly. (CS_p 3.c) Head office fails to add—or postpones adding—necessary safety features owing to cost or schedule constraints. (CS_p 3.d) Head office plans to update the system properly, but the power plant is updated improperly.
SR_p: Possible safety requirements (1/2)
(SR_p 3.a) Head office must check all of its power plants technically and periodically and listen to the operating staff to understand the plant status, use contexts and associated risks properly, and must identify the factors that should be updated for improved plant safety. (SR_p 3.b) Head office must constantly ensure that it added necessary safety features to all of its power plants in a timely manner, and must continuously update its perception of the adequacy of the safety features by demonstrating that they work properly—and other features do not inhibit safety features—at any condition in the use contexts. (SR_p 3.c) Head office must maintain enough resources to add necessary safety features in a timely manner. (SR_p 3.d) Head office must accurately and unambiguously communicate the system update to its suppliers and constructors, and must ensure that all of its power plants are updated as planned.
UCA_p: Unsafe control actions (2/2)

(UCA_p 4-1) Head office fails to train NPP staff enough to prevent or mitigate accidents. (UCA_p 4-2) Head office trains NPP staff erroneously and they cause accidents. (UCA_p 4-3) Head office stops training NPP staff when they remain untrained.
CS_p: Causal scenarios leading to UCAs (2/2)
(CS_p 4.a) Head office does not know or misunderstands the skill of NPP staff required to prevent or mitigate accidents. (CS_p 4.b) Head office erroneously believes that such training is unnecessary or has no urgency. Otherwise, it inadvertently provides instruction that conflicts with safe operation. (CS_p 4.c) Head office fails to train—or stops training—NPP staff for safety owing to human resource constraints. (CS_p 4.d) Head office plans training properly, but the training is conducted improperly. (CS_p 4.e) Appropriate training is provided for the first time, but it gradually becomes routine and emasculated.
SR_p: Possible safety requirements (2/2)
(SR_p 4.a) Head office must assess the skill level of NPP staff periodically. (SR_p 4.b) Head office must constantly ensure that it provides effective training for NPP staff, and must continuously update its perception of their capability of performing properly—and other features do not inhibit their safe operation—at any condition in the use contexts. (SR_p 4.c) Head office must maintain enough resources to train NPP staff in a timely manner. (SR_p 4.d) Head office must accurately and unambiguously communicate the aims and contents of training to the trainers and see if the training is properly conducted by them. Feedback on control actions must be accurately and continuously gathered from NPP staff in a timely manner. (SR_p 4.e) Head office must devise a method to prevent the training from becoming emasculated, such as conducting a surprise inspection or randomizing the contents of inspection.

Table 3-6: UCAs of NRA in Peacetime, Causal Scenarios and Safety Requirements

UCA_p: Unsafe control actions (1/3)
(UCA_p 5-1) NRA fails to provide effective regulations. (UCA_p 5-2) NRA provides wrong regulations that make the power plant vulnerable. (UCA_p 5-3) NRA fails to enforce regulations in time.
CS_p: Causal scenarios leading to UCAs (1/3)
(CS_p 5.a) NRA does not know or misunderstands the plant status, use contexts and associated risks critical for plant safety, or the power company conceals such information. (CS_p 5.b) NRA erroneously believes some effective regulations to be unnecessary or have no urgency, and/or other policies conflicting with safety to be beneficial. Otherwise, regulations gradually become routine and emasculated. (CS_p 5.c) NRA fails to enforce/update—or postpones enforcing/updating—regulations owing to human resource constraints, or pressures from outsiders. (CS_p 5.d) NRA plans to enforce regulations, but the power company does not fully comply with them.
SR_p: Possible safety requirements (1/3)
(SR_p 5.a) NRA must inspect all the nuclear power plants across the nation periodically, and must maintain the expertise enough to discern the plant status and associated risks, and to identify the factors that should be updated for improved plant safety. (SR_p 5.b) NRA must constantly update its perception of the efficacy of regulations over power companies. A third party must continuously check whether effective regulations are formed and properly enforced and must make recommendations, if necessary. —*See also (SR_p 9.a) through (SR_p 9.c) with regard to scientists providing advice and recommendation.* (SR_p 5.c) NRA must maintain enough resources to enforce and update regulations in a timely manner, but must be immune from outside pressures. (SR_p 5.d) NRA must accurately and unambiguously communicate the aims and contents of regulations to the power companies, and must check periodically whether these regulations have been complied with as intended.
UCA_p: Unsafe control actions (2/3)

(UCA_p 6-1) NRA fails to prepare Off-site Center enough to withstand extreme events. (UCA_p 6-2) NRA improperly prepares Off-site Center and makes it vulnerable. (UCA_p 6-3) NRA prepares Off-site Center too late. (UCA_p 6-4) NRA stops preparing Off-site Center when it remains vulnerable to extreme events.
CS_p: Causal scenarios leading to UCAs (2/3)
(CS_p 6.a) NRA does not know or misunderstands the states and associated risks of Off-site Centers, or erroneously believes that updates of Off-site Centers are unnecessary or have no urgency. Otherwise, NRA inadvertently adds features that could inhibit Off-site Centers from working properly. (CS_p 6.b) NRA fails to update—or postpones/stops updating—the Off-site Center owing to cost or schedule constraints. (CS_p 6.c) NRA plans to update Off-site Center properly but does so improperly.
SR_p: Possible safety requirements (2/3)
(SR_p 6.a) NRA must check all the Off-site Centers across the nation technically and periodically to understand their states and to see whether they work properly at any time, and must identify the factors that should be updated to maintain their functions. (SR_p 6.b) NRA must maintain enough resources to update Off-site Centers in a timely manner. (SR_p 6.c) NRA must accurately and unambiguously communicate the update of Off-site Centers to their suppliers and constructors.
UCA_p: Unsafe control actions (3/3)
(UCA_p 7-1) NRA fails to provide effective Guideline for CAO. (UCA_p 7-2) NRA provides ineffective Guideline for CAO. (UCA_p 7-3) NRA provides Guideline for CAO too late.
CS_p: Causal scenarios leading to UCAs (3/3)
(CS_p 7.a) NRA erroneously believes it provided an effective Guideline, when it did not. Otherwise, NRA inadvertently adds features that could inhibit the Guideline from working properly. (CS_p 7.b) NRA does not have enough expertise on nuclear emergency response, or it fails to

provide/update—or postpones providing/updating—a Guideline owing to human resource constraints. (CS_p 7.c) NRA forms the Guideline, but the aims and contents are not properly communicated to CAO.
SR_p: Possible safety requirements (3/3)
(SR_p 7.a) CAO must check the effectiveness of the Guideline provided by NRA, and recommend it, if necessary, to revise the Guideline. (SR_p 7.b) NRA must maintain enough resources to provide and update a Guideline in a timely manner. (SR_p 7.c) NRA must accurately and unambiguously communicate the aims and contents of the Guideline to CAO in a timely manner.

Table 3-7: UCAs of CAO in Peacetime, Causal Scenarios and Safety Requirements

UCA_p: Unsafe control actions
(UCA_p 8-1) CAO fails to support planning of disaster prevention by local bodies. (UCA_p 8-2) CAO impedes sound planning of disaster prevention by local bodies. (UCA_p 8-3) CAO supports planning of disaster prevention by local bodies too late. (UCA_p 8-4) CAO stops supporting planning of disaster prevention when local bodies need help.
CS_p: Causal scenarios leading to UCAs
(CS_p 8.a) CAO does not know or misunderstands whether the Regional Disaster Prevention Plans formed by local bodies conform to the latest Guideline, or erroneously believes that providing support for local bodies is unnecessary or has no urgency. Otherwise, CAO inadvertently adds features that could inhibit their Regional Disaster Prevention Plans from working properly. (CS_p 8.b) CAO fails to support—or postpones/stops supporting—planning of disaster prevention by local bodies owing to human resource constraints. (CS_p 8.c) CAO understands the aims and contents of the Guideline as a basis of Regional Disaster Prevention Plans, but communicates them to local bodies improperly.
SR_p: Possible safety requirements

(SR_p 8.a) CAO must assess periodically whether all of the Regional Disaster Prevention Plans formed by local bodies conform to the latest Guideline and are effective enough for disaster prevention, and must identify the factors that should be updated in these plans. (SR_p 8.b) CAO must maintain enough resources to support planning of disaster prevention by local bodies in a timely manner. (SR_p 8.c) CAO must accurately and unambiguously communicate the aims and contents of the Guideline—as a basis of their Regional Disaster Prevention Plans—to local bodies.

Table 3-8: UCAs of Scientists/IAEA in Peacetime, Causal Scenarios and Safety Requirements

UCA_p: Unsafe control actions
(UCA_p 9-1) Scientists/IAEA fail to provide advice to head office/manufacturer or recommendation to NRA. (UCA_p 9-2) Scientists/IAEA provide wrong advice or recommendation that could mislead the head office/manufacturer or NRA. (UCA_p 9-3) Scientists/IAEA provide advice to head office/manufacturer or recommendation to NRA too late. (UCA_p 9-4) Scientists/IAEA stop providing advice or recommendation when they are still necessary.
CS_p: Causal scenarios leading to UCAs
(CS_p 9.a) Scientists/IAEA do not know or misunderstand whether power companies, manufacturers and NRA perform sufficiently with regard to maintaining safety, or erroneously believe that providing advice or recommendation is unnecessary or has no urgency. (CS_p 9.b) Scientists/IAEA fail to provide—or postpone/stop providing—advice or recommendation owing to human resource constraints, or pressures from outsiders, or believe providing advice or recommendation is not their business. (CS_p 9.c) Scientists/IAEA form the advice or recommendation properly, which, however, is understood improperly by power companies, manufacturers or NRA.
SR_p: Possible safety requirements

(SR_p 9.a) Scientists/IAEA must assess periodically whether power companies, manufacturers and NRA perform sufficiently with regard to maintaining safety, and must identify the factors that should be improved. (SR_p 9.b) Scientists/IAEA must be mandated to serve as a "watchdog over nuclear safety," must maintain enough resources to provide advice for power companies/manufacturers and recommendation for NRA in a timely manner, but must be immune from outside pressures. (SR_p 9.c) Scientists/IAEA must accurately and unambiguously communicate the aims and contents of the advice to power companies/manufacturers and the recommendation to NRA.

3.4.2 Causal Factors of Unsafe Control Actions in an Emergency

Similarly to 3.4.1, the causal scenarios that could lead to unsafe control actions in an emergency (See 3.3.2) are listed in Tables 3-9 through 3-15 below by each stakeholder. Note that these hazardous control actions in an emergency may stem from insufficient preparation in peacetime.

Table 3-9: UCAs of the Power Plant in an Emergency, Causal Scenarios and Safety Requirements

UCA_e: Unsafe control actions
(UCA_e 1-1) Power plant does not send plant status when emergency happens. (UCA_e 1-2) Power plant sends plant status too late after emergency happens. (UCA_e 1-3) Power plant stops sending plant status when the accident is not solved.
CS_e: Causal scenarios leading to UCAs
(CS_e 1.a) There are no sensors that can detect the state of emergency inside the power plant. Otherwise, such sensors are broken/have broken down, or do not work properly. (CS_e 1.b) Algorithm to send plant status has a defect, or the signal is not transmitted properly, because of damage to—or aged deterioration of—transmission circuits, for instance.

SR_e: Possible safety requirements
(SR_e 1.a) The power plant must be equipped with sensors that can detect the state of emergency, and these sensors must be maintained to work properly at any condition. (SR_e 1.b) Algorithm to send plant status and transmission circuits must be constantly checked and upgraded to work properly at any condition.

Table 3-10: UCAs of NPP Staff in an Emergency, Causal Scenarios and Safety Requirements

UCA_e: Unsafe control actions (1/2)
(UCA_e 2-1) NPP staff fails to report the emergency to NRA or local bodies. (UCA_e 2-2) NPP staff reports the emergency to NRA or local bodies too late.
CS_e: Causal scenarios leading to UCAs (1/2)
(CS_e 2.a) NPP staff does not recognize the signal of emergency. Otherwise, they misunderstand the signal, or erroneously believe that it is a false alarm or not safety-critical. —*See also (CS_e 1.a) and (CS_e 1.b) with regard to the power plant sending plant status.* (CS_e 2.b) NPP staff does not know how to deal with the emergency. (CS_e 2.c) NPP staff reports the emergency, but it is not communicated either to NRA or to local bodies properly, because of damage to—or aged deterioration of—transmission circuits, for instance.
SR_e: Possible safety requirements (1/2)
(SR_e 2.a) The signal of emergency must be easily recognized and unequivocal, but must not be generated when it is not an emergency. NPP staff must be capable of correctly identifying the state of emergency. —*See also (SR_e 1.a) and (SR_e 1.b) with regard to the power plant sending plant status.* (SR_e 2.b) Head office must provide effective training for NPP staff periodically and must ensure each staff member has a clear understanding of what to do and how to do so in case of an emergency. (SR_e 2.c) NPP staff must ensure that the reports of emergency are accurately and unambiguously communicated both to NRA and to local bodies at any condition.
UCA_e: Unsafe control actions (2/2)

(UCA_e 3-1) NPP staff fails to manage the accident properly.

(UCA_e 3-2) An erroneous action by NPP staff exacerbates the accident.

(UCA_e 3-3) NPP staff responds to the accident too late.

(UCA_e 3-4) NPP staff stops managing the accident when it is not solved.

CS_e: Causal scenarios leading to UCAs (2/2)

(CS_e 3.a) NPP staff does not recognize the signal of emergency. Otherwise, they misunderstand the signal, or erroneously believe that it is a false alarm or not safety-critical. —*Same as (CS_e 2.a) above.*

(CS_e 3.b) NPP staff does not know how to deal with the emergency, or fails to do so owing to human resource constraints. Otherwise, NPP staff misunderstands the emergency, or erroneously believes no (immediate/further) control actions should be provided. —*See also (CS_p 2.b) with regard to NPP staff operating the power plant in peacetime.*

(CS_e 3.c) NPP staff inadvertently takes an erroneous control action owing to button confusion or mode confusion. —*Same as (CS_p 2.c) in peacetime.*

(CS_e 3.d) NPP staff chooses correct control actions, but they are not properly processed in a timely manner, because of damage to—or aged deterioration of—transmission circuits, for instance. —*See also (CS_p 2.d) with regard to NPP staff operating the power plant in peacetime.*

SR_e: Possible safety requirements (2/2)

(SR_e 3.a) The signal of emergency must be easily recognized and unequivocal, but must not be generated when it is not an emergency. NPP staff must be capable of correctly identifying the state of emergency. —*Same as (SR_e 2.a) above.*

(SR_e 3.b) NPP staff must be provided with enough resources and sufficiently trained to deal with any kind of emergencies, and must be motivated always to make safer choices. Feedback on control actions must be accurately and continuously gathered from the power plant in a timely manner. —*See also (SR_p 2.b) with regard to NPP staff operating the power plant in peacetime.*

(SR_e 3.c) Button arrangement and operation mode must be simple and intuitive enough (*i.e.* not too complicated) to avoid confusion, and any input—if *and* only if it is potentially hazardous—must be double-checked. —*Same as (SR_p 2.c) in peacetime.*

(CS_e 3.d) NPP staff must periodically check safety features so that they work properly in a timely manner at any condition. —*Same as (SR_p 2.d) in peacetime.*

Table 3-11: UCAs of the Head Office in an Emergency, Causal Scenarios and Safety Requirements

UCA_e: Unsafe control actions
(UCA_e 4-1) Head office fails to support NPP staff to mitigate the accident. (UCA_e 4-2) Head office supports NPP staff erroneously and the staff exacerbates the accident. (UCA_e 4-3) Head office supports NPP staff too late to mitigate the accident. (UCA_e 4-4) Head office stops supporting NPP staff when they need assistance.
CS_e: Causal scenarios leading to UCAs
(CS_e 4.a) The plant status is not transmitted to the head office. —*See also (CS_e 1.a) and (CS_e 1.b) with regard to the power plant sending plant status.* (CS_e 4.b) Head office does not know how to deal with the emergency, or fails to do so owing to human resource constraints. Otherwise, head office misunderstands the emergency, or erroneously believes that NPP staff provided appropriate control actions when they actually did not. (CS_e 4.c) Head office chooses right actions to support NPP staff, but they are not properly communicated to NPP staff in a timely manner, because of damage to—or aged deterioration of—transmission circuits, for instance.
SR_e: Possible safety requirements
(SR_e 4.a) Head office must ensure (*e.g.* on the occasion of periodical drills) that the plant status is transmitted properly in a timely manner at any condition. —*See also (SR_e 1.a) and (SR_e 1.b) with regard to the power plant sending plant status.* (SR_e 4.b) Head office must maintain enough resources to correctly understand the state of emergency and continuously support NPP staff in a timely manner. Feedback on control actions must be accurately and continuously gathered both from the power plant and from the NPP staff in a timely manner. (SR_e 4.c) Head office must ensure that accurate and unambiguous communication to NPP staff takes place in a timely manner at any condition.

Table 3-12: UCAs of NRA, CAO and local bodies in an Emergency, Causal Scenarios and Safety Requirements

UCA_e: Unsafe control actions (1/3)
(UCA_e 5-1) NRA fails to provide advice to power company. (UCA_e 5-2) NRA provides wrong advice to power company and the company exacerbates the accident. (UCA_e 5-3) NRA provides advice to power company too late. (UCA_e 5-4) NRA stops providing advice to power company when it needs assistance.
CS_e: Causal scenarios leading to UCAs (1/3)
(CS_e 5.a) Off-site Center does not provide enough information on plant status for NRA in a timely manner. *—See also (CS_e 8.a) through (CS_e 8.c) with regard to the Off-site Center sending information.* (CS_e 5.b) NRA does not know how to deal with the emergency, or fails to do so owing to human resource constraints. Otherwise, NRA misunderstands the emergency, or erroneously believes that the power company provided appropriate control actions when it actually did not. (CS_e 5.c) NRA devises right advice to support the power company, but it is not properly communicated to the power company in a timely manner, because of damage to—or aged deterioration of—transmission circuits, for instance.
SR_e: Possible safety requirements (1/3)
(SR_e 5.a) Off-site Center must be capable of sending enough information on plant status to NRA in a timely manner at any time. *—See also (SR_e 8.a) through (SR_e 8.c) with regard to the Off-site Center sending information.* (SR_e 5.b) NRA must maintain enough resources to correctly understand the state of emergency and continuously support the power company in a timely manner. Feedback on control actions must be accurately and continuously gathered both from the Off-site Center and from the power company in a timely manner. (SR_e 5.c) NRA must ensure that accurate and unambiguous communication to the power company takes place in a timely manner at any condition.
UCA_e: Unsafe control actions (2/3)

(UCA_e 6-1) NRA or CAO fails to provide advice to PM Office.

(UCA_e 6-2) NRA or CAO provides wrong advice and PM Office exacerbates the accident.

(UCA_e 6-3) NRA or CAO provides advice to PM Office too late.

(UCA_e 6-4) NRA or CAO stops providing advice to PM Office when it needs assistance.

CS_e: Causal scenarios leading to UCAs (2/3)

(CS_e 6.a) Off-site Center does not provide enough information on plant status for NRA—or NRA does not communicate it to CAO—in a timely manner. *—See also (CS_e 8.a) through (CS_e 8.c) with regard to the Off-site Center sending information.*

(CS_e 6.b) NRA or CAO does not know how to deal with the emergency, or fails to do so owing to human resource constraints. Otherwise, NRA or CAO misunderstands the emergency, or erroneously believes that PM Office does not need—or no longer needs—assistance from both organizations when it actually does.

(CS_e 6.c) NRA or CAO devises right advice to support PM Office, but it is not properly communicated to PM Office in a timely manner.

(CS_e 6.d) There is a gray zone that neither NRA nor CAO is mandated to take care of, or they provide conflicting advice to PM Office.

SR_e: Possible safety requirements (2/3)

(SR_e 6.a) The Off-site Center must be capable of continuously sending enough information on plant status for NRA—and NRA must communicate it to CAO—in a timely manner at any time. *—See also (SR_e 8.a) through (SR_e 8.c) with regard to the Off-site Center sending information.*

(SR_e 6.b) NRA and CAO must maintain enough resources to correctly understand the state of emergency and continuously support PM Office in a timely manner. Feedback on control actions must be accurately and continuously gathered from PM Office in a timely manner.

(SR_e 6.c) NRA and CAO must ensure that accurate and unambiguous communication to PM Office takes place in a timely manner at any time.

(SR_e 6.d) The demarcation between NRA and CAO must be clearly defined, and they must work closely with each other to eliminate conflicting advice to PM Office.

UCA_e: Unsafe control actions (3/3)

(UCA_e 7-1) NRA or local bodies fail to dispatch personnel to Off-site Center. (UCA_e 7-2) NRA or local bodies dispatch personnel to Off-site Center too late. (UCA_e 7-3) NRA or local bodies stop dispatching personnel when emergency continues.
CS_e: Causal scenarios leading to UCAs (3/3)
(CS_e 7.a) NRA or local bodies do not recognize the report of emergency from NPP staff. —*See also (CS_e 2.a) through (CS_e 2.c) with regard to NPP staff reporting the emergency.* (CS_e 7.b) NRA or local bodies do not know that they must dispatch personnel to Off-site Center when they receive the report of emergency, or fail to do so owing to human resource constraints. (CS_e 7.c) NRA and local bodies plan to dispatch personnel to Off-site Center, but the group from either side (or both sides) cannot reach the Off-site Center because of some obstacle such as traffic suspension.
SR_e: Possible safety requirements (3/3)
(SR_e 7.a) NRA and local bodies must make sure that a report from NPP staff can be received at any time. —*See also (SR_e 2.a) through (SR_e 2.c) with regard to NPP staff reporting the emergency.* (SR_e 7.b) NRA and local bodies must maintain enough resources to correctly understand the state of emergency and dispatch predetermined personnel to the Off-site Center without delay. (SR_e 7.c) NRA and local bodies must identify every possible obstacle that might hamper their dispatch to Off-site Centers, and must eliminate these obstacles as much as possible.

Table 3-13: UCAs of the Off-site Center in an Emergency, Causal Scenarios and Safety Requirements

UCA_e: Unsafe control actions
(UCA_e 8-1) Off-site Center fails to send information to NRA or local bodies. (UCA_e 8-2) Off-site Center sends incorrect information to NRA or local bodies. (UCA_e 8-3) Off-site Center sends information to NRA or local bodies too late. (UCA_e 8-4) Off-site Center stops sending information when NRA and/or local bodies need it.
CS_e: Causal scenarios leading to UCAs

(CS_e 8.a) The plant status is not transmitted to the Off-site Center. *—See also (CS_e 1.a) and (CS_e 1.b) with regard to the power plant sending plant status.* (CS_e 8.b) The personnel dispatched to the Off-site Center do not know how to deal with the emergency. Otherwise, they misunderstand the plant status, or erroneously believe that some information need not be sent to NRA or local bodies (immediately/anymore). (CS_e 8.c) The personnel dispatched to the Off-site Center try to send information to NRA or local bodies, but the information is not properly communicated to NRA or local bodies in a timely manner, because of damage to—or aged deterioration of—transmission circuits, for instance. *—See also (CS_p 6.a) through (CS_p 6.c) with regard to NRA preparing Off-site Center in peacetime.*
SR_e: Possible safety requirements
(SR_e 8.a) NRA, in cooperation with power companies, must ensure (*e.g.* on the occasion of periodical drills) that the plant status is transmitted properly to Off-site Centers in a timely manner at any condition. *—See also (SR_e 1.a) and (SR_e 1.b) with regard to the power plant sending plant status.* (SR_e 8.b) Personnel predetermined for dispatch to Off-site Centers must develop and maintain capability to correctly understand the state of emergency and send sufficient information to NRA and local bodies in a timely manner. (SR_e 8.c) NRA and local bodies must ensure that personnel dispatched to Off-site Centers communicate the information to them accurately and unambiguously in a timely manner at any condition. *—See also (SR_p 6.a) through (SR_p 6.c) with regard to NRA preparing Off-site Center in peacetime*

Table 3-14: UCAs of PM Office in an Emergency, Causal Scenarios and Safety Requirements

UCA_e: Unsafe control actions
(UCA_e 9-1) PM Office fails to provide information or to order evacuation. (UCA_e 9-2) PM Office provides wrong information that endangers residents. (UCA_e 9-3) PM Office provides information or orders evacuation too late.
CS_e: Causal scenarios leading to UCAs

(CS_e 9.a) NRA does not provide sufficient or accurate information on plant status for PM Office in a timely manner. Otherwise, CAO does not provide enough support for off-site emergency response for PM Office in a timely manner. *—See also (CS_e 6.a) through (CS_e 6.d) with regard to NRA and CAO providing advice.* (CS_e 9.b) PM Office does not know how to deal with the emergency. Otherwise, it misunderstands the plant status, or erroneously believes that immediate actions for evacuation are unnecessary. (CS_e 9.c) PM Office announces an evacuation order, but it is not properly communicated to the local bodies, because of damage to—or aged deterioration of—transmission circuits, for instance.
SR_e: Possible safety requirements
(SR_e 9.a) NRA and CAO must maintain enough resources to continuously support PM Office in a timely manner at any time. *—See also (SR_e 6.a) through (SR_e 6.d) with regard to NRA and CAO providing advice.* (SR_e 9.b) PM Office must maintain enough resources to correctly understand the state of emergency and to provide information/order evacuation in a timely manner. Feedback on control actions must be accurately and continuously gathered from local bodies in a timely manner. (SR_e 9.c) PM Office must ensure that accurate and unambiguous communication to local bodies takes place in a timely manner at any condition.

Table 3-15: UCAs of Local Bodies in an Emergency, Causal Scenarios and Safety Requirements

UCA_e: Unsafe control actions
(UCA_e 10-1) Local bodies fail to protect residents. (UCA_e 10-2) Local bodies protect residents too late. (UCA_e 10-3) Local bodies stop protecting residents when they need help.
CS_e: Causal scenarios leading to UCAs
(CS_e 10.a) Local bodies do not recognize the report of emergency from NPP staff, or the evacuation order announced by PM Office. *—See also (CS_e 2.a) through (CS_e 2.c) with regard to NPP staff reporting the emergency, and (CS_e 9.a) through (CS_e 9.c) with regard to PM Office providing*

information or ordering evacuation. (CS_e 10.b) Local bodies do not know how to deal with the emergency, or fail to do so owing to human resource constraints. Otherwise, they misunderstand the emergency, or erroneously believe that residents do not—or no longer—need protection when they actually need help. *—See also (CS_p 8.a) through (CS_p 8.c) with regard to CAO supporting the planning by local bodies in peacetime.* (CS_e 10.c) Local bodies take protective measures such as an evacuation ordered by PM Office, but it is not properly communicated to residents in a timely manner, because of damage to—or aged deterioration of—transmission circuits, for instance.
SR_e: Possible safety requirements
(SR_e 10.a) Local bodies must make sure that both a report from NPP staff and an evacuation order from PM Office can be received at any time. *—See also (SR_e 2.a) through (SR_e 2.c) with regard to NPP staff reporting the emergency, and (SR_e 9.a) through (SR_e 9.c) with regard to PM Office providing information or ordering evacuation.* (SR_e 10.b) Local bodies must maintain enough resources to correctly understand the state of emergency and to protect residents in a timely manner. Feedback on control actions must be accurately and continuously gathered from residents in a timely manner. *—See also (SR_p 8.a) through (SR_p 8.c) with regard to CAO supporting the planning by local bodies in peacetime.* (SR_e 10.c) Local bodies must ensure that accurate and unambiguous communication to residents takes place in a timely manner at any condition.

3.5 Summary and Findings

As has been discussed in this chapter, the STPA process revealed a number of unsafe control actions in the control structure for the safety of nuclear power plants in Japan after the Fukushima Daiichi nuclear disaster, the causal scenarios by which these unsafe control actions could occur, and possible safety requirements to prevent these causal scenarios. Although this analysis may not be precise enough for each stakeholder to use in practice, partly because there could be more potentially hazardous control actions especially within the physical process (*i.e.* power plants) and within each organization, the analysis using

this simple methodology can be easily extended from the whole picture to more specific, technical or intra-organizational control loops.

Notably, although the stakeholders have made efforts to improve the safety control structure as discussed in Section 3.1, the STPA process demonstrated that the "Safety Myth" (*i.e.* overconfidence in safety) or administrative issues, both of which were described as important causal factors in Chapter 2, might still come into play as causal factors, such as "(CS_p 3.b) Head office erroneously believes that such safety features are unnecessary or have no urgency" and "(CS_e 6.d) There is a gray zone that neither NRA nor CAO is mandated to take care of, or they provide conflicting advice to PM Office."

At the same time, it was also revealed that investment for safety and sound safety culture can be possible safety requirements that subdue these causal factors, such as adding safety features to nuclear power plants and maintaining resources, as well as NPP staff being motivated always to make safer choices. Nevertheless, given that safety culture, in particular, is intangible in nature and is not easy to establish or maintain in practice, control loops to complement it (*e.g.* enabling NPP staff to make allegations to NRA against the management) should be created, as discussed in the last chapter.

Reviews of the safety control structure, including the evaluation of policy and the implementation of emergency preparedness drills, must be performed in terms of whether each stakeholder satisfies its safety requirements, and how effective the control structure is to eliminate the unsafe scenarios. Some of these safety requirements are crucial for effective emergency response, and must be met even when a severe, compound nuclear disaster should occur—*i.e.* when, as was the case in the Fukushima Daiichi nuclear disaster discussed in the previous chapter, disruptions in communication and transportation networks may occur and a large number of personnel in the national and local governments may be tied up with their response to the natural disasters.

3.6 References

[1] Leveson, N. (2012). “Engineering a safer world: systems thinking applied to safety”. Engineering systems. Cambridge, Massachusetts: MIT Press.

[2] TEPCO’s Efforts towards Nuclear Reform (n.d.). Retrieved December 10, 2015, from http://www.tepco.co.jp/en/nu_reform/index-e.html

[3] Nuclear Reform Monitoring Committee (n.d.). Retrieved December 10, 2015, from http://www.nrmc.jp/en/index-e.html

[4] Tokyo Electric Power Company, Inc. (2013), “Fukushima Nuclear Accident Summary & Nuclear Safety Reform Plan,” available at: http://www.tepco.co.jp/en/press/corp-com/release/betu13_e/images/130329e0801.pdf

[5] Kansai Electric Power Company, Inc. (2014), “Commitment to Enhancing Nuclear Safety,” available at: http://www.kepco.co.jp/english/corporate/pr/2014/__icsFiles/afieldfile/2014/09/18/2014_aug_1.pdf

[6] Basic Policy on the Reform of an Organization in charge of Nuclear Safety Regulation (Cabinet Decision, August 15, 2011), available at: https://www.nsr.go.jp/data/000099639.pdf

[7] Nuclear Regulation Authority (n.d.). Retrieved January 5, 2016, from https://www.nsr.go.jp/english/index.html

[8] International Atomic Energy Agency (n.d.), “IAEA Mission Says Japan’s Regulatory Body Made Fast Progress, Sees Challenges Ahead”. Retrieved January 22, 2016, from https://www.iaea.org/newscenter/pressreleases/iaea-mission-says-japan%E2%80%99s-regulatory-body-made-fast-progress-sees-challenges-ahead

[9] Nuclear Regulation Authority (2013), “Enforcement of the New Regulatory Requirements for Commercial Nuclear Power Reactors,” available at: http://www.nsr.go.jp/data/000067212.pdf

Chapter 4. Conclusion

This thesis analyzed, in the social and inter-organizational context, why the stakeholders could not prevent the Fukushima Daiichi nuclear disaster (Chapter 2), and what the potentially hazardous control actions could be with regard to the future nuclear safety in Japan (Chapter 3).

To achieve these purposes, STAMP methodologies—CAST and STPA—were applied; the overall safety control structures were visualized based on the responsibility of each stakeholder and the interactions between them, and the (potential) flaws and causal factors in those control structures were either identified or estimated.

These findings, as summarized below, could ultimately be used by the stakeholders to identify their safety requirements that would improve and maintain the efficacy of the present safety control structure.

4.1 Overall Summary

In Chapter 2, the CAST process revealed that virtually all the stakeholders involved in the Fukushima Daiichi Nuclear Power Plant made inadequate or unplanned control actions regarding the safety design, safety management and emergency response, which, in combination, contributed to the accident.

This lack of preparedness against severe accidents or compound nuclear disasters resulted from several causal factors, such as a complacent assumption called the “Safety Myth,” misconceptions about “defense-in-depth” and reluctance by local bodies to change their disaster prevention plans. The “Safety Myth,” in particular, had been strengthened over time by the micromanagement of hardware, and underlying this dynamic had been the risk of lawsuits and the administrative issues of the nuclear operator and the national government, such as lack of leadership on nuclear safety, flawed safety culture, lack of

resources at the regulatory bodies and bureaucracy.

In Chapter 3, the STPA process revealed unsafe control actions that could occur in the current safety control structure, and the causal factors, that is, how these unsafe control actions might be triggered.

It is certain that, at least apparently, the causal factors of the Fukushima Daiichi nuclear disaster have been mitigated thanks to the post-accident improvements of the safety control structure made by the stakeholders; for instance, the establishment of a new regulatory body, assuming most of the roles and responsibilities of nuclear safety that were formerly shared among several governmental organizations, has dramatically reduced the administrative complexity within the national government. Nevertheless, these causal factors have not disappeared; overconfidence in safety may affect the mental models of the stakeholders and make them erroneously believe that some safety measures are unnecessary or have no urgency, or administrative issues may hamper smooth communication and coordination between them. It was also shown at the same time that investment for safety and sound safety culture count as safety requirements by which the stakeholders can keep these causal factors under control.

4.2 Recommendations

Based on the findings above, several recommendations to strengthen the current safety control structure were developed for some key stakeholders, as shown below.

4.2.1 Nuclear operators

It is extremely important for each power company to establish its safety culture, so that the staff feels comfortable to raise concerns and the management (head office) constantly updates their mental models

on both the plant status and the skill of their staff. Such safety culture should be effectively institutionalized and maintained in close cooperation between the staff and the management.

Although it is beyond the scope of this thesis to discuss how to create sound safety culture, lessons from the Fukushima Daiichi nuclear disaster should be thoroughly shared as a firm basis for all the nuclear operators, and preservation of the remnants of the accident should be considered for educational purposes.

With the domestic power market fully liberalized in April 2016, and given that some of the aging nuclear reactors may cease operation in the near future, it might be possible that the nuclear operators will cancel or postpone some of the investments essential for nuclear safety in favor of cutting costs, which may also cause the retreat of their safety culture. To counter that risk, the operators should consider having experts or other third parties monitor whether they maintain effective safety features and safety culture, and the signs of dysfunctional safety culture—especially the "culture of denial" and the "paperwork culture," as discussed in Chapter 2—must be detected and addressed immediately.

4.2.2 Nuclear Regulation Authority

The Nuclear Regulation Authority (NRA) should play a pivotal role always to ensure through the regulations that the whole safety control structure—not only the control loops it is directly involved in—functions and would function against the worst scenarios possible. Inspections, periodic reviews of the safety management system and emergency preparedness drills should be designed so that NRA can fulfill that role, and performance metrics should be developed to objectively measure and evaluate the soundness of the safety control structure.

Specifically in regulating the nuclear operators, NRA should establish criteria to assess the safety culture of the power companies, which would be similar to the nine "traits of a positive safety culture" described

in the Safety Culture Policy Statement[5] of Nuclear Regulatory Commission (NRC) of the United States.

Furthermore, NRA should create and maintain a "bypassing" or "backup" loop between NRA and the power company staff, by which the staff can make allegations anonymously when the management is not ready to hear their voices.

4.2.3 Cabinet Office

As described in Chapter 3, the Cabinet Office (CAO) now takes charge of the response to nuclear disasters in addition to other types of disasters. CAO should publish the principles on how to prepare for and respond to compound nuclear disasters as well as severe accidents, so that local bodies can plan their own response to protect their residents should such worst-case scenarios occur.

CAO should then ensure that these preparedness and response plans are incorporated in their Regional Disaster Prevention Plans, and should continuously check through emergency preparedness drills whether the local bodies are capable of responding as planned—and whether CAO itself can coordinate smoothly with NRA in supporting the Prime Minister's Office—even in a compound nuclear disaster and/or a severe accident.

4.2.4 Scientists and IAEA

Because of the technical and social complexity with regard to the nuclear safety, scientists and the International Atomic Energy Agency (IAEA) should be given a mandate to make advice and

[5] US Nuclear Regulatory Commission (NRC) (2011, Tuesday June 14). Final Safety Culture Policy Statement. *Federal Register*, Vol. 76, No. 114, 34773-34778. The traits of a positive safety culture include "Leadership Safety Values and Actions," "Continuous Learning," "Environment for Raising Concerns," "Questioning Attitude," etc.

recommendations as a "watchdog over nuclear safety," when appropriate, to make sure that risks (*i.e.* the causal scenarios) as well as safety requirements are well understood by the stakeholders in considering the safety design, safety management and emergency response, and that and key safety principles such as "defense-in-depth" are properly embedded in the safety control structure.

The nuclear operators and the government not only should create and maintain communication channels to exchange opinions with scientists and IAEA, but also should work together with them—but should not collude with them—in solving their problems.

4.3 Future Works

This thesis put an emphasis on safety management (*i.e.* system operation) and emergency response, and revealed in most part the risks between different organizations, except for the power companies where it focused on the head office, staff, and the power plant, respectively.

The CAST analysis could be expanded, provided that there's sufficient information, into the details of the system design and development process inside General Electric with regard to the Fukushima Daiichi Nuclear Power Plant, to answer the questions such as why the design team provided the system design that would prove to be unsafe, and whether the safety requirements set by the project management were appropriate.

The STPA process could be applicable to the analysis of the risks inside each organization. For instance, NRA itself consists of one chairperson and four commissioners, and its Secretariat comprises government officials, as discussed in Chapter 3. It will be useful to focus on the control structure within NRA in order to identify the causal scenarios that could dampen effective controls by commissioners over the Secretariat, or even those inside the Secretariat.

Finally, the use of STPA is not necessarily limited to the analysis of nuclear safety; the process could also be expanded to discuss nuclear security issues such as counterterrorism efforts.