APPLICATION OF SYSTEM SAFETY FRAMEWORK IN HYBRID SOCIO-TECHNICAL ENVIRONMENT OF EURASIA

by

Azamat Abdymomunov

Bachelor of Arts in History, Political Science,
Indiana University, 1997

Diploma, International Relations,
Kazakh State University, 1997

Master in Public Policy, Kennedy School of Government,
Harvard University, 1999

SUBMITTED TO THE SYSTEM DESIGN AND MANAGEMENT PROGRAM
IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE IN ENGINEERING AND MANAGEMENT
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

April 15, 2011

Signature of Author: _____

Azamat Abdymomunov
System Design and Management Program
April 15, 2011

Certified by: _____

Nancy Leveson
Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Supervisor

Accepted by: _____

Patrick Hale
Director, System Design and Management Fellows Program

This Page Intentionally Left Blank

APPLICATION OF SYSTEM SAFETY FRAMEWORK IN HYBRID SOCIO-TECHNICAL ENVIRONMENT OF EURASIA

by
Azamat Abdymomunov

Submitted to the System Design and Management Program
on April 15, 2011

in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

Abstract

The political transformation and transition of post-Soviet societies have led to hybrid structures in political, economic and technological domains. In such hybrid structures the roles of government, state enterprise, private business and civil society are not clearly defined. These roles shift depending on formal and informal interests, availability and competition for limited resources, direct and indirect financial benefits, internal and external agendas.

In an abstract sense, a hybrid is "anything derived from heterogeneous sources, or composed of elements of different or incongruous kinds" (Hybrid). If transition is a process from one state to another, *hybrid* is a state unto itself. In the context of this thesis *Hybrid Socio-Technical Environment* means the co-existence of different institutions and policies, state and private business entities, old and new technologies, managerial models and practices of planning and market economies, collectivist and individualist value systems.

Rapid technological progress, coupled with shifts in political and economic structures, may produce long-lasting disturbances in a society. Such disturbances are result of the hybrid society's contradictory nature. Some of these disturbances appear in the form of large-scale systemic accidents, such as the Sayano-Shushenskaya Hydroelectric Power Station accident.

The rigid and outdated Soviet socio-technical system was broken down into multiple independent systems and subsystems to increase operational flexibility, with very limited capital investment. A twenty-year transition period (1990-2010), proved the survivability of the Soviet system, which was able to perform its primary functions even with partial capacity.

However, recent large-scale accidents are clear signs that the system is stretching beyond its limits. Changes in the socio-technical landscape (multiple stakeholders and variety of interests) suggest that the traditional approaches of Reliability Theory, with its inward focus, may not be an effective tool in identifying emerging challenges. The outward-focused

System theory approach takes into consideration key characteristics of the changing hybrid socio-technical landscape, as well as motivations of multiple stakeholders.

The research concludes that insufficient capital investment and backlog in maintenance shifts are key systemic factors that allow migration of organizational behavior from a safe to an unsafe state. Additional analysis has to be conducted to prove this conclusion.

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

Acknowledgements

> *"… the excellent teacher is the source of all temporary happiness and certain goodness, beginning with the production of a single good quality and the reduction of a single fault in a student's mind and eventually encompassing all the knowledge beyond that" (Tsong-Kha-Pa).*

I would like to thank Professor Nancy Leveson, my thesis advisor, who changed my view of the world in ways far beyond the topic of this thesis. I am equally appreciative for both the life lessons that she has given me and for sharing draft chapters of her new book, which has guided me through each step of this a yearlong journey.

I would like to thank three most important persons in my life – my daughter Malika, who is my inspiration; my wife Leyla who is my life; and my mother Saule, who is my faith. Your unconditional love is the only thing that helps me achieve these heights. I am grateful to my father Kurmanbek, my sons Dinmohamed and Daniyar, and my brother Nurzhan. I will do everything to make you proud of me.

I would like to thank Fiona Hill of the Brookings Institute for being my friend and for encouraging me to take this journey.

I would like to thank Pat Hale, Director of System Design and Management Fellows Program at MIT for believing in me and making me part of the MIT community.

Last but not least, I am grateful to my classmates System Design and Management Fellows of 2009 and 2010 for most interesting and vibrant year in my life.

This Page Intentionally Left Blank

Table of Contents

List of Abbreviations

BrkHPS	Bratsk Hydroelectric Power Station
CGS	Corporate Governance Score
FASPM	Federal Agency for State Property Management (*Rosimuschestvo*)
FAS	Federal Antimonopoly Agency
FSETAI	Federal Service for Environment, Technological and Atomic Inspection (*Rostekhnadzor*)
GRARM	Group Regulator for Active and Reactive Powers
GW	Gigawatt(s)
GWh	Gigawatt-hour(s)
HPS	Hydroelectric Power Station
KPI	Key Performance Indicators
kWh	Kilowatt-hour(s)
MIT	Massachusetts Institute of Technology
MW	Megawatt(s)
PMPCS	Power Management and Process Control System
RAO UES	Russian Joint-Stock Company United Energy System of Russia, or RAO UES of Russia
SDM	System Design and Management
SREGS	Siberian Regional Energy Grid System
SSHPS	Sayano-Shushenskaya Hydroelectric Power Station
STAMP	Systems-Theoretic Accident Model and Process
SUGSD	Siberian Unified Grid System Dispatch
UES	same as RAO UES
UI HPS	Ust Ilimsk Hydroelectric Power Station

List of Figures

This Page Intentionally Left Blank

Chapter 1. Introduction

"Ultimate truth and the consciousness perceiving it are like water put in water, indifferentiable" (Dalai Lama).

1.1 Motivation

Over the last three decades the world has experienced dramatic technological transformation. Speed and abundance of information; complexity of decision-making systems; dissemination of knowledge and instant access to new and low- cost technologies; mobility of capital, labor and ideas are changing the world around us. Such changes are even more obvious in the developing world.

Technological shift is also visible in the post-Soviet landscape. Here, however, technological progress has been coupled with a shift in the political system. Such coupling has created long-lasting disturbances in society, where the borders of responsibility between government, private sector and civil society are still in the process of transitional formation and not clearly defined. The political transformation and transition of post-Soviet societies have led to hybrid structures in political, economic and technological domains.

In an abstract sense, a hybrid is "anything derived from heterogeneous sources, or composed of elements of different or incongruous kinds" (Hybrid). If transition is a process from one state to another, *hybrid* is a state unto itself. In the context of this thesis *Hybrid Socio-Technical Environment* means co-existence of different institutions and policies, state and private business entities, old and new technologies, managerial models and practices of planning and market economies, collectivist and individualist value systems.

Rapid technological progress, coupled with shifts in political and economic structures, may produce long-lasting disturbances in a society. Such disturbances are the result of the hybrid society's contradictory nature. Some of these disturbances could be in the form of large-scale systemic accidents, such as the Sayano-Shushenskaya Hydroelectric Power Station accident.

The goal of this thesis is to explain such hybrid characteristics through a vital sector of a planned economy – the electricity sector - using the particular example of the Sayano-Shushenskaya Hydroelectric Power Station accident.

Twenty years after splintering into fifteen national entities, the Soviet industrial infrastructure is facing physical decay and the constant challenge of the market economy. The rigid and outdated Soviet socio-technical system was broken into multiple independent systems and subsystems to increase operational flexibility, with very limited capital investment.

Until recently the electricity generation sector, prioritized by communist ideology and a lynchpin of the Soviet political economy, remained a reliable industry. Despite mounting challenges, the governments of Eurasia continue to rely on this sector for rapid economic recovery by keeping electricity costs for national industries below market price.

> "On September 17, 2009 an accident shut down the Sayano-Shushenskaya Hydroelectric Power Station, Russia's single largest power facility, with an installed capacity of 6,721 megawatts (MW), which typically produces about 24.5 billion kilowatt-hours (kWh) of electricity annually. This represents about 2.4 percent of Russia's total electricity production and about 3 percent of Russia's installed generating capacity. The facility generated about 11–12 percent of the power supplied to the Siberian integrated regional grid system, which stretches from east to west about 3,000 km, from the Russian-Chinese border east of Lake Baikal to the oil-producing area of West Siberia "(Sagers, Freedenberg, & Mahnovski, 2009).
>
> "Turbine 2, the oldest among 10 turbines at the Sayano-Shushenskaya Hydro Power Station (SSHPS), was ripped from its seating at 8:13 am on August 17, 2009. Within seconds, a deluge of water began flooding the facility's turbine hall and engine rooms, causing a transformer explosion and short circuiting, crippling the plant's electrical systems as well as causing devastating structural damage. Fortunately the hydro plant's 245.5m-tall arch gravity dam was not breached. Management failures and technical shortcomings were blamed the disaster, in which 75 people died" (Fleming, 2009).

SSHPS is the largest power plant in Russia and the sixth-largest hydro station in the world. It produced 15% of Siberia's and 2% of Russia's total generation, with generation capacity of 6.4GW. SSHPS is part of the Yenisei hydro cascade. Within the Siberian Energy System the station is the major source for stabilizing peak power fluctuation.

Construction of the station started in 1968 and ended, after significant delay, in 1988. Prior to this accident, the SSHPS had experienced three major accidents - all related to seasonal floods - in 1979, 1985, 1988. Construction of the Shore spillway, originally postponed due to lack of funds, began in 2005 and was completed one year after the accident, in September 2010 (RusHydro, September 28, 2010).

SSHPS's parent company RusHydro's market capitalization was $10 billion as of July 2009. At the end of that year total installed hydropower capacity was 25,336.6 MW. It has 50 hydro plants, including the largest - the SSHPS. In 2008 the company generated 80,273 GWh of electricity (International Water Power and Dam Construction, 2009). RusHydro is a state-controlled power generation holding with 60.37% (RusHydro, 2010) ownership of the Federal Agency for State Property Management (*Rosimuschestvo*). Minority stakes are in the hands of Russia's aluminum producing conglomerate, RUSAL.

The magnitude of the accident and the symbolism of this particular power station as a premier Soviet industrial accomplishment present a rare opportunity for reconsidering

existing mental models of safety and creating an awareness that "accidents are complex processes involving the entire socio-technical system" (Leveson, 2009).

1.2 Hypothesis and Objectives

The hypothesis of this thesis can be summarized in the three following paragraphs:

> In hybrid socio-technical landscape the roles of government, state enterprise, private business and civil society are not clearly defined. Their roles fluctuate depending on formal and informal interests, availability and competition for limited resources, direct and indirect financial benefits, and internal and external agendas.
>
> After the fall of The Soviet Union its rigid and outdated socio-technical system was broken down into multiple independent systems and subsystems to increase operational flexibility, with very limited capital investment. A twenty-year transition period (1990-2010) demonstrated the durability and survivability of the Soviet system, which continued to perform its primary functions even at partial capacity. "Failures of some or a majority of system components lead only to gradual degradation of the system's ability to perform its functions/operations" (Ushakov, 2000).
>
> However, recent large-scale accidents are clear signs that the system is reaching its limits. Changes in the socio-technical landscape (multiple stakeholders and variety of interests) suggest that traditional approaches of the Reliability theory, with its inward focus, may not be an effective tool to identify emerging challenges. The outward System theory approach takes into consideration key characteristics of the changing hybrid socio-technical landscape, as well as the motivations of multiple stakeholders.

The objective of this thesis is to bring clarity to three different domains: (1) mental models, (2) the powerlessness of management, and (3) the sustainability of infrastructure.

Structure of mental models dictates our behavior and language and constrains how we construct reality

By structure I mean first and foremost the structure of mental models of decision makers. In the post-Soviet society *a system* is associated with a hierarchical structure with an individual being at the very bottom of the hierarchy, whereas *the system* typically implies a political system or political regime.

Personal inability to resist the political system has left the legacy of old mindsets in which people subconsciously focus attention on particular individuals (heroes or villains) rather than systemic problems. The old Stalinist saying "replace the person, solve the problem" (*net cheloveka, net problemy*) suggests that the easiest and most frequently used explanation in accident investigations is human error.

In addition, language presents another barrier in presenting the System Theory and System Safety approach. As Dekker states, *our language constrains how we construct reality*. I will address this issue in more detail in Chapter 2. But, as a brief example, let's look at several translation dilemmas:

The word *safety (bezopasnost')* has dual translation in the Russian language as both security and safety. Thus *Public safety* (*obschestvennaya bezopasnost'*) is often translated and understood as domestic or internal security. The closest translation to *System safety* is probably *safety/security of the system* (*bezopasnost' systemy*), which also has a self-protective security connotation.

Even in narrow technical language *security of technology* (*technicheskaya bezopasnost'*) is often associated with security from outside threats and factors. The term *industrial security/safety* (*promyshlennaya bezopasnost'*) is referred to physical processes within an industrial site, whereas *reliability (nadyozhnost')* refers to internal characteristics of a system.

Just this small example suggests that there must be a considerable gap between the individual and a system in which the individual is estranged from the system and the role of each individual is limited. What could be safe for *the system* may not necessarily be safe for individual and vice versa. The safety of the individual is not connected to the safety/security or reliability of *the system.*

The powerlessness of management to react to emerging unsafe situations is one of the key factors in systematic migration of organizational behavior

This thesis employs three major sources of information: (1) the report of the official investigation conducted by the Federal Service for Environment, Technological and Atomic Inspection (FSETAI) (Rostekhnadzor, 2009) and Russia's Ministry for Emergency immediately after the accident, (2) the official parliamentary report (Council of Federation, 2009a) and (3) special opinions of 45 experts, attached to the Parliamentary Report (Council of Federation, 2009b), which may not reflect the official position.

Three other sources of reference that helped to reconstruct a full picture of the accident are: (1) publicly available information of RusHydro (owner of the SSHPS), (2) press coverage in the national and regional media and (3) discussion in the Russian blogosphere. I would like to stress that the Russian-speaking blogosphere is a natural extension of its growing civil society. Instant and active discussion, the sharing of information and sources, photographs and witness accounts on numerous chat and blog platforms (most visibly Live Journal and forum.dron.ru) left the government with no choice but to make public investigation reports of both FSETAI and Parliamentary Commission available.

Study of these six sources of information suggests a preliminary conclusion that middle management was aware of the problem at the station. Moreover, in hindsight, the expert community was not terribly surprised by the accident. Thus the problem had been brewing for some time. It is not the absence of awareness, but rather powerlessness to react to an

emerging unsafe situation, that allows for the systematic migration of organizational behavior.

In this thesis I will try to differentiate how much of this powerlessness could be attributed to the limited availability of legal and regulatory instruments, as opposed to lack of safety culture. However, it seems that insufficient capital investment and backlog in maintenance shifts are key systemic factors that allow migration of organizational behavior from a safe to an unsafe state.

Developing a clear framework of Sustainability of Critical Infrastructure could increase public awareness of socio-technical landscape and system safety.

Over the last decade a lot has been said and written about the sustainable use of environmental resources. The public today has some degree of awareness of environmental changes that are taking place around us. I believe that a similar approach could be used in increasing awareness about the sustainability of critical infrastructure. By critical infrastructure I mean infrastructure such as electrical power systems, railroads, public utilities, highways etc. that allows society to function safely and effectively for the benefit of its members.

Rapid changes in societies may offer new, efficient and fast technological improvements such as new software for power management, highway traffic management or water purification systems. However, unless significant investments are made in the maintenance and modernization of physical infrastructure, such improvements can stretch the existing rigid critical infrastructure to its limits, with devastating consequences.

Public understanding of existing infrastructural limits, awareness of the social-technical landscape and system safety may theoretically lead to higher public investment in infrastructure (which often requires increase in taxation), an increased mandate to the government with regard to strengthening the regulatory environment in the private sector, as well as coupling investment incentives with investment obligations for the private sector. Such processes will also lead to regulatory changes and, in particular, to price regulations, i.e. how tariffs are being calculated and approved. One reason for underinvestment is the low profitability of infrastructure companies since capital investments are made from net profits.

1.3 Objective of the Thesis

System safety is uncharted water for many contemporary policy makers in the former Soviet Union. The thesis research will attempt to develop a System Safety Framework that can be integrated into public policy, market regulation and insurance sectors across Eurasia. In this context I will study Russia's Sayano-Shushenskaya Hydroelectric Power Station accident of August 17, 2009 as the most recent and most severe accident in terms of economic and human consequences.

The objective of the research is to describe the process of migration from a safe to an unsafe environment using the System Theory approach. The dynamics of systematic

migration will include a survey of the political, legislative, economic and cultural factors that allowed such migration to take place.

The magnitude and symbolic importance of the Sayano-Shushenskaya Hydroelectric Power Station accident present an opportunity to define important and long-lasting lessons for decision makers. It also represents an opportunity to increase public awareness concerning the sustainability of critical infrastructure, the socio-technical landscape and system safety in general.

1.4 Thesis Approach and Structure

Chapter Two: Rigidity of Reliability Theory vs. Dynamics of System Theory

This chapter will compare and contrast Reliability Theory and System Theory. The Reliability Approach was developed by engineers for the needs of a rigid twentieth-century state-planned economy and military-industrial complex. I argue that System Theory is better suited to the hybrid dynamic environment of Eurasia, which in this case refers to the geographical, geopolitical, infrastructural and socio-economic and cultural domain of former Soviet Union.

This chapter will also address issues of Language, Concept and Mental Models that define the framework of the discussion and its key terminology.

It is important to define terminology, its boundaries and relevance to the discussion. In the first part of this chapter I will describe key differences in translation and different contextual environments in which words are used. I will also attempt to explain how language affects our mental models in analyzing and describing safety.

Context definition will be followed by a brief introduction of System Theory and key principles of system safety. A short historical and literature review will be added to strengthen the base, and define the parameters, of discussion. Finally, I will return to the subject of terminology-mapping vocabulary and concepts that are necessary for further discussion.

***

The next three chapters of the thesis will build knowledge around this particular accident through a Hierarchy Theory approach that structures a system into different levels of complexity. This analytical approach focuses on abstract properties and "the fundamental difference between one level of complexity and another. Its ultimate aim is to explain the relationship between different levels: what generates levels, what separates them, and what links them" (Leveson, 2009).

The system-safety approach employs key principles of Hierarchical Theory in which safety is an emergent property. In simple words, this means that safe or unsafe operations may emerge as the result of relations between different levels of hierarchy. In such multilevel co-existence higher levels of hierarchy set conditions for the safe or unsafe behaviors of

lower levels. Since most such dynamics are non-linear, the interaction of lower-level components may in turn affect the constraints of higher levels of complexity.

In the case of SSHPS, each higher level of hierarchy - starting from Russia's United Energy System down - imposed constraints on each lower level of hierarchy. On the other hand, operations on the lower levels of hierarchy result in a higher level of complexity. If we abstract from a specific socio-technical level of the SSHPS accident to core principles system safety framework, we can look at the accident through the level prism (Leveson, 2009):

Level 1: Chain of Events;
Level 2: Conditions that Led to Such Events; and
Level 3: Systemic Factors that Allowed Such Conditions to Emerge Over Time.

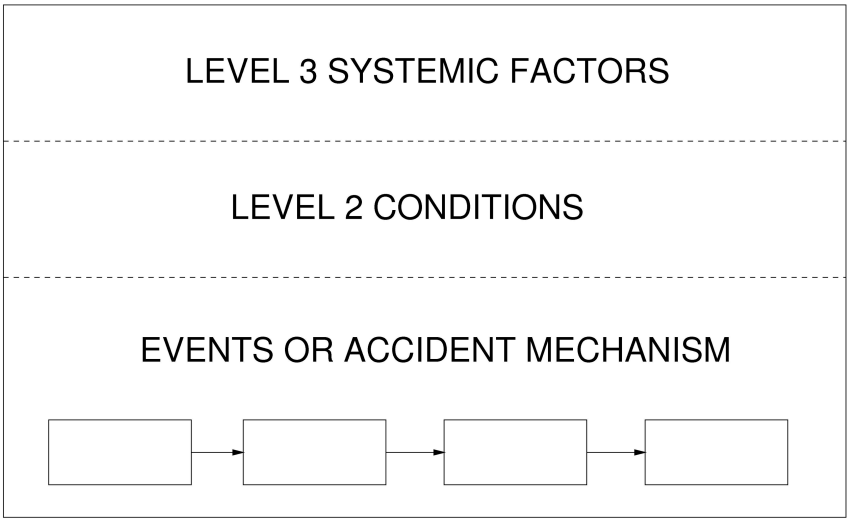

Figure 1: Hierarchical Model (Leveson, 2009)

Chapter Three: System Boundary and Chain of Events

Defining the chain of events is just the first step in understanding proximate processes. This is important, but not sufficient, in understanding the accident. I will provide the reader with key facts about SSHPS's system legacy, and its major design flaws, that are critical to overall analysis. I will then describe the evolution of the system boundary over time. Finally, readers will be presented with a description of proximate events at SSHPS prior and during the accident.

SSHPS has two complementary - and contradictory – goals: (1) generation of electricity and (2) stabilization of the regional energy grid. The origins of these goals are rooted in the evolution and disintegration of a super–system (Siberian energy system) into several inter-dependent systems as the result of the liberalization process that took place over the last decade.

The conflict of goals between the RusHydro holding and the Siberian Regional Energy Grid System, each with its separate goals and operational priorities, is one of the critical dynamics that was not anticipated by the system's original Soviet design engineers in the 1970s.

Chapter Four: Conditions

The purpose of this chapter is to employ a Systems-Theoretic Accident Model and Process - or STAMP - to analyze the SSHPS accident. We discussed hierarchical theory in the previous chapter. Complex systems are analyzed on different levels. STAMP presents an accident from multiple analytical positions. STAMP allows us to be flexible, to set multiple viewing points in terms of time, to visualize hierarchical levels and proximity to the event.

I will take my readers through seven levels of operations, starting from the operational service of the SSHSP and ending with the Federal Safety Agency (FSETAI). On every level, I will try to apply the STAMP model's clear and simple steps, as developed and described by Professor Nancy Leveson (2009):

1. Safety requirements and constraints;
2. Controls;
3. Context;
4. Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions;
5. Reasons for flawed control actions and dysfunctional interactions.

Chapter Five: Socio-Technical Landscape

The goal of this chapter is to briefly describe the evolution of the Soviet and, later, Russian electricity sector before and after 2000. For this purpose I will build two causal-loop models to identify, describe and compare key dynamics that are of interest to this research. Unfortunately the scope and availability of data do not allow building an actual system dynamics model. Such a model will require extensive research capabilities that are presently unavailable.

In this chapter I also will map Russia's decision-making and legislative processes; the evolution of the regional governments' role in public utility management; and the fundamental role of electricity generation sector in Russia's economy. I'll provide an overview of ten years of liberalization reforms (1992-2008) in the sector and its future perspectives, and address delays caused by the dynamics of Russia's legal and regulatory environments.

Chapter Six: Conclusion

The research will present a hierarchical structure of accident factors identified in time and space. The main deliverable of the thesis is to construct a "spatial picture" of a single accident in order to focus the attention of Eurasian policy makers on the problem of sustaining critical infrastructure and the socio-technical nature of complex accidents.

The deliverable can be transmitted directly via summary translated into Russian and/or indirectly by sharing the finding with international financial institutions (IFI), such as The World Bank, European Bank for Reconstruction and Development, Asian Development Bank, etc., which are actively involved in financing infrastructural projects in Eurasia.

The research may also have limited commercial application for private financial institutions involved in insuring complex infrastructure in the region, as well as for multinational corporations interested in building or upgrading complex infrastructural systems in Eurasia.

This Page Intentionally Left Blank

Chapter 2. Rigidity of Reliability Theory vs. Dynamics of System Theory

> *"While a system traditionally is modeled by decomposition into structural elements, the dynamic behavior of systems and actors is modeled by decomposition of the behavioral flow into events" (Jens Rasmussen).*

This chapter compares and contrasts Reliability Theory and System Theory. The Reliability Approach was developed by engineers for the needs of a rigid twentieth-century state planned economy and military-industrial complex. I argue that System Theory is better suited to the hybrid dynamic environment of Eurasia, which in this case refers to the geographical, geopolitical, infrastructural and socio-economic and cultural domain of the former Soviet Union.

This chapter will address issues of language, concept and mental models that define the discussion's framework and key terminology. It is important to define terminology, and to establish its parameters and relevance to the discussion. In the first part of this chapter I will describe key characteristics of the Reliability Theory and provide a brief historical overview. I will also attempt to explain how language affects our mental models in analyzing and describing safety.

Context definition will be followed by a brief introduction of System Theory and key principles of system safety. A brief conceptual introduction will strengthen the base and define the parameters of discussion. To illustrate a comparison of Reliability and System Theories more fully, I will briefly discuss SSHPS initial design within the context of Soviet expansion in Siberia. Finally, I will map five major gaps between the two approaches, stressing that System Theory approach allows us to detect and accurately characterize the changing dynamics of a hybrid socio-technical landscape.

2.1 Overview of the Evolution of Reliability Theory in the Soviet Union

The Soviet Union has long been a stronghold of Reliability Theory. The Russian school of Reliability Theory dates from the late 1950s - early 1960s. The first Union-level conference on reliability took place in 1958, one year after the launch of Sputnik. By that time it was clear that the rapidly expanding Soviet military industrial complex demanded new scientific frameworks.

By the late 1950s several unofficial research groups had been formed in aerospace and navy research centers in Moscow, Leningrad and other cities. This process gained official recognition when the school's founder, Professor Gnedenko, founded a reliability seminar at Moscow State University that grew into an 800 member collaborative community of mathematicians, statisticians, physicists and engineers. Gnedenko, Belyaev and Solovyev published their first work on reliability, *Mathematical Methods in Reliability Theory*, in

1965, the same year Barlow and Proschan published their *Mathematical Theory of Reliability* in New York (Ushakov, 2000).

In 1970, Kozlov and Ushakov published *Reliability Handbook*, which together with *Mathematical Methods in Reliability Theory* became table books for engineers across the USSR and dominated conceptual thinking for years to come. In the same year Professor Ushakov, founder of the *Gnedenko e-Forum*, the International Group on Reliability, presented milestone works of the Soviet/Russian school of Reliability Theory in his key-note lecture *Reliability: Past, Present, Future*.

As the Cold War increased its pace, this school of thought expanded its influence in the USSR - Moscow, Leningrad (shipbuilding), Kiev (electronics), Riga (aviation), Irkutsk (energy), etc.—each specializing in specific areas of the Soviet military industrial complex.

In 1960 by Professor L.A. Melentiev established the Energy Systems Institute at the Siberian Branch of Soviet Academy of Science. Based in Irkutsk, the institute concentrated on energy and electricity sector challenges. Its major research topics included theory and methods of systems studies in the energy sector; study on interrelations between the economy and energy; scientific and methodological support of energy programs for Russia, its regions and areas; theory and methods for comprehensive study and control of reliability and survivability of the fuel and energy complex and energy systems; theory and methods for management and control of electric power system operation and development; theory of hydraulic circuits and methods for mathematical modeling and optimization of heat-, water-, oil- and gas-supplying systems; theory and methods of extreme thermodynamics (Voropai).

Let us now summarize the key concepts of Reliability Theory (Ushakov, 2000. ; Gnedenko, Belyaev, & Solovyev, 1969). This is necessary to establish the scope of further discussion:

1. The Reliability Theory: “the overall scientific discipline… that develops general methods of evaluating the quality of systems from known quantities of their component parts… The reliability theory establishes the regularity of occurrence of defects in devices and methods of prediction”.
2. Increasing complexity: “Increase in the number of elements leads to decrease in the reliability of overall performance. But, at the same time, the increasing importance of tasks carried out by such devices requires their ever-increasing reliability…One of the most intriguing problems in reliability theory is the development of principles of design of a complex apparatus that will function even when some of its elements will not”.
3. Effectiveness: “characterizes a system’s ability to perform its main functions even with partial capacity. Failures of some (or even a majority of) system components lead only to gradual degradation of the system’s ability to perform its functions/operations”.
4. Survivability: **“**a special property of a system to “withstand impacts.” These impacts can be unpredictable inner failures (usually due to operator errors), environmental

influences (earthquakes, floods, hurricanes) or hostile human acts (enemy military operations or terrorist acts).
5. Safety: "a special property of a system characterizing effective performance of its main predetermined functions (production of goods, electrical power generation, gas and oil transportation, etc.) without dangerous environmental consequences for people and nature. Safety is usually considered in probabilistic terms that are close to those used in a "pure" reliability analysis".
6. Security: "is sometimes considered as a part of reliability-survivability problem. Indeed, many systems must not only operate reliably but also at the same time provide protection against non-sanctioned access".

The Soviet school of Reliability Theory has, over its fifty-year life, proven an enduring and successful developmental model. Its implementation allowed for the development of a robust, survivable Soviet infrastructure, which in many respects satisfied the economic and technical requirements of the planned economy.

One significant characteristic of the Reliability Theory is its focus on the internal components of a system. The theory analyses a system outside its context. In other words, human behavior, organizational culture, legal, economic and political environment are all exogenous factors that have secondary effects on the system.

The inward-focused semantics of the theory suggests that growing complexity could be resolved by increased reliability of a system's individual components, a decreased number of defects within the system and ability to predict emergence of errors and accidents.

The focus on "main predetermined functions" rules out the concept that a system may have emergent and/or unanticipated behavior. The concept of survivability assumes that a system has to have properties that can allow it to operate even with failed components and/or with a changed environment around the system.

2.2 Brief Overview of the System Theory

Now, let us define the framework of System Theory. There are three key assumptions (Leveson, 2009) that System Theory approach challenges:

1. Complexity cannot be addressed with physical decomposition of the system into separate physical components and decomposition into separate events over time. Each system, besides its main functions, has emergent behavior.
2. When components are integrated into a system, they become subject to numerous non-linear interactions, what often are called dynamics or causal-loop interactions.
3. Interaction between sub-systems result in emergent characteristics of complex systems that cannot be captured by traditional decomposition approaches.

In his *Introduction to General System Thinking*, Gerald M. Weinberg (1975) suggests three major systems categories with respect to methods of thinking:

1. Organized simplicity (machines): decomposition into a finite number of components, where interactions between components are defined and predictable.
2. Organized complexity (systems): "too complex for analysis and too structured for statistics".
3. Unorganized complexity (aggregates): "systems that are complex, but yet sufficiently random in their behavior so that they are sufficiently regular to be studied statistically… Randomness is the property that makes the statistical calculations come out right".

It is organized complexity that is most difficult for Reliability Theory to capture, from either a logical or statistical point of view. With technological progress and the growing interconnectivity of different systems, there is a significant migration of technologies from organized simplicity to organized complexity.

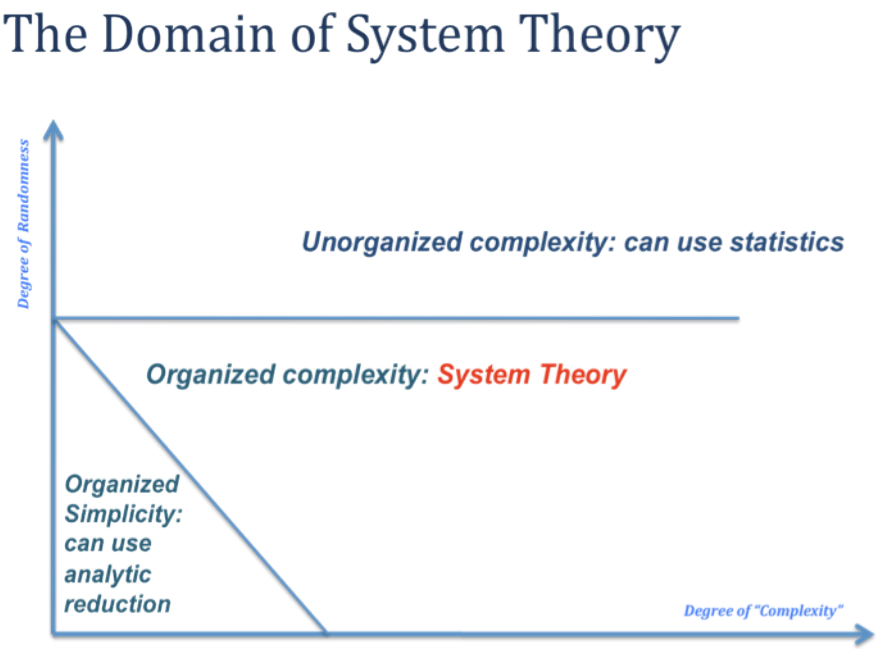

Figure 2: Three Categories of Systems (Leveson, 2009)

2.3 Short Excursus Into Evolution of SSHPS

To make our comparison of the Reliability and System Theories more concrete, let us briefly address SSHPS initial design and purpose. The initially coupled roles of SSHPS, namely, (1) electricity generation and (2) stability of the Siberian Energy System amid any disruption, were not clearly separated between state and private interests. I will cover this subject in greater detail in Chapter 3, which will define the system borders of SSHPS.

The political transformation and transition of post-Soviet societies have led to hybrid structures in political, economic and technological domains. Transition from a planned to a

market economy has created long-lasting disturbances in societies in which governmental, private sector and civil society boundaries of responsibility are still in the process of formation and not clearly defined. The government's role in ownership of critical/strategic enterprises and infrastructure is creating a conflicting regulatory environment.

SSHPS is an example of the dynamic co-existence of old and new technologies. The digital revolution and introduction of software into electromechanical subsystems created additional emergent complex system characteristics unanticipated by its original designers.

The co-existence of old and new technology, coupled with hybrid economic characteristics (both market and state-interventionist), created a new operational environment, while mental models and expectations that the system would continue to operate reliably remained unchanged.

The generation and culture gap between old-school engineers and Russia's new managers also reduced the ability to learn from previous experience. The station was built for the purpose of developing Siberia's industrial regions under the rigid demands of a planned economy; its design did not anticipate the cyclical demands of an emerging market economy.

On August 17, 2009 both the public and experts were shocked by the news of the accident, which concerned what was considered a very reliable traditional technology – hydropower generation. The principles of hydropower have been known since ancient Egypt and Mesopotamia and could be abstracted in terms of organized simplicity. The reliability of each component, however complex and powerful, could be calculated and measured.

On the other hand, SSHPS is a complex system. It generates 6.4 gigawatts of electric power, is part of a larger hydropower cascade that includes two more stations, and plays an important role of keeping the integrated Siberian Regional Electricity Grid stable.

The system-thinking approach forces us to put the SSHPS into natural, knowledge, human and economic contexts. The snapshot below shows the dynamics of how different processes that go through our system are evolved over time and how the system itself is subject to emergent processes.

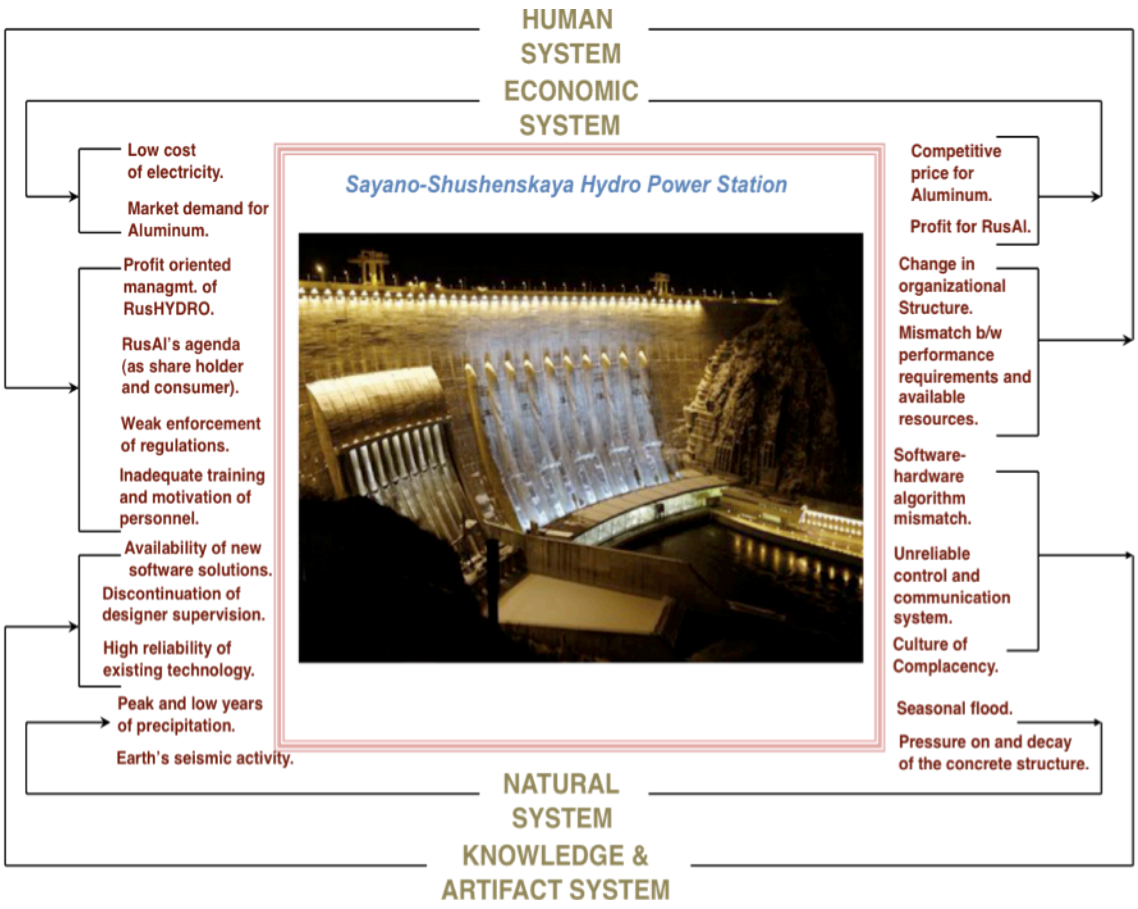

Figure 3: Socio-Technical Environment (adapted from Crawley (2007))

2.4 Five Major Gaps Between Two Theories

The socio-technical landscape that surrounds the SSHPS is much more complex and different from the one for which the station was initially designed. Changes in the socio-technical landscape suggest that traditional approaches of the Reliability Theory, with its inward focus, may not be an effective tool to identify emerging challenges. The System Theory approach, however, takes into consideration both the key characteristics of the changing hybrid socio-technical landscape and the motivations of multiple stakeholders. Below are the five major gaps that in my opinion do not allow the old approach to sense and capture the changing dynamics in which SSHPS found itself prior to the accident.

Moving from Tunnel Vision to Holistic Overviews of the Entire Socio-Technical Landscape

Complete understanding of the causes of any accident is often hindered by the ways in which the accident is described in newspapers and official reports. This approach is a practical way for people to comprehend, investigate, draw parallels, identify patterns, conclude, learn lessons and prevent similar accident situations in the future.

Reliability Theory fits perfectly the logic of a chain of events. It provides facts that become midpoints in the accident narrative that investigators reconstruct. Facts are not perceived

as “intersection points” offering an array of equally valid choices but as process points that underline when and where incorrect decisions were made.

Hindsight gives investigators reconstructing accident narrative better and more complete information than the actors whose decisions led to failure. Hindsight bias may, however, exaggerate the importance of an accident’s factual narrative as it minimizes less-obvious contextual issues that contributed to accident formation.

As Nancy Leveson puts it, “viewing accidents as chains of events and conditions may limit understanding and learning from the loss and omit causal factors that cannot be included in an event chain” (Leveson, 2009) and “event-based models are poor at representing systemic accidents factors such as structural deficiencies in the organization, management deficiencies, and flaws in the safety culture of the company or industry (Leveson, 2009).

Reliability Should Not Be Confused With Safety

A system can be reliable but unsafe, as well as safe but unreliable. The conflict between reliability and safety goes even deeper (Leveson, 2009). On one hand, if the system is reliable it can be safe overall, while deterioration in reliability may lead to a decrease in safety. On the other hand, there could be situations in which an increase in reliability may lead to a decrease in safety and vice versa. In other words, the relationship between reliability and safety is not linear; it can be as diverse as the emergent relations of a system’s subcomponents. In the case of the SSHSP accident only 10 out of 75 casualties at the station were involved in the station’s core operational activities. The other 65 were workers employed by a subsidiary company (Council of Federation, 2009a) in charge of station maintenance. These people could have been evacuated from the station as the situation emerged. In other words, had proper remedial action been taken, unreliable equipment need not have led to a dangerous situation for the majority of the station’s workers.

In Eurasia, political agendas have historically played an important role in decision-making. It was often the case that achieving policy goals (political goals, economic development, budget constraints, push for technological modernization, greater public utility) was a greater priority than the safety of citizens and consumers. With the evolution of market reforms, this trend has received new impulse as financial insurance tools are used to mitigate technological risks. In either case, “reliability is often quantified as a mean time between failure” (Leveson, 2009) in terms of political, engineering or financial loss.

In the majority of situations decision-makers and experts recognize difference between (1) reliability for political and/or financial gains, and (2) safety of people in and around particular systems. It is the public that may confuse and interchange these two concepts. The trade-off between reliability and safety are very often conscious choices of decision makers rather than confusion of terms.

The irreconcilable dilemma faced by the reliability approach and its probabilistic assessment is that it neither integrates new and often immeasurable factors into its framework nor ignores such factors when they are irrelevant.

Role of Operators in Accidents and The Culture of Blame

In the aftermath of an accident, one can easily list logical arguments about how and why people should have foreseen and prevented upcoming events. We easily judge people who failed to take proper action. We focus on such personal shortcomings as absence of proper training and experience, health conditions, hours of proper sleep, etc. We tend to focus our attention on people who happened to be closest to the accident in terms of time and space.

Human error is often associated with the role of human operators who are supposed to activate, deactivate, control, intervene and prevent an emergency situation. As systems become more complex so do the roles of operators. All characteristics prone to complex systems - hierarchy, segmentation, expansion of borders, etc. – are applicable to the changing role of operators. In other words, complex systems are managed on different levels, from different locations and often by operators with different control and prevention tools, mental models, organizational cultures and economic priorities.

In the case of the SSHPS accident, there were at least three major operational points: the Siberian Dispatch Center, the Central Operation Room of the Bratsk Hydro Power Plant and the Central Operation Room of the SSHPS. Each had different priorities prior to and during the accident, each had limited abilities to intervene and prevent the accident, each had incomplete and insufficient information about the emerging accident.

More importantly, each of the three operating rooms was no more than the end-point of a linear chain of events. Reverse-engineering the accident based on such end-points may provide a limited and distorted picture, leading to an incomplete and flawed conclusion. Reliability Theory stresses the internal components of each of the subsystems and questions why the system was unable to operate when some of its components failed. System Theory attempts to recreate the environment in which these decisions were made. "Without changing the environment, human error cannot be reduced for long. We design systems in which operator error is inevitable and then blame the operator and not the system design" (Leveson, 2009).

Role of Software in Accidents

The role played by software brings us back to the discussion of co-existence of old and new technologies. Software today presents engineers with significant shortcuts that allow them to "write down the design of instructions to accomplish the desired goal" (Leveson, 2009). The introduction and adaptation of new mechanical and software components (subsystems) into existing systems raise issues that the Reliability approach is unable to address.

For example: a new Power Management and Process Control System (PMPCS) was introduced into SSHPS's design during the station's 28th year of operation. The logical

design of the software and the electro-mechanical design of the power plant were conducted years apart, in vastly different technological environments. The algorithms of PMPCS and SSHPS's oldest turbine were not properly implemented. The original designers could not have anticipated the new power management system characteristics. Thus the software modernization of the SSHPS should have taken into account changes to the system over time and synchronized implementation of the new software with the original subsystems of SSHPS.

The initially coupled roles of SSHPS—(1) electricity generation and (2) stability of the Siberian Regional Energy Grid System amid any disruption—were not clearly separated between state and private interests. Designers of the power management software introduced to manage SSHPS did not recognize the separation of such roles.

Static Versus Dynamic View of the System

The Reliability Theory's definition of system borders focuses attention on internal and measurable components of the system. The reliability approach helps to construct a static and clearly defined system. External and/or immeasurable factors are ignored and considered irrelevant.

The evolution of the Siberian Regional Energy Grid System, and the sporadic and fragmented introduction of power management software at the SSHPS, have over time changed the operating environment. Operators at the station, and at the Siberia Regional Dispatch Center, have an efficient and effective - but incomplete - picture of the process as well as limited abilities to manage the process. The growing complexity of relations between operator and machines, between operators, and between machines may lead to new types of accidents. A new operational environment may lead to unanticipated new types of human errors

All this suggests that systems exist in a highly dynamic environment. As Rasmussen says, "accidents are often caused not by a coincidence of independent failures but instead reflect a systematic migration of organizational behavior to the boundaries of safe behavior under pressure towards cost-effectiveness in an aggressive, competitive environment" (Rasmussen & Svedung, 2000).

In sum, this catalogue of factors requires that we revisit problems of critical infrastructure in general and the SSHPS accident in particular. The system safety approach offers different perspective on dealing with complexity, looking at complex systems in terms of hierarchical levels in which "each level imposing constraints on the degree of freedom of the components at the lower level" (Leveson, 2009) as opposed to focusing on primary predetermined functions and the survivability of critical components.

This Page Intentionally Left Blank

Chapter 3. System Boundaries and Chain of Events

"Many good ideas are really two ideas in one – which form a bridge between two realms of thought or different points of view" (Marvin Minsky).

The purpose of this chapter is to introduce readers to the SSHPS as a system, describe key events that took prior and during the accident and take an initial step in comprehending the accident's complexity.

As I mentioned before, event-based reconstruction of an accident creates a tunnel vision in which many critical factors and developments are omitted as irrelevant and insignificant. Defining the chain of events is just a first step in understanding proximate processes. This is important—but insufficient—in understanding an accident.

The danger here is that we often are satisfied with such incomplete pictures. We rush to conclusions. We search for pre-existing mental models of historical accidents. On the contrary, the nature of complex system tells us that potential accidents may be unique in nature. A broader analysis of the accident will give us an understanding of the system theory approach that we can use in forward-looking mode.

I will briefly stop to give the reader key facts about SSHPS's System Legacy. I will then spend substantial time describing the evolution of the system's boundaries over time. Finally, readers will be presented with a description of proximate events at SSHPS prior to and during the accident.

3.1 System Legacy

Prior Floods and the Spillway

Both the Official Investigation Report by Rostekhnadzor and the Report of the Parliamentary Commission state that no external physical processes had significant affect on the event before or during the accident. However, it is worth mentioning that three previous accidents were related to seasonal high water and spring flooding.

Major flooding accidents took place in 1979, 1985 and 1988. On May 23, 1979, while the station was under construction, record-high water led to the emergency discharge of water through the unfinished waste weir, which led to flooding of the only operating turbine. It took 112 days to re-start the generator.

In 1985 and 1988 major floods tested the station, which led to partial destruction and flow up overall of the hydraulic jump basin. All three accidents showed the need for the alternative shore spillway that was initially designed as part of the SSHPS complex (Council of Federation, 2009a). However, due to financial difficulties, construction of the alternative

spillway was delayed until 2005. It was incomplete at the time of the 2009 accident; information about its readiness as of that time is unavailable.

The presence of the alternative spillway could have given immediate and long-term advantage to SSHPS during the most recent accident. An emergency discharge through an alternative shore spillway could have helped to localize the accident in a shorter period of time.

In the aftermath of the accident, presence of the discharge spillway could have eased pressure on the hydraulic jump basin, which had to operate in emergency-discharge mode for more than a year. Such conditions led to heavy ice build-up on the dam during Siberian winter and a gradual change in the subsoil of the dam's foundation during spring and summer, compromising the hydraulic basin's structural integrity. The three combined factors created a long-term safety threat jeopardizing populations living downstream from the station.

The alternative shore spillway was completed in record time in early September 2010, which gave much-needed relief to the hydraulic jump basin and to the station's three operational turbines (Goncharenko, 2010).

Experimental Design of Turbine 2

The station's design was in many respects experimental. It experienced a number of contingency situations and received follow-up services from its project designers up until the mid-1990s. In particular, its oldest turbine, Turbine 2, was experimental in nature, with only two safe regimes of operation. It had two safe zones that were recommended for operation. These were Load Zone 1: from 0 to 265 Megawatt and Load Zone 3: from 570 to 640 Megawatt. There was also unsafe Load Zone 2 between from 265 to 570 Megawatts (Council of Federation, 2009a). The turbine's designers recommended passing through the unsafe zone as quickly as possible. However, the headwater, which determines the speed of water, as well as absence of the spillway, also played roles in how quickly the turbine could pass through unsafe mode.

The turbine limitations were known, as was information about equipment maturity and overhaul cycles. Prior to official acceptance of the station's full operation in 2000 the research institute that provided post-acceptance service was not involved in maintenance or modernization of the turbine. On March 12, 2009 (6 months prior to the accident) Turbine 2 underwent capital repair. The station's Chief Engineer took pride in the fact that this repair entailed introduction of a management system for individual servomotors, which provided individual hydraulic actuators for each turbine blade. This was the first time this technology had been employed (RusHydro, March 23, 2009).

Other design flaws

In terms of safety constraints, hydro electricity generation is considered a mature technology whose behavior is fully studied and understood. However, after the accident, the Official Investigation Report by FSETAI and the Report of the Parliamentary Commission came to the conclusion that the station's design had several flaws.

The station's design did not include a guaranteed (alternative) power source for the emergency closing valve. The system for automatic return of the emergency closing valve did not react because its design had not included such an emergency scenario. The turbine room did not separate turbines into silos (something not generally practiced in the design of hydro power stations).

3.2 System Boundaries and Evolution of the System Over Time

Drawing boundaries of the system is a very difficult task, especially for such a complex system. There can be different interpretations of where boundaries should be drawn. First and foremost, however, we need to recognize that SSHPS is just a subsystem of a higher-level system and its processes. It should be thus considered within a larger context.

More importantly, SSHPS was initially a subsystem of a single higher-level system. However, liberalization of the electricity market, followed by separation of power generation and transmission, led to a situation in which SSHPS became a subsystem of two different higher-level systems—(1) RusHydro holding and (2) Siberian Regional Energy Grid System—each with separate goals and operational priorities.

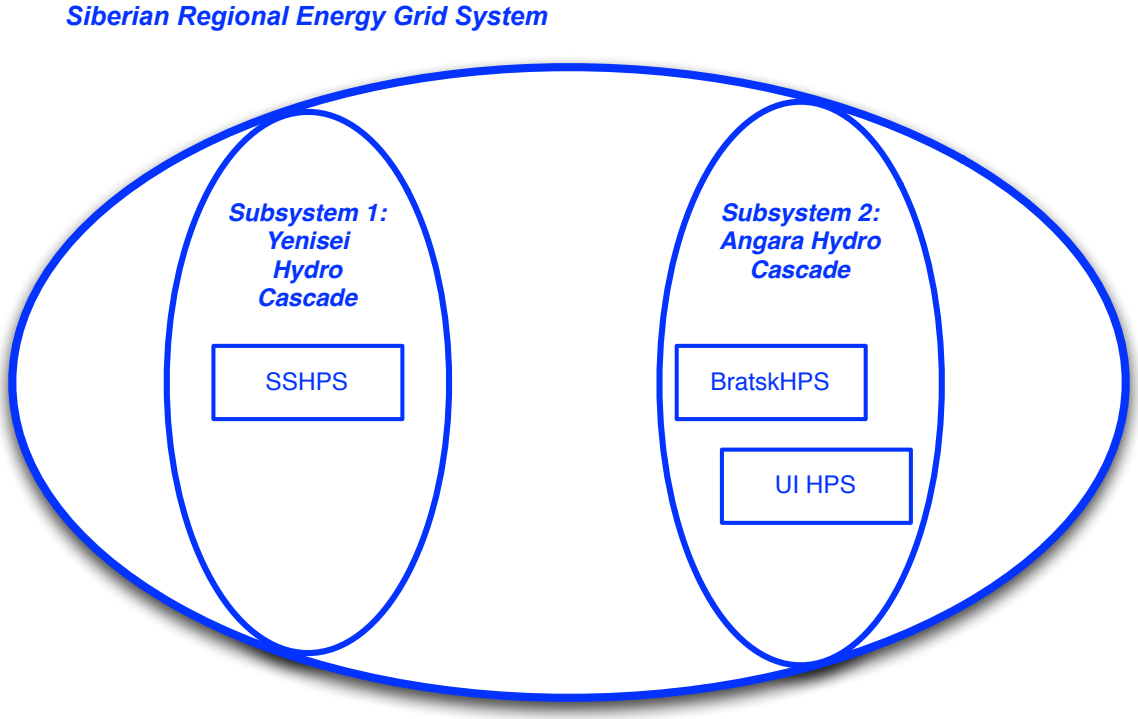

Figure 4: System Boundary Prior to 2000

There are several definitions of what constitutes a system. System boundaries are context-dependent, and they shift depending on context analysis.

If we consider a system as more than the sum of its components, then SSHPS fits into the Siberian Regional Energy Grid System; its goal as such is to maintain the stability of the energy grid system, achieved by an increase or decrease in power generation.

If we consider that a system is a set of directly and indirectly interconnected "components that act together as a whole to achieve some common goal, objective, or end" (Leveson, 2009), SSHPS becomes a subsystem of Russia's State controlled energy holding RusHydro, with the goal of generating low-cost electricity for industrial production, particularly the production of aluminum.

At the time of its original design, when SSHPS was expected to be part of a single super-system, these two goals had to be coordinated. Immediate priority was given to the system's stability, while long-term priority was focused on the power generation. As generation and transmission functions were separated into two different systems, these two goals were divorced, each coming under the purview of a different system.

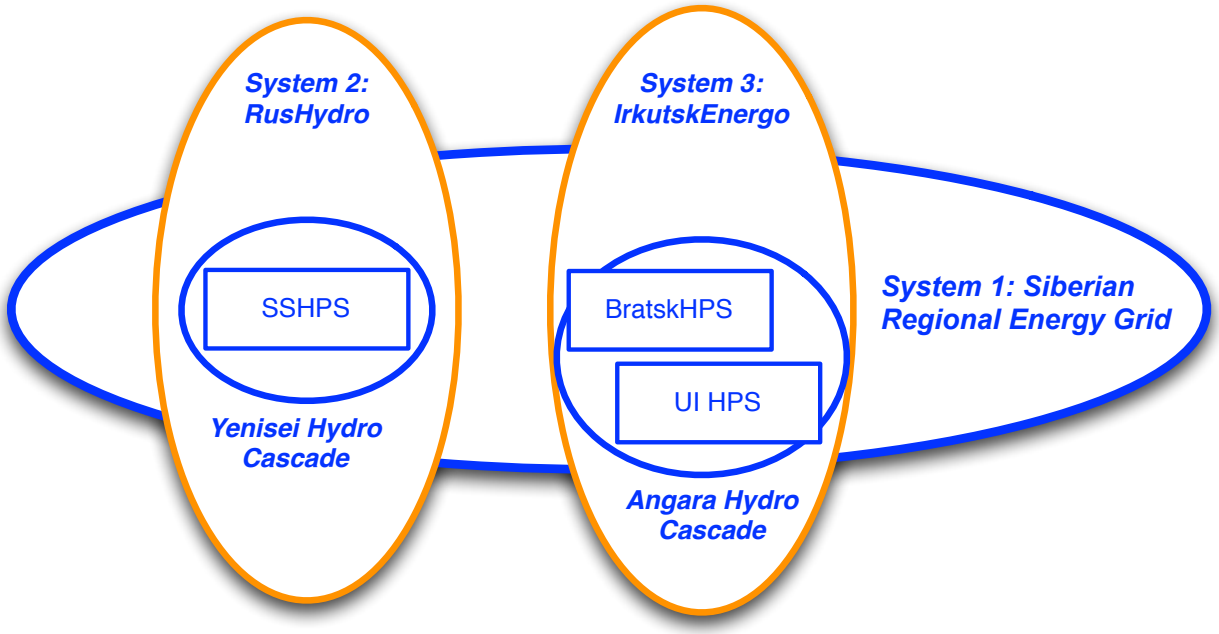

Figure 5: System Boundaries After 2000

System 1: Siberian Regional Energy Grid Operator. Subsystem 1.1: SSHPS.
System 2: RusHydro. Subsystem 2.1: SSHPS.
System 3: IrkutskEnergo. Subsystem: 3.1 Bratsk HPS, Subsystem 3.2: Ust Ilimsk HPS.

Only these three HPSs —SSHPS, Ust Ilimsk HPS and Bratsk HPS—are hydropower stations used to stabilize the Siberian Regional Energy Grid System (Rostekhnadzor, 2009). Bratsk and Ust Ilimsk hydropower stations are part of the Angara hydro cascade located approximately 1500 km northeast of SSHPS. These stations are part of Irkutsk Power Generation and Distribution Company *IrkutskEnergo* (IrkutskEnergo, 2007); 50,19 % belongs to En+ Group (Ispolatov, 2010) controlled by Russian oligarch Oleg Deripaska, who also a CEO of Russia's Aluminum producing conglomerate RUSAL. 40% of the stakes are still in the hands of the Federal Agency for State Property Management (*Rosimuschestvo*).

Generation Domain

The chart below describes the generation domain in detail. According to The Law on Electricity Energy, the government intervenes in the Electricity Sector in order to ensure the unity of system process control and management; safeguard the balance of interests between producers and consumers of electricity; manage state property in the electricity industry; introduce and regulate tariffs for specific services, etc. (Russian Federation, 2003).

In the power generation domain, the goals of SSHPS include generation of low-cost energy, overall safety and reliability of the station, the safety of station personnel, and the safety of 50,000 people living downstream from the station.

Prior to the 2009 accident, the main hazard at the station was high water during flood season and the aging dam's structural integrity. Both required constant monitoring, and both were considered exogenous factors (weather, time, season, temperature, etc.). Most significant among such exogenous factors are 1) water level of the upper reservoir that determined the headwater, and 2) significant temperature fluctuation that affected the water levels.

The life-cycle of the existing electricity generation infrastructure was another prime source of the problem. Complex measurements of infrastructure deterioration were not practiced. Infrastructure deterioration factors did not affect financial planning, maintenance or technical safety behaviors. In other words, in the case of this particular accident, not only had operator behavior become unsafe, but also there are symptoms that the system itself had gradually started to migrate to an unsafe domain.

Representatives of the Federal Service for Environmental, Technical and Atomic Inspection (FSETAI) did not inspect hydro-turbine units because they were not categorized as hazardous industrial facilities. Newly adopted law on Technical Regulations had not yet established a regulatory framework for follow-up. Some existing technical regulations were reclassified from "required" to "recommended" mode.

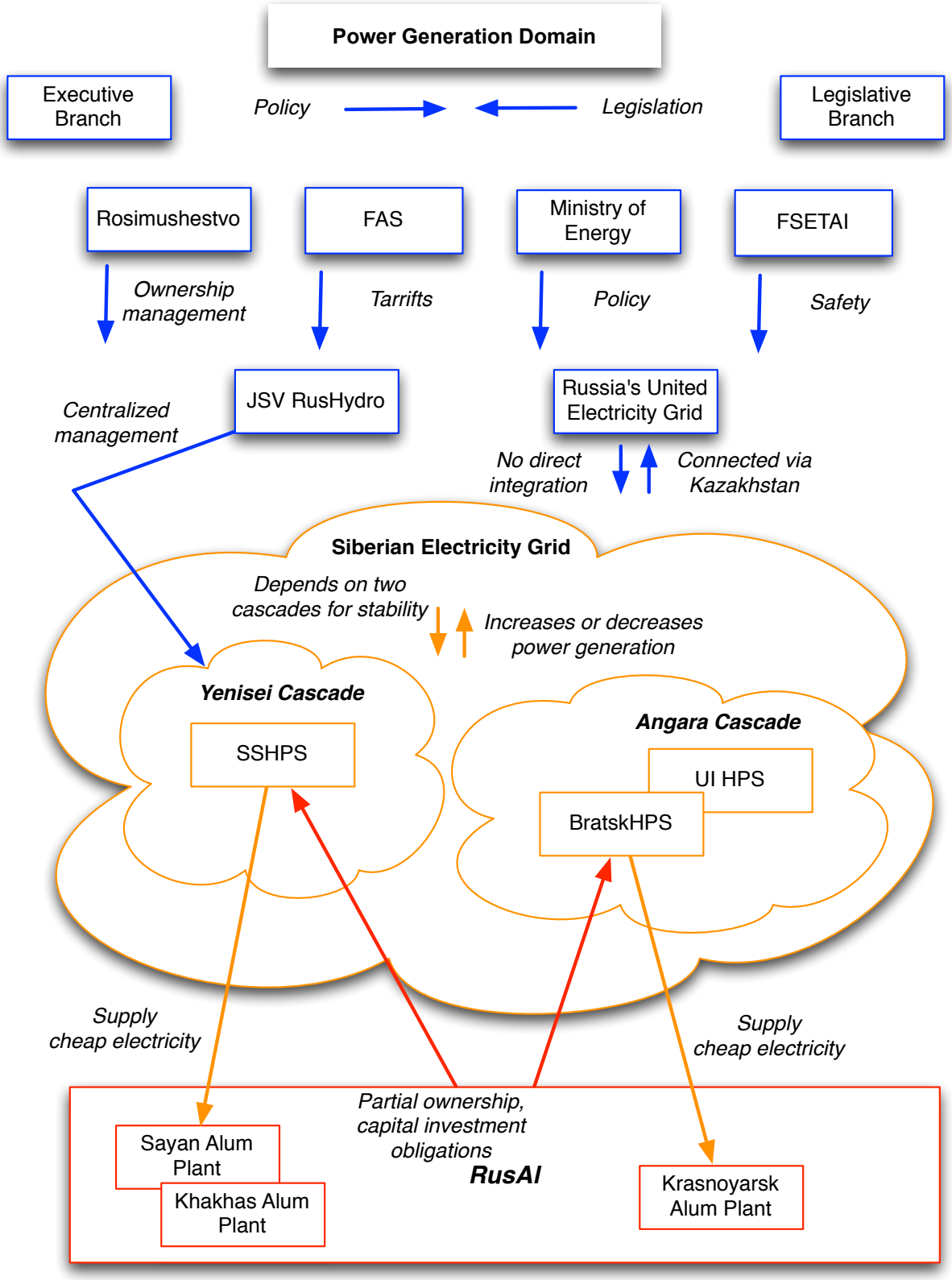

Figure 6: SSHPS in Power Generation Domain

Operation Dispatch Management Domain

The goal of SSHPS in the Operation Dispatch Management Domain was to remain a reliable source for voltage and frequency of the Siberian Electric System and to actively participate in stabilization when necessary.

The technological foundations of Russia's Electricity sector are a unified national electrical network, territorial distribution networks and a unified system of operation dispatch. The Law on Electric Power Sector serves to ensure a reliable power supply and power quality that meets the requirements of technical regulations (Russian Federation, 2003).

The Siberian Regional Energy Grid System is not directly integrated with the European part of the United Energy System, relying instead on Kazakhstan's infrastructure, which connects the European and Siberian energy systems. During the accident, significant amount of power had to be transferred from Kazakhstan to keep the Siberian system stable until thermal power plants were able to increase production.

System hazards on the level of the Siberian Regional Energy Grid System are possible grid blackouts, which, in the context of the harsh Siberian climate and the region's energy-intensive heavy industry, can have significant economic effects. As a result, the Siberian Unified Grid Combined System Dispatch focused its attention on electricity grid stability, reliability and synchrony.

As one expert points out, in the majority of Russia's regional electricity networks it is acceptable practice to compensate for the recovery of reactive power by means of electricity generation. Such a systemic characteristic of using brute force of fluctuating power generation leads to "decrease of functionality capabilities and deterioration in operation modes of power stations' generators, as well as overall decrease of reliability of the energy system" (Council of Federation, 2009b).

In addition to the legacy hazard, fragmented introduction of new methods and instruments of power management systems (active and reactive power management instruments) led to further complexity and confusion.

Further deregulation of the electricity market in 2011 will require the generation, transmission and distribution components of a previously integrated infrastructure to be more flexible and responsive to fluctuation in the demand and supply of electricity. "Temporal flexibility" becomes the new system's requirement, which was not considered in its original design. Such a requirement will add more uncertainty to an already fragmented and aging electricity system.

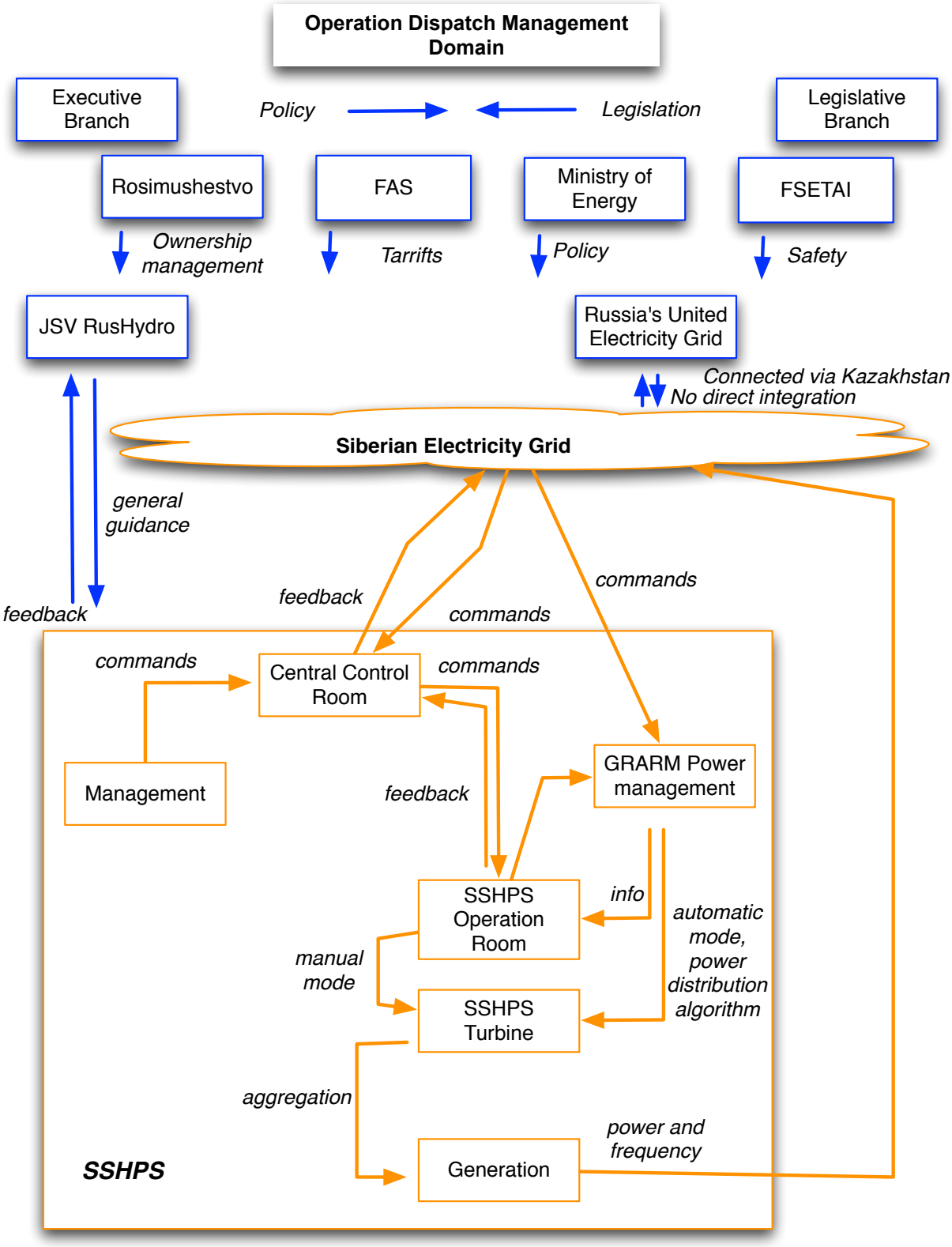

Figure 7: Operation Dispatch Management Domain

3.3 Proximate Events at SSHPS

This section describes proximate events occurred prior and during the accident. The description is based on the report of the official investigation conducted by FSETAI (Rostekhnadzor, 2009) and the official parliamentary report (Council of Federation, 2009a). The time of events mentioned is local; the date format is dd.mm.year.

19:14, 16.08.2009 – On the order of the Siberian Dispatch Center, Turbine 2 at the SSHPS was turned on from reserve mode.

20:20, 16.08.2009 - Fire broke out at Bratsk HPS the night prior to the accident. The Central Control Room of the Bratsk HPS reported shutdown of the automatic frequency control system, automated system, and voice communication with the regional transmission company and its local control dispatch. Two main fiber-optic cables that provided Bratsk HPS's communication went down. Equipment for the main and reserve communication channels was off. The automatic frequency control system and voice communication with the Siberian Unified Grid Combined System Dispatch (SUGCSD or Siberian Dispatch Center) was down.

20:31,16.08.2009 - After the loss of communication with Bratsk HPS the dispatcher at the Siberian Dispatch Center orders operators at the SSHPS to switch Control group of active and reactive power (GRARM) to automated mode from the Central automatic frequency control system at the Siberian Dispatch Center. Between 20:31, 16.08.2009 and 4:12, 17.08.2009 SSHPS was managed in distant mode by the SUGSD from city of Kemerovo, approximately 800 km northwest of SSHPS and 2500 km west of Bratsk HPS.

20:50, 16.08.2009 - The fire at the Bratsk HPS was localized. At 21:00 Operator at Bratsk HPS was able to reach the dispatcher at the SUGSD by regular cell phone. For 40 minutes the Bratsk HPS was unmonitored by the Siberian Dispatch Center. At 10:03, 17.08.2009 emergency mode was switched off and communication was reestablished.

4:00, 17.08.2009 - Crew shift took place at the SSHPS (local time 8:00). Nine of the ten turbines were in operation (including Turbine 2). Turbine 6 was in reserve. Total active power of the operating turbines - 4400 megawatt, the level of headwater elevation – 537.11 meters.

Figure 8: Siberian Regional Energy Grid System (Sagers, et al., 2009)

Prior to the accident the vibration amplitude of the Turbine 2 cover bearing increased 4 times. After yet another capacity decrease, the locking pins of Turbine 2 cover fractured, leading to increased fluctuation of the rotor. As a result, the whole hydraulic component was moving up in the shaft. The power plant was flooded through the empty shaft of Turbine 2.

As the rotor passed a certain level on the shaft it switched to pumping mode, which created excessive pressure on the blades of the turbine. Turbine 2's still working cross head and rotor destroyed Turbine Room and turbines 2, 3 and 4.

4:13, 17.08.2009 - Working personnel of the Turbine room heard a loud slap in the vicinity of Turbine 2, followed by surge of head of water. In the Central Control Room sound-and-light alert was turned on.

Operational communication, operational electricity, automated systems, signaling/warning systems, and system for indicator and monitoring were shut down. Operators of the Central Control Room visually (via window) saw a flow of water (about one meter high) from the Turbine Room. Several passages of the Turbine Room were destroyed. Active load shedding to 0 megawatt, including internal needs. The Turbine room was destroyed by Turbine 2, subsequent power outage and lost to the flood.

5:00, 17.08.2009 - Emergency services were notified about limited flooding of the Turbine Room. The first emergency group arriving on the scene was not prepared for the magnitude of the accident.

5:20, 17.08.2009 - At the top of the dam technological valves of each turbine were closed manually and the flow of water was stopped. The Turbine Room remains flooded at the tail water level of the dam. Drainage of the Turbine Room was not possible due to dysfunctional valves behind the turbines.

7:32, 17.08.2009 - External power was supplied to frame crane at the top of the dam.

7:50, 17.08.2009 - The emergency crew opened valves of the spillway dike manually.

9:07, 17.08.2009 - The balance of the incoming and outgoing water was restored. The level of headwater elevation – 537.16 meters. Mainskaya HPS downstream completed contingency water discharge. After initial visual assessment, turbines 2, 7 and 9 were destroyed. Turbines 1 and 3 were significantly damaged.

11:04, 17.08.2009 - Siberian Energy Systems was stabilized.

13:07, 17.08.2009 - Accident was localized.

This Page Intentionally Left Blank

Chapter 4. Identifying Conditions Using STAMP Analysis

"Complexity usually arises from a small number of disproportionally complex procedures" (Henry, Kafura, 1984).

"A program is a human artifact, a real-life program is a complex human artifact; and any human artifact of sufficient size and complexity is imperfect" (De Millo, Lipton, Perlis, 1979).

The purpose of this chapter is to employ the Systems-Theoretic Accident Model and Process (STAMP) to analyze the SSHPS accident. Hierarchy theory was discussed in the previous chapter. STAMP presents an accident from multiple analytical positions. STAMP allows us to be flexible, to set multiple viewing points in terms of time, hierarchical levels and proximity to the event.

The STAMP model's clear, simple steps were developed by Professor Nancy Leveson (2009). They are:

1. Safety requirements and constraints
2. Controls
3. Context
4. Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions
5. Reasons for flawed control actions and dysfunctional interactions:

4.1 First Level Operations: Operations Service/Turbine room

Safety Requirements and Constraints:
Operation service is located in closest proximity to the turbines. Accurate information generated by monitoring equipment allows operators to maintain awareness of the overall process. Physical presence of personnel in the turbine rooms is partially due to the legacy of existing systems, as well as the fact that monitoring equipment used at the station was insufficient and/or unreliable to operate without constant human presence.

Inadequate Control Actions:
Operators do not have significant control functions; they have to maintain monitoring equipment—especially operators responsible for the electricity quality, i.e. its frequency and voltage.

Context in Which Decisions Are Made:

a. Roles and responsibilities

Being in closest proximity to turbines, operators also have to maintain discipline in the operation-dispatch process and immediately inform the direct line of management about emergency situations.

Operators' major responsibilities include adherence of the operational mode of the turbines, monitoring parameters of operational equipment, and monitoring operations that involve the start and shutdown of turbines.

b. Environmental and behavior-shaping factors

On the day of the accident, the operators were in contingency mode as the command to start Turbine 2 came down. Operators knew about the limitations of Turbine 2, and the fact that it was the oldest turbine at the station and had undergone overhaul earlier that year. The head of the unit (49 years old) had more than 8 years of experience in the position.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:

The degree to which personnel were aware of the emergency situation on the regional grid level remains unclear. During the 4 hours prior to the accident Turbine 2 was managed remotely from the Siberian Dispatch Center. After the accident it was clear that commands sent from the Siberian Dispatch Center through the automated system had distributed the load unevenly to turbines 2, 7 and 9. It is not clear when information about the increase in the vibration of Turbine 2 was passed on to the Central operation room and further to the Siberian Dispatch Center. The load on the turbine increased and decreased several times within few hours. It seems the accident took place as the Operation Service was trying to slow down Turbine 2 manually.

Reasons for flawed control actions and dysfunctional interactions:

It is clear that there was inadequate communication between Operations, The Central Control Room and the Siberian Dispatch Center.

As Turbine 2 was taken over by the Siberian Dispatch Center, personnel could have reported data about the turbine's anomalous behavior to the Central Room of the SSHPS, but it is unclear if this information was relayed to the Siberian Dispatch Center. There was no direct communication or feedback channel that allowed Turbine Room personnel to communicate with the dispatch center in case of emergency.

4.2 Second-Level Operations: SSHPS's Service Units

Production and Technical Service

Safety Requirements and Constraints:

The head of the Production and Technical Service is responsible for maintaining continuous and reliable operation of the turbines.

According to the Official Accident Report (Rostekhnadzor, 2009), these responsibilities also included informing the direct line of report about emergency situations and the interruption of the operation in case of emergency according to standard operational procedures.

Inadequate Control Actions:
The turbines (hydro-aggregates) of the SSHPS had three layers of "defense" (Rostekhnadzor, 2009):

- Main protection: includes 15 different functions, a majority of them focused on the operation and reliability of the main generator.
- Reserve protection: includes 7 functions primarily focused on protecting the rotor of the turbine from overload.
- Hydro-mechanical protection: includes 9 functions that could be activated in case the turbine had to be turned off.

None of the 31 functions were directly related to increases of vibration in the turbine. Only one main function was indirectly related to vibration; it addressed asynchrony of the generator.

According to the official investigation report, the head of the Production and Technical Service did not provide personnel with qualitative operational instructions and timely reconsideration of these instructions. The head of the Production and Technical Service also failed to conduct proper analysis and assessment of equipment conditions (Rostekhnadzor, 2009).

Context in Which Decisions Are Made:
Turbine 2 had a complete overhaul in 2005 and an intermediate overhaul in 2009 (finished on March 16, 2009) with installation of individual hydraulic actuators for each turbine blade (Rostekhnadzor, 2009). According to the accident report, the head of the service may not have had complete information about Turbine 2's history and problems. The head of the service (51 years old) had only 2 months of experience in that position.

a. Roles and responsibilities

As the accident developed the head of the service had sufficient vibration data that was coming of from the turbine. However, it seems that the Head of Production and Technical Service may not have had enough time to communicate the findings or did not have enough time to react.

b. Environmental and behavior-shaping factors

The turbine's control mechanisms were imbedded in its cover, which cut loose as vibration peaked. It is possible that at some point it was not possible to stop the turbine manually as it went out of control.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
There was a time lag between two events: (1) when the turbine was switched from reserve to operational mode by the SSHPS's Central Room and (2) when the Siberian Dispatch Center assumed remote mode operation of the turbine. It is not clear when the Head of the Production and Technical Service became aware of the second event.

Reasons for flawed control actions and dysfunctional interactions:
Inadequate coordination or communication, as well as incomplete awareness of the emerging situation, may have been the reasons for flaws. The Head of Production and Technical Service knew about Turbine 2's limitations, but operated in contingency mode and may not have known about the intent of the regional dispatch center. In other words, he did not have a full picture of the emerging situation that had been taking place within the Siberian Regional Energy Grid System.

Equipment Monitoring Services

Safety Requirements and Constrains:
Most of the monitoring systems built into the SSHPS were based on analog technology and dispersed along huge monitoring dashboards. Lower-hierarchy subsystems have sensors only in their close proximity. Such dispersion of sensors and fragmentation of information did not allow the monitoring service to aggregate information in a timely and adequate manner.

The responsibilities of the Head of Equipment Monitoring Services included the following functions: guaranteeing operation of the sensor equipment and system; maintaining operational readiness; detecting and preventing anomalies in the system.

Inadequate Control Actions:
Turbine 2's vibration control monitors were not put into operation; vibration data was thus not considered by either station management or service personnel (Rostekhnadzor, 2009).

It is not clear if the Head of Equipment Monitoring Services received, processed and analyzed the results of any indirect vibration data that was coming from the turbines on time. Due to contingency mode, dispersion of sensors and diversity of data, he could not make an objective decision.

Even if he realized that sensors were showing anomalous behavior, he could not intervene to make decisions and actions with regard to turbine operation. There is also a possibility he did not have enough time to communicate the findings or did not have enough time to react.

Context in Which Decisions Are Made:

a. **Roles and responsibilities**

The head of the unit (42 years old) had only 2 months of experience at that position. It is most likely that as head of the service he had little sufficient experience or no training for such emergency situations.

b. **Environmental and behavior-shaping factors**

According to the Official Investigation Report (Rostekhnadzor), Turbine 2 operated outside the accepted limits 210 times, with a total of 2520 seconds, since the last most recent

maintenance that took place six months prior to the accident. Dangerous capacity fluctuation seemed to have been acceptable behavior.

On the day of the accident Turbine 2 changed its planned and emergent capacity 12 times. Between 23:14 of 16.08.2009 and 8:13 of 17.08.2009 such fluctuation resulted in six occasions when Turbine 2 operated outside recommended limits (Council of Federation, 2009a). It seems that on that day unacceptable capacity fluctuations were part of the contingency routine.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
The Chief SSHPS Engineer was called in at 6:35 am on 17.08.2009, i.e. 98 minutes before the accident (Council of Federation, 2009a). This means that people at Equipment Monitoring Services would have had a chance to inform management about Turbine 2's anomalous behavior at least two hours before the accident had vibration data existed.

Reasons for flawed control actions and dysfunctional interactions:
Head of Equipment Monitoring Services possibly understood that the problem was emerging, but could not imagine the gravity of the situation and had inadequate control mechanisms with which to respond.

Reliability and Technical Safety Service

Safety Requirements and Constraints:
The Head of Reliability and Technical Safety Service was responsible for both the safety of people at working at the station and the reliability and safety of equipment. However, the direct safety of personnel is not defined as a priority in his list of responsibilities.

Safety instructions for power stations and electricity grids are defined by decree of Russia's Ministry of Energy (2003). The list of responsibilities includes: maintaining operational-dispatch discipline; maintaining equipment in a state of operational readiness; providing efficient and reliable production of electricity; implementing industrial safety rules; providing uniform measurements during production; the transmission and distribution of energy.

Inadequate Control Actions:
Most workers who died at the station were not part of the station's core operational personnel. They were maintenance staff performing maintenance functions on the station's lower decks. The majority of casualties were employees of maintenance subcontractors. At the time of the accident there were about 300 people present at the station (Rostekhnadzor, 2009). The morning shift started its working day at the station at 8:00 am, just 13 minutes before the accident. Reliability and Technical Safety Service did not take any action that could have prevented people from starting their working shift.

Context in Which Decisions Are Made:

a. Roles and responsibilities

It is not clear who was responsible for the safety of station and subcontractor employees at the station.

The Head of Reliability and Technical Safety Service had more than 6 years and 8 months' experience in this position.

b. Environmental and behavior-shaping factors

A contingency situation initially emerged beyond the station's physical border, thus outside the area of responsibility of Head of Reliability and Technical Safety Service. As the situation emerged, personnel focused on the grid's emergency level. Attention and priority was given to stabilization of the regional grid system. Unacceptable capacity fluctuation of the turbine had happened before; these events were not considered extraordinary.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:

There was no clear delineation of responsibility for human safety by either The Reliability and Technical Safety Service or The Economic Security and Regime Service. The head of Reliability and Technical Safety Service was primarily concerned with the reliability of equipment. The head of the Economic Security and Regime Service, another unit created as part of the reforms at the station, was supposed to be responsible for emergency situations and the evacuation of people. He was not aware of the situation emerging at the station, however, and was outside the flow of information.

Reasons for flawed control actions and dysfunctional interactions:

Attention was focused on the emergency at the regional grid level. It did not occur to the heads of the Reliability and Technical Safety Service and the Economic Security and Regime Service, or to the station's Chief Engineer, to halt the working day until the situation became clear.

It is possible that the Head of Reliability and Technical Safety Service had not considered coupling problems between software and hardware or the possibility that such coupling would lead to devastating results.

Technological Systems Management Service

Safety Requirements and Constraints:

The Head of Technological System Management Service is responsible for Power Management and Process Control System of the station. His responsibility includes the following functions: guaranteeing synchrony and unity measurements of between generation; transmission and distribution of electricity; maintaining operational readiness; servicing and maintaining sensor systems; understanding behavior of the Power

Management and Process Control System; testing the system extensively during the testing and acceptance period.

Inadequate Control Actions:

a. Roles and responsibilities

It is unclear whether the Head of Technological System Management Service failed to properly record the anomalous incidents of system prior to the accident. It is also unclear whether this information was reported to management. After the accident, the Official Investigation Report found that in the total hours of operation since the last maintenance in March 2009, Turbine 2 operated outside the accepted limits 210 times, for a total of 2520 seconds (Council of Federation, 2009a).

b. Environmental and behavior-shaping factors

It is not clear whether the Head of Technological System Management Service was present, in any capacity, during the acceptance process of Turbine 2. Nor is it clear whether he was present for the testing and certification of the upgraded Power Management and Process Control System (GRARM) between March-July 2009.

The algorithm of the Upgraded Power Management and Process Control System was not synchronized properly with the turbines. The software developer did not consult the turbine manufacturer with regard to the turbine's specifications or its unique or faulty characteristics (Council of Federation, 2009b).

Context in Which Decisions Are Made:

The Head of Technological System Management Service (53 years old) had only 3 months of experience in that position. It is not clear whether he was fully familiar with the legacy of Turbine 2.

Turbine 2 was one of the earliest turbines commissioned for operational service. It began operating with a temporary runner on November 5, 1979 and a regular runner on November 7, 1986 (Rostekhnadzor, 2009). The turbine was experimental in nature and had only two safe regimes of operation. It had two safe zones that were recommended for operation. These were Load Zone 1: from 0 to 265Megawatt and Load Zone 3: from 570 to 640 Megawatt. There was also unsafe Load Zone 2 between from 265 to 570 megawatts (Council of Federation, 2009a).

The Turbine manufacturer was present at the station and provided technical support until the late 1990s. The manufacturer recommended that, while switching from one mode to another, the unsafe load zone should be passed very quickly to avoid increases in vibration. Adherence to these recommendations would preclude Turbine 2's inclusion in the Power Management and Process Control System (Council of Federation, 2009b).

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
As the Siberian regional grid level emergency became clear, the Head of the Technological System Management Service assumed the Power Management and Process Control System would regulate the active power load among operating turbines, while the distribution of reactive power would maintain maximum robustness. The mental model that the software system would balance emerging anomalies proved to be faulty.

Reasons for flawed control actions and dysfunctional interactions:
The Head of the Technological System Management Service possibly understood the gravity of the emerging situation, but could not interfere in the process since his functions were secondary to the Operations. He assumed that Operation Service and the Siberian Dispatch Service had the same amount of information.

4.3 Third level of operations: Power Management and Process Control System

Safety Requirements and Constraints:
In 2005 the Sankt-Petersburg-based company called *Rakus* began the large-scale modernization of the automated process control systems (APCS) Sayano-Shushenskaya and Mainsk HPS with Siemens Solution Partner Automation.

A key element of the Power Management and Process Control System is the Group Regulator for Active and Reactive Powers (GRARM), which was developed by its subcontractor *Promavtomatika*. GRARM function was configuration and distribution of the planned and unplanned loads that come through the Automatic system for regulating frequency and power from the Siberian Unified Grid System Dispatch. The system is supposed to calculate the load of new order that comes from the dispatch center and distribute this load between individual regulator units at each of the station's turbines.

Inadequate Control Actions:
According to the Parliamentary report there were mishaps and diversions during different stages of software development. The requirements of the new software system were not consented to and approved by *Lenhydroproject*, the station's general designer.

During the developmental stage the system's design, structure and specifications were subject to many iterative changes. The Parliamentary report stresses that the Power Management and Process Control System specifications included only control and visualization of the turbine's vane position. The specifications did not include scenarios in which the turbine's vanes are desynchronized. Another omission pointed out by the report was the absence of reserve/alternative sources of power supply for the Power Management and Process Control System (Council of Federation, 2009a).

With regard to GRARM, the Parliamentary report indicates that system requirements were developed by station personnel, and did not include (1) criteria for developing functional priorities for turbines operating under GRARM, (2) individual load limits and unsafe mode

regimes for each turbine, (3) the individual characteristics and structure of each turbine. Moreover, there were no criteria for selecting priority turbines and no time limits for such priority to remain active. The impact algorithm on GRARM that served as an interface with the automatic frequency control system was not consistent with the turbine manufacturer's requirements.

As mentioned before, one of the new and unique improvements of the overhauled Turbine 2 was introduction of management systems for individual servomotors. This allowed for individual hydraulic actuators for each turbine blade, which was a technology that had not been used before (RusHydro, March 23, 2009).

Context in Which Decisions Are Made:
In 1998 the original Soviet-made automated system was discharged as "morally obsolete" due to increased number of failure occurrences and absence of the service suppliers (Rostekhnadzor, 2009). Decommission of the original software led to fragmentation of the command and control systems, in particular synchronized water discharged functions for both SSHPS and the Mainsk HPS, located downstream, which now had to be managed separately.

The new GRARM was accepted into testing mode in 2006 and, after six months, into operational mode. 2006 was the last year when developers from *Promavtomatika* visited the station. Later that year individual regulators, with whom GRARM was connected, were replaced by the SSHPS personnel without the technical assistance of its subcontractor.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
Initially the GRARM was developed as a monitoring and visualization program and did not include safety functions in the case of anomalous behavior of the station's turbines.

GRARM had no safety functions. The system was not obligatory, and SSHPS could have operated with GRARM turned off. In fact, when the operator at the Siberian Unified Grid System Dispatch required GRARM to be turned off, he would give shutdown commands to the SSHPS operators.

It is important to stress that station personnel had reported several incidents with GRARM. Such incidents included unsanctioned by the regional dispatch access to the system and drops in power load (Council of Federation, 2009a). There were some attempts made to add safety features to protect the system from unauthorized access. However, such attempts were unsystematic, fragmentary and did not address GRARM's core technical specifications.

Reasons for flawed control actions and dysfunctional interactions:
The Parliamentary report states that the original design of the Power Management and Process Control System had a safety function that would give shutdown command to turbines. There was also an option to imbed a preventive alarm system. However, after

testing the system, it was kept in a purely informative mode. We can assume the reason the alarm system was turned off was that it would have shut down the turbine every time it passed through the unsafe load zone (from 265 to 570 Megawatt) (Council of Federation, 2009a).

In addition, there was no vibration data input into the GRARM system. Since the system had no criteria for turbine prioritization, vibration data would not have made any difference. However, if the system had been structured to include a prioritization algorithm, a vibration input and a preventive alarm system, operators would have had a better understanding of the emerging situation.

The fact that the system allowed simultaneous operation of turbines under GRARM and in a manual mode led to additional complexity for SSHPS operators. At the moment of the accident, 6 turbines were under GRARM and 3 were operated manually.

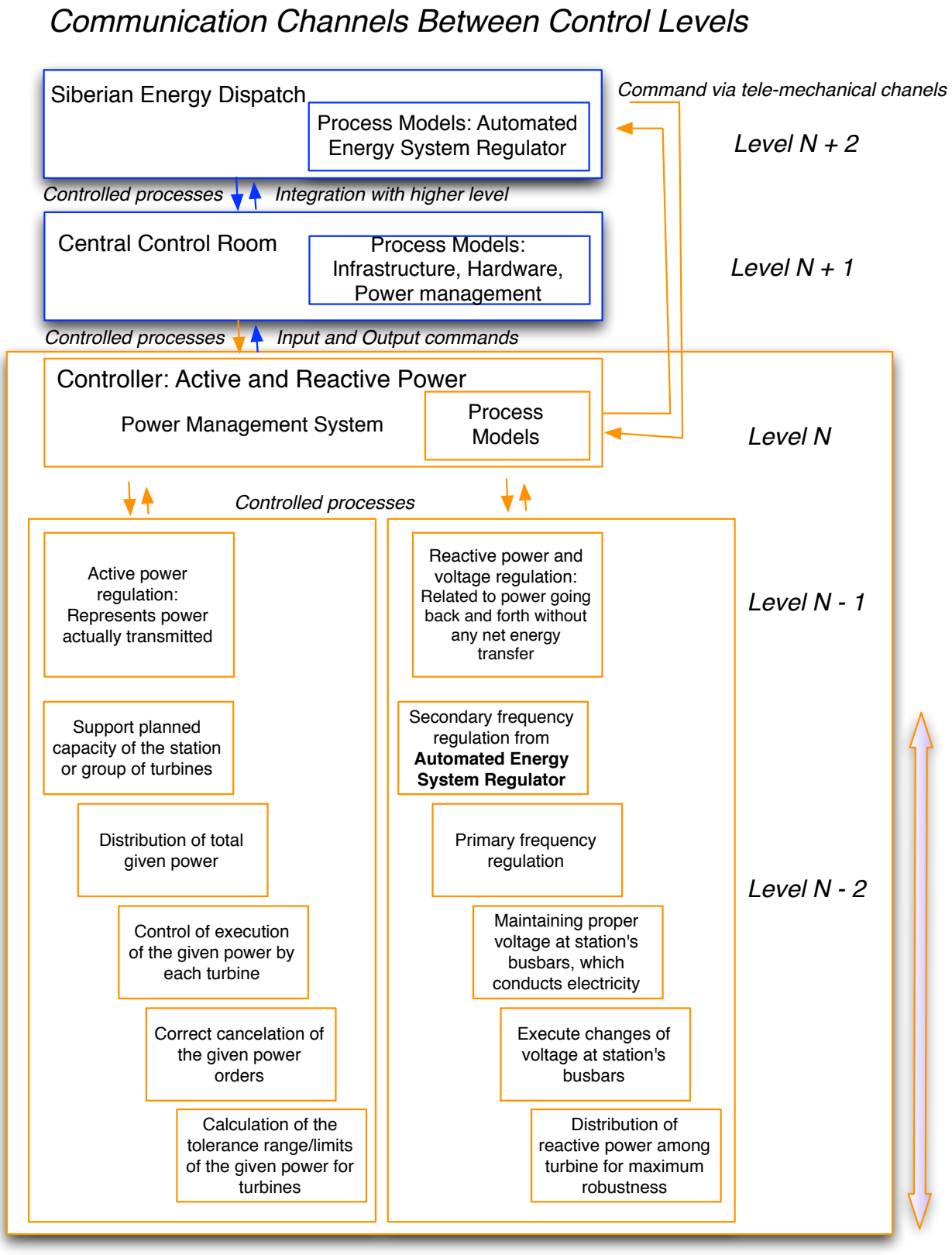

Figure 9: Description of Group Regulator for Active and Reactive Powers (GRARM)

4.4 Fourth Level of Operations: Management of the Station

Deputy Chief Engineer for Operation

Safety Requirements and Constraints:
The Deputy Chief Engineer for Operations oversees Operations Service, Equipment Monitoring Services (which include the electro-technical laboratory, the laboratory for technical diagnostics and laboratory for hydro-technical structures), the Mainsk hydro structure (located downstream from the main station), and the Technological System Management Service.

Inadequate Control Actions:
As the key manager responsible for operations the Deputy Chief Engineer for Operations had to aggregate information that was arriving prior the accident from the different station units that reported to him. The key information junction was between Operation and Monitoring Services. Fragmented information generated by these two services had to be put together into one complete picture of the problem emerging at the station.

Context in Which Decisions Are Made:
The Deputy Chief Engineer for Operations was a 55 year-old engineer with 3 years and 7 months of experience in that position.

He and the heads of subordinate services seems to have given their main attention to the situation emerging on the grid level, i.e. in the interaction between the station and Siberian Dispatch Center level.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
Information and data generated by the monitoring service were not given proper attention. At this level of control, the management must have had a complete picture of the emerging situation. The Deputy Chief Engineer for Operations had authority to intervene into the operations of his services and those of the regional dispatch center to adjust their decisions and actions.

Reasons for flawed control actions and dysfunctional interactions:
It seems that, instead of making independent decisions, the Deputy Chief Engineer for Operations chose to inform the Chief Engineer, his direct superior. The most likely explanation for such action was the unusual nature of the emerging situation, as well as an underestimation of the magnitude and scale of the possible accident.

Deputy Chief Engineer for Engineering

Safety Requirements and Constraints:
The Deputy Chief of Engineer for Technology is responsible for the Production and Technical Service and the Maintenance Planning and Preparation Service.

The Deputy Chief of Engineer for Technology is responsible for evaluating station conditions, planning overhaul arrangements and measures, and commissioning the overhaul execution.

Inadequate Control Actions:
The actual maintenance service and its resources were separated from the station. These services were organized into a subsidiary company that had to build its relations with SSPHS through outsourcing contracts. Basic routine maintenance interaction within the station was transformed into contractual relations between so-called core and non-core actives.

Context in Which Decisions Are Made:
Making maintenance and overhaul non-core activities of the SSHPS was part of the introduction of new corporate practices.

The Deputy Chief of Engineer was a 54 year-old engineer with 2 years 5 months of experience in his position. That means he was present during the acceptance of the intermediate overhaul of Turbine 2 and the introduction of the Power management software program in spring 2009.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
It is not clear why station personnel – who understood the limitations of Turbine 2 - would make it a priority turbine in the Power Management and Process Control System, which was managed by the Siberian Regional Dispatch Center.

Reasons for flawed control actions and dysfunctional interactions:
Complacency, and the belief that existing technology was reliable, led to a major accident. After the accident, the official investigation report found that in the total hours of operation since the last maintenance (in six months of March 2009) Turbine 2 operated outside the accepted limits 210 times, for a total of 2520 seconds (Council of Federation, 2009a). These violations all took place under this Deputy Chief of Engineer for Technology.

Chief Engineer of the SSHPS

Safety Requirements and Constraints:
The Chief Engineer, along with two of his deputies, had a complete or holistic picture of the emerging situation. The Chief Engineer had authority to communicate with the Regional Dispatch center and question its decisions and commands.

The Chief Engineer is responsible for overall station safety; he directly supervises the Reliability and Technical Safety Service.

The two deputies mentioned above report to him directly, which means that issues of maintenance, modernization and acceptance of new or overhauled systems take place under his direct supervision.

Two additional critical functions that had to be monitored by the Chief Engineer were (1) development, acceptance and enforcement of functional instructions performed by his deputies and the station's services and (2) education and training of the station's personnel, given the fact that the majority of management had limited experience.

Inadequate Control Actions:
The Chief Engineer had limited authority with regard to the station's financial planning. In other words budgetary resources that were at the disposal of the SSHPS management could not have matched modernization and maintenance needs. Rather it would have required an investment program approved by RusHydro's headquarters.

While it is not clear why Turbine 2 was put into priority mode for the regional dispatch center, this decision was made before his arrival at the station.

Context in Which Decisions Are Made:
The Chief Engineer of the SSHPS was called in at 6.35 of 17.08.2009, i.e. 98 minutes before the accident (Council of Federation, 2009a). Turbine 2 was already in operation and the first signs of anomalous behavior were obvious. The Chief Engineer was 58 years old, with 3 years and 9 months of the experience in this particular position.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
According to the Parliamentary Report, the Chief Engineer had to stop Turbine 2 as soon as it was clear that the turbine's vibration was reaching unacceptable levels (Council of Federation, 2009a). Instead the turbine remained in the priority mode. It seems that the accident took place as station personnel were trying to manually slow Turbine 2.

Reasons for flawed control actions and dysfunctional interactions:
It is unlikely the Chief Engineer did not have enough authority, information or time to aggregate available information to make his decision.

However, it was not clear if the decision to shut down Turbine 2 would affect the total generated output of the SSHPS. In other words, it is not clear if the Power Management and Process Control System allowed stopping the turbine independently from the other 5 turbines of the station that were managed by the Siberian Unified Grid System Dispatch. Total shutdown of the station could have affected the stability of the Siberian Regional Energy Grid System, which eventually happened after the explosion of Turbine 2.

One of the key consumers of electricity in the Siberian Energy System is Russian Aluminum (RUSAL), which is the world's key aluminum producer, as well as a key stakeholder in both RusHydro (owner of SSHPS) and IrkutskEnergo (owner of Bratsk HPS). The accident at the

station affected several of RUSAL's aluminum smelters (Khakass aluminum processing plant, 480 Mw; and Sayan aluminum processing plant, with 1040 Mw).

Director of the SSHPS

Safety Requirements and Constraints:
The Station Director understands SSHPS strategy as well as SSHPS's role and importance within the RusHydro holding. His responsibilities include: station safety and development of contingency scenarios for emergency situations; development, acceptance and enforcement of functional instructions performed by his deputies and the station's services; education and training of station personnel, given the fact that majority of management had limited experience.

Inadequate Control Actions:
It appears likely that his budget planning, acquisition and contractual authority were diluted by the holding's head office in Moscow. Major maintenance and overhaul projects conducted at the station were organized by the holding's Moscow headquarters, while station's maintenance units were removed from the station and organized into a separate subsidiary after being reclassified as non-core activities.

Context in Which Decisions Are Made:
The Director delegated most responsibilities for daily operation of the station responsibility to the Chief Engineer. The assumption of most of the director's managerial responsibilities by company headquarters gradually led to a state of complacency.

The director was a 56 year-old engineer with 2 years and 8 months of experience at the position. At the time of the accident he was absent from the station.

The day of the accident was the Director's birthday.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
It is not clear why the Director did not arrive at the station before or immediately after the accident. He was not able to maintain a line of communication with regional emergency services. It took another 40 minutes for station management to inform regional emergency services about the accident. Emergency services were told about a moderate accident; the first crews to arrive on the scene were thus unprepared.

The Director did not understand that the station's design did not include an alternative power source for the emergency closing valve. The valves had to be closed manually as Turbine 2 exploded. The station's design did not separate turbines in safe blocks as on nuclear stations. No adequate emergency planning or training was conducted.

Reasons for flawed control actions and dysfunctional interactions:
It seems that the Director of SSHPS misunderstood or refused to accept the accident's catastrophic scale. He delayed responding to the emerging situation, and delayed informing

authorities as well. He also initially reported the accident as a limited incident. It is also likely that he underestimated the number of casualties, since the majority of the casualties were from the station's maintenance subsidiary.

4.5 Fifth Level of Operations: Siberian Unified Grid System Dispatch (SUGSD)

Operational-dispatch management is regulated by Russia's Federal Electricity Energy Law. It is a set of measures for centralized management of technological modes of power-generation facilities and power-receiving electricity consumers (Russian Federation, 2003).

The system operator is a specialized organization responsible for centralized operational dispatch management within the domain defined by the Unified Energy System of Russia. The system operator is responsible for issuing mandatory dispatching commands and orders to electricity generators and electricity consumers (Russian Federation, 2003).

SUGSD is responsible for (1) ensuring the balance of power production and consumption, (2) ensuring hierarchical principles in which level subjects of the system are subordinated to higher-level dispatched subjects and commands, (3) unconditional execution of load-controlled, dispatching commands and orders given by dispatching management to electricity generators and consumers of the system, (4) implementation of measures aimed at ensuring safe operation and preventing emergency situations, (5) taking measures aimed at ensuring Unified Energy System of Russia's normalized reserve-generating capacity (Russian Federation, 2003).

Inadequate Control Actions:
Power Management and Process Control System (PMPCS) at SSHPS did not include any safety mechanisms in its specifications. Turbines cannot be started and stopped from SUGSD; they could be started manually at the station. SUGSD had no information on the engineering status of hardware or software at the SSHPS (Council of Federation, 2009a).

Context in Which Decisions Are Made:
According to the Official investigation report, the SSHPS and SUGSD did not share or exchange information on either the specifications of the Power Management and Process Control System or the engineering status of the station's turbines (Rostekhnadzor, 2009).

At the time of the accident the dispatch center managed 6 turbines via the Power Management and Process Control System and the station's operators managed 3 turbines manually.

The situation emerged in between midnight and early morning, with the most critical period around 7.30-7.45. There is no information when operators' working shift took place.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
The operator at SUGSD gave general commands to PMPCS, not to particular turbines. The operator at the dispatch center had no information about increased vibration and unsafe modes of Turbine 2. He or she had no data or reasons to respond to any anomalies in power fluctuations by changing frequency and energy generation.

Reasons for flawed control actions and dysfunctional interactions:
The operator's major priority was to maintain stability in the energy system, which he or she did. The operator was preoccupied with the emergency situation (fire and loss of communication) at the Bratsk HPS, and dispatch commands to the SSHPS were made to solve the problem on the level of the Regional grid to maintain system stability. The reliability and safety of any particular turbine was not the operator's responsibility and such responsibility was not part of the operator's mental model.

4.6 Sixth Level of Operations: RusHydro Management

Safety Requirements and Constraints:
RusHydro ranks second among the world's top 50 most rapidly developing energy companies, just behind Ultrapar Participacoes SA, Brazil. (RusHydro, November 3, 2010) According to its strategy, the company anticipates industry consolidation trends, in which "the shortage of public financial resources necessitates a large-scale investment program to be implemented by industry entities, creating prerequisites for a consolidated management system" (RusHydro, June 16, 2010).

In terms of safety requirements and constraints, its management aims to: maintain information about the economic and physical security of RusHydro; develop uniform technological policy in regard to automatic process control systems, automated power management and communication systems; achieve control over implementation of production program and engineering policy of its subsidiaries; develop comprehensive plans for R&D, maintenance, modernization and investment; control and monitor the lifecycle of critical systems and equipment, including standardization and updating corporate instruments with key indicators that can allow conducting lifecycle monitoring; develop and implement optimal modes for its hydro resources and electricity generation; develop an information stream for data in its hydroelectricity operations; and conduct technical audits and inspections of subsidiaries.

Inadequate Control Actions:
The state holding was built and operated as a top-down corporation. There seemed to be a mismatch between declared goals and the company's Key Performance Indicators (KPI) that were approved by Board of Directors of the Company (RuStocks.com, October 31, 2008). Until 2009 RusHydro's KPI were focused on the company's financial and economic effectiveness. Salary, non-monetary benefits, and management bonuses were based on meeting KPI (RusHydro, 2009).

"KPI performance calculation and assessment are carried out in accordance with RusHydro's Procedure for KPI Performance Calculation and Assessment approved by a resolution of RusHydro's Board of Directors on 26.09.2008 (Minutes No. 62) with subsequent amendments (resolutions by RusHydro's Board of Directors on 24.12.2008 (Minutes No. 69) and on 11.05.2010 (Minutes No. 97)." (RusHydro, December 24, 2008)

It was not possible to find the 2008 KPI Procedures (Minutes No. 62). However, from a secondary source we may conclude that these KPI Procedures did not include reliability and safety issues (Council of Federation, 2009b). At the end of 2008, the Board made a decision to acquire civil liability insurance for operators of hazardous industrial facilities and hydro generating installations (RusHydro, December 24, 2008). Basically the Board made financial decisions to mitigate possible and/or emerging engineering problems.

Context in Which Decisions Are Made:
The holding was established in 2004 as a spinoff from Russia's energy monopoly as the result of deregulation reforms. It manages 20 branches and 48 other subsidiaries.

Introduction of corporate management emphasizes centralization of financial flows as the holding's major goal of increasing market value. Market value is the company's key measurement of success. As of July 3, 2009 the group's market capitalization was USD 10 billion. By the end of 2009 the total installed hydropower capacity was 25,336.6 Megawatt.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
Geographical dispersion of RusHydro's assets and infrastructure are the company's most obvious challenges. Regional and engineering differences made it difficult to impose comprehensive standards on all holding sites. Its hydropower plants are different in size, age, power generation and relation to downstream consumers of electricity. There were also differences in regional priorities. For example, infrastructure in Siberia is relatively modern compared to Russia's other regions and demands a unique approach given the fact that RusHydro stakeholder's (RUSAL's) major assets are located in the Siberian region. The priorities that the Board had to face were aimed at new mega projects in Siberia rather than maintaining existing infrastructure.

Reasons for flawed control actions and dysfunctional interactions:
In 2008 Standard & Poor published its Corporate Governance Score on RusHydro. According to this report the company had CGS-5+ or "moderate corporate governance processes and practices overall. A company in these scoring categories has, in Standard & Poor's opinion, weaknesses in several of the major areas of governance analysis" (Standard&Poors, 2008).

The report stressed a number of weaknesses, which did not include issues of safety or reliability, but rather concerns about government interference in the company's business:

1. There are risks that the government may require RusHydro to engage in commercially unattractive projects that serve strategic and social goals. These risks

are only partially compensated by the presence of a constructive dialogue between the company and minority shareholders.

2. The board of RusHydro does not include a significant independent element, which limits its ability to mitigate risks associated with the government's influence (Standard&Poors, 2008).

In the corporate culture there is a general understanding that technical regulations and safety issues are "administrative barriers" for efficient operations. Whereas maintenance and capital repair was perceived from a purely financial planning perspective, rather than with regard to the technological lifecycle.

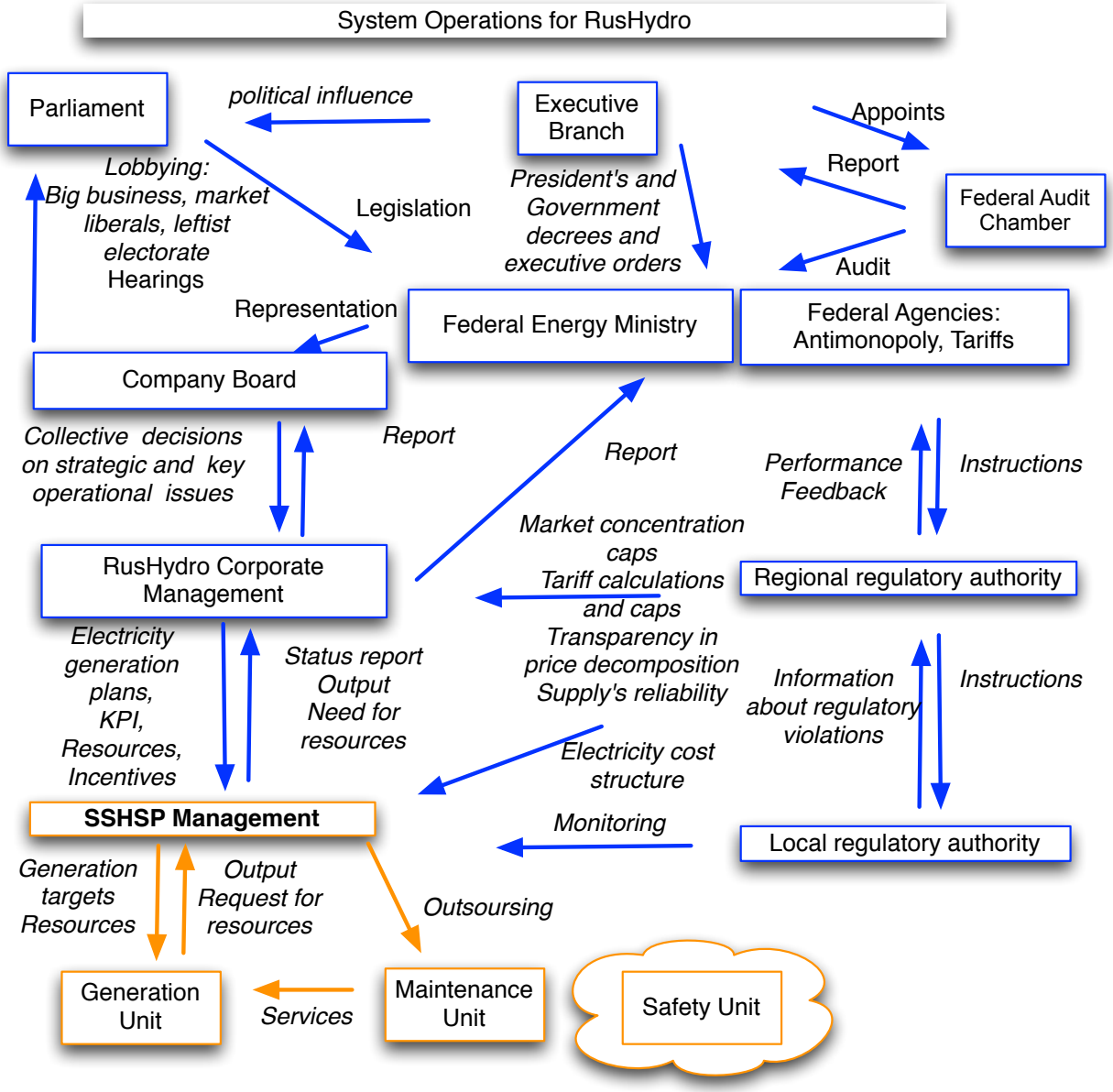

Figure 10: System Operations for RusHydro

4.7 Seventh Level Operations: Siberian Inter-Regional Office FSETAI

Safety Requirements and Constraints:
Three Federal Laws guide the Federal Service's activities in the electricity generation sector: The Law on Industrial Safety (Russian Federation, 1997) (Articles 9 and 10) lists a wide range of requirements for organizations and personnel that operate hazardous facilities. It also outlines readiness measures for containing possible emergencies.

The office conducts technical and other inspections in nine major areas, including the safety of power systems and of hydro technical structures. The Siberian Inter-Regional Office was created in 2004 as part of program of the constitutional reforms that introduced Federal districts, an intermediate administrative structure between regions and Moscow.

Inadequate Control Actions:
There are two other Federal Laws that regulate activities of hydropower stations: The Law on Safety of Hydro Technical Installations, and The Electricity Energy Law. The Law on Safety of Hydro Technical Installations addresses safety of hydroelectric power stations, spillways, water outlet structures, etc.; it is enforced by the Ministry of Natural Resources. Additionally, the Electricity Energy Law (Russian Federaion, 2003) covers issues of operational licensing, operational-dispatch structure, and government regulation of the electricity market. It is in the domain of the Ministry of Energy. In addition, the Federal Audit Chamber investigates activities of state-run companies and federal government-funded projects (Beskhmelnitsyn, 2009).

Due to such legal overlap, federal inspectors rarely exercise their authority to stop production processes. Inspection results can be challenged through Federal offices or courts. Inspections can be conducted only on annual basis; some findings are made in the form of recommendations.

Context in Which Decisions Are Made:
The Siberian Inter-Regional Office watches over 12,210 businesses and organizations which manage hazardous industrial facilities, 329,511 electricity consumers, 138,958 heating energy consumers, 127 hydro technical structures, 11,029 facilities that are subject of environmental monitoring.

Dysfunctional interactions, failures, and flawed decisions, leading to erroneous control actions:
Two hydro power stations and the Siberian Dispatch center were under the authority of three different sub regional inspection units of the Federal Service. Thus, until the accident, the possibility of a complex, multi-party failure was not considered a hazardous scenario.

More importantly, inspectors did not inspect hydro turbine units since they were not categorized as hazardous industrial facilities. In 2007, the Federal Audit Chamber's Analysis of the Impact of Investment Programs of The Electricity Energy Sector pointed out that the "wear of certain types of hydraulic equipment - hydraulic turbines, hydro generators and hydro - exceeded 60% and reached a critical level" (Beskhmelnitsyn, 2009).

However, technical modernization was addressed as an investment problem that RusHydro had to solve with increased state and internal investment.

Reasons for flawed control actions and dysfunctional interactions:
The station's design and possible flaws derived from the design were not subject to revision. Power Management and Process Control System (and interaction between several facilities) was never considered a hazard and never inspected as one complex system. We cannot say that modernization was not in RusHydro's agenda. However, problems of aligning infrastructure had to compete with new infrastructural projects (such as the construction of the Boguchansk Hydro Power Station) for funding and wait in the holding's "investment queue."

As we mentioned previously, corporate culture frequently perceived technical inspections as bureaucratic and administrative barriers to efficient operations. Such issues had to be fixed quickly, using shortcuts rather than long-term solutions.

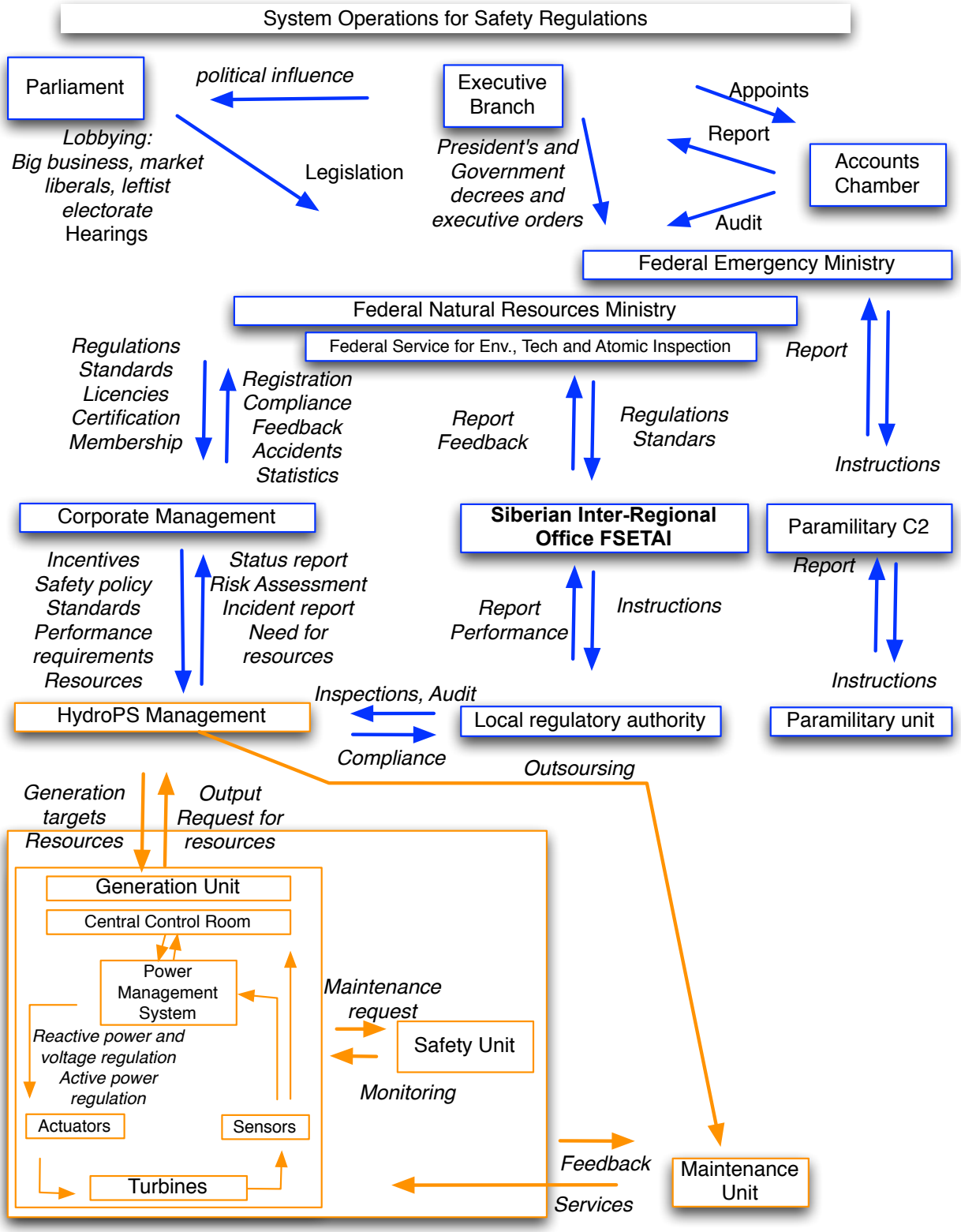

Figure 11: System Operations for Safety Regulations

Chapter 5. Socio-Technical Landscape and Systemic Factors

"The only relevant learning in a company is the learning done by those people who have the power to act" (Arie P.De Geus).

The goal of this chapter is to briefly describe the evolution of the Soviet—and, later, Russia'— electricity sector before and after 2000. For this purpose I will present two causal-loop diagrams comparing and contrasting Soviet central planning environment and the market-driven environment of present Russia.

I will identify, describe and compare the key dynamics of interest to this research. Unfortunately the scope and availability of data do not allow building an actual system dynamics model. Such a model will require extensive research capabilities that are presently unavailable.

In this chapter I also will map decision-making and legislative processes in Russia; the evolution of the regional governments' role in public utility management; the fundamental role of the electricity generation sector in Russia's economy; an overview of ten years of liberalization reforms in the sector, and its future perspectives; and delays resulting from tensions between the dynamics of Russia's legal and regulatory environments.

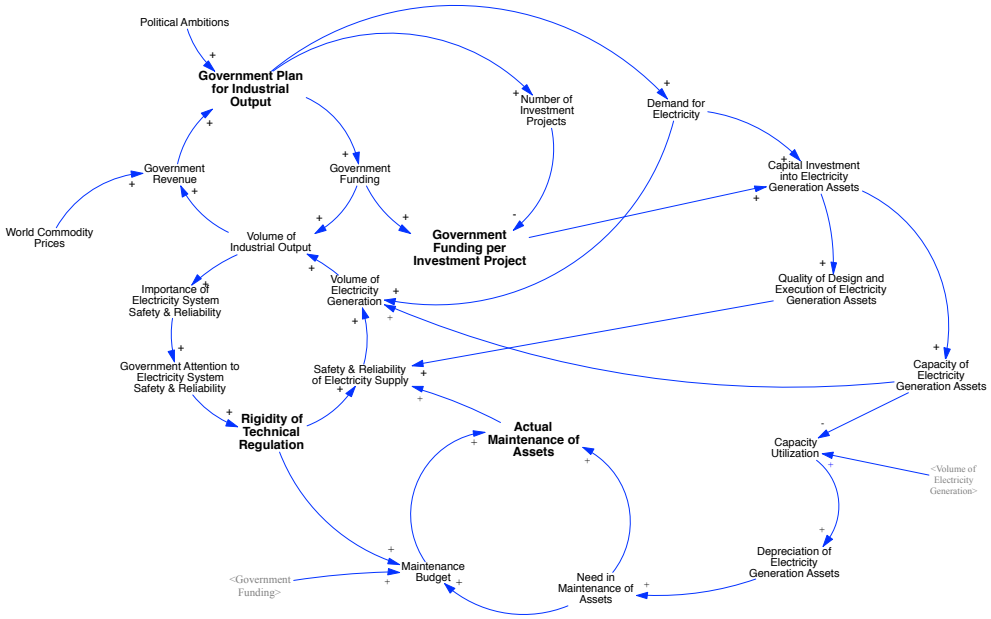

Figure 12: Central Planning

In one paragraph this history can be summarized as evolution from (1) the central planning and rapid industrialization of the first half of the twentieth century; (2) to expansion, overinvestment and misinvestment of the second half of the twentieth century, (3) to unsystematic privatization and chaotic liberalization of an undermanaged infrastructure from1992-2008.

From a technical perspective, evolution of the system has been broken down into four functional elements: Generation, Transmission, Distribution, Supply and Tariff-setting regime. Later in this chapter I will present more a detailed overview of this transition. Let us start with the Central planning environment.

5.1 Central Planning: Controlled Environment of the Past

The electricity generation sector, which is the backbone of the Soviet economy, remained the country's most reliable industry. The system dynamics causal loop diagram describes key variables of that model in more details. Let us look at the four major causal loops in the diagram:

Government Driven Electricity Output Growth

The State was the primary force that pushed demand for electricity and investment into its infrastructure. Five-year development plans, driven by the political priorities of the Communist Party, set the stage for the nation's Industrial Development, or what we call *Government Plan for Industrial Output*. Execution of the Government's plan led to an increased *Electricity Demand* and required an increase in *Electricity Output*. In those instances where existing capacities did not satisfy growing demand, *Capital Investment into Electricity Generating Assets* had to be made. This process led to increase in *Capacity and Volume of Electricity Generation*, and reinforced increase in *Industrial Output* (see figure below).

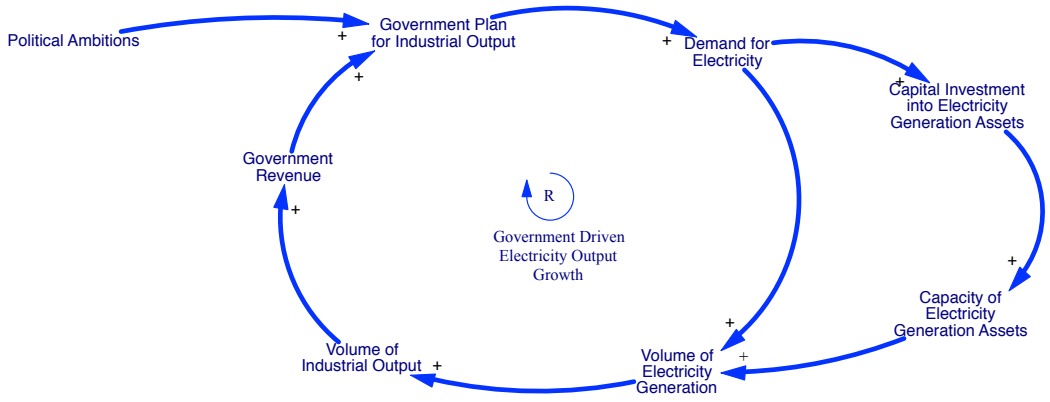

Figure 13: Government Driven Electricity Output Growth

Overstretching Government Resources

The Government Plan for Industrial Output led to an increase in the *Number of Investment Projects.* This increase led to competition for limited resources among administrative regions, state industries, ministries and projects. With the increase in the *Number of Investment Projects* (nation-wide projects), *Government Funding per Investment Project* dropped.

Capital Investment into Electricity Generation Assets had to be stretched over time and space. In the case of SSHPS, the total time of station construction took twenty-seven years (start in 1963, testing mode in 1978, full functional mode 2000) (Rostekhnadzor, 2009). Deficit in capital led to compromises in *Quality of Design and Execution of Electricity Generation Assets.*

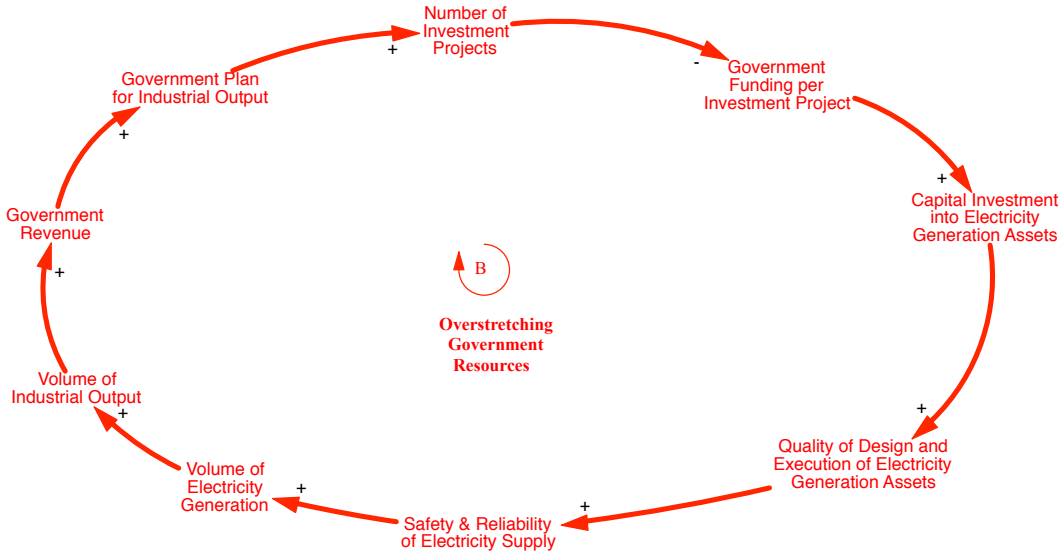

Figure 14: Overstretching Government Resources

Compromises in the quality or completeness of the original design led to decreases in *Safety and Reliability of Electricity Supply*. As mentioned in Chapter 3, prior to the 2009 accident, SSHPS had experienced three major (and several minor) accidents, most of which were related to seasonal flooding. These problems could have been avoided with the operation of the alternative spillway. The spillway could have given immediate and long-term backing to SSHPS at the time of the latest accident. After the accident the water had to be discharged through an emergency spillway, which affected the structural integrity of the station's dam.

Due to financial difficulties the construction of the alternative spillway was started only in 2005. At the time of the 2009 accident it was not yet completed. An emergency discharge through an alternative shore spillway could have helped localize the accident in a shorter period of time. Two months after the accident, the Russia's Prime Minister allocated 115 million USD to complete the spillway (RIA Novosti, September 8, 2009).

Rigidity of Technical Regulations Ensures Safety and Reliability

In Chapter 2, I gave a brief overview of the Reliability Theory school in the Soviet Union that had to satisfy the development of Soviet civil and military industrial complex. In our diagram, the *Rigidity of Technical Regulation* comes about as the result of *Government's Attention to Safety and Reliability*. With high rigidity comes high *Safety and Reliability of the Electricity Supply*.

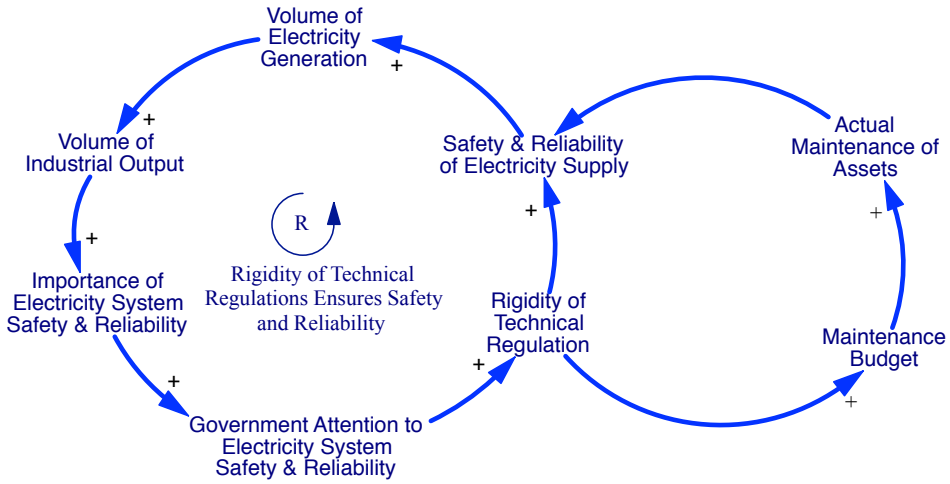

Figure 15: Rigidity of Technical Regulations Ensures Safety and Reliability

In our particular example of the Siberian Regional Energy Grid System, a stable and reliable supply to aluminum and other smelters was vital for the national economy. Increase in *Volume of Electricity Generation* resulted in higher industrial output. The stability of industrial output, and the upward dynamics of its volume, stressed the importance of *Electricity System Safety and Reliability* for the national economy.

On the left side of the main loop, we can see two other important variables. *Rigidity of Technical Regulation* pressured Soviet management to allocate the necessary *Maintenance Budget*, which in its turn led to an increase in the actual maintenance work conducted for the sake of safety and reliability.

1.4 Timely Maintenance Ensures Sustainability of the Infrastructure

The last but not least important loop of the model of the Russia's electricity sector is its sustainability loop, in which *Capacity Utilization* increased *Depreciation of the Electricity Generation Assets* and subsequently the need for maintenance. All other things being equal, we assume that the need in maintenance led to higher safety and reliability through increases in *Maintenance Budget* and *Actual Maintenance Of Assets.*

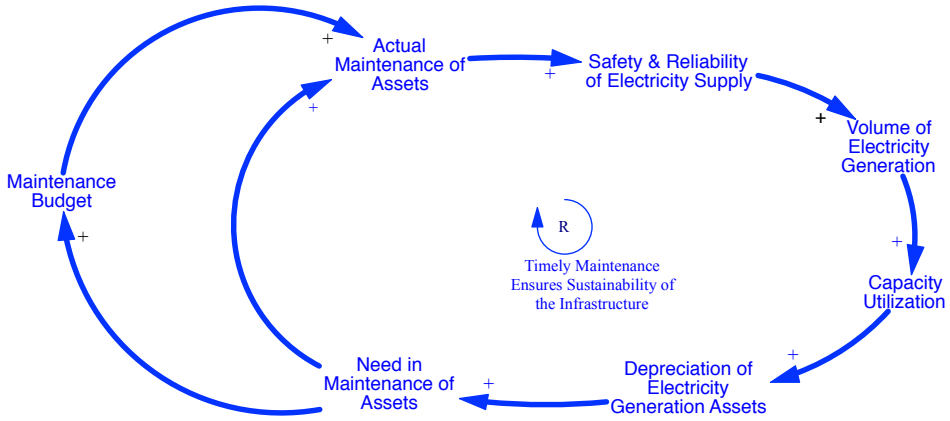

Figure 16: Timely Maintenance Ensures Sustainability of the Infrastructure

Of course if one would like to make the model more complex, it can be argued that, with the constant expansion of the electricity sector, the government had to decide whether to spend money on maintenance or capital investment. Moreover, expanded infrastructure requires increases in maintenance budget, in which internal completion leads to an overstretching of resources. The same dynamics as described in 5.2, above, concerning Overstretching Government Resources, with the difference that instead of capital investment one can plug-in the maintenance budget.

So by combining these four major causal loops we have a model that is characterized by heavy government intervention in priority formulation and interest in high industrial output, as well as high capital and maintenance investment and rigid technical regulations. The model's major flaw is that when politically driven goals and priorities are not under control, model dynamics could lead to the system's overexpansion (overinvestment). This in turn places additional burden on existing projects in terms of maintenance, and on projects under construction in terms of completion and completeness.

The extent of the transition process of Russia's electricity sector (1992-2008) is so broad, that it could distract us from the main purpose of this chapter. The chronology and key facts of the transition are given as an attachment at the end of the chapter.

5.2 Formation of Hybrid System

Let us now look at the current state of Russia's electricity sector. In order to make the model more relevant to the thesis, I have introduced several variables that are related to Aluminum production.

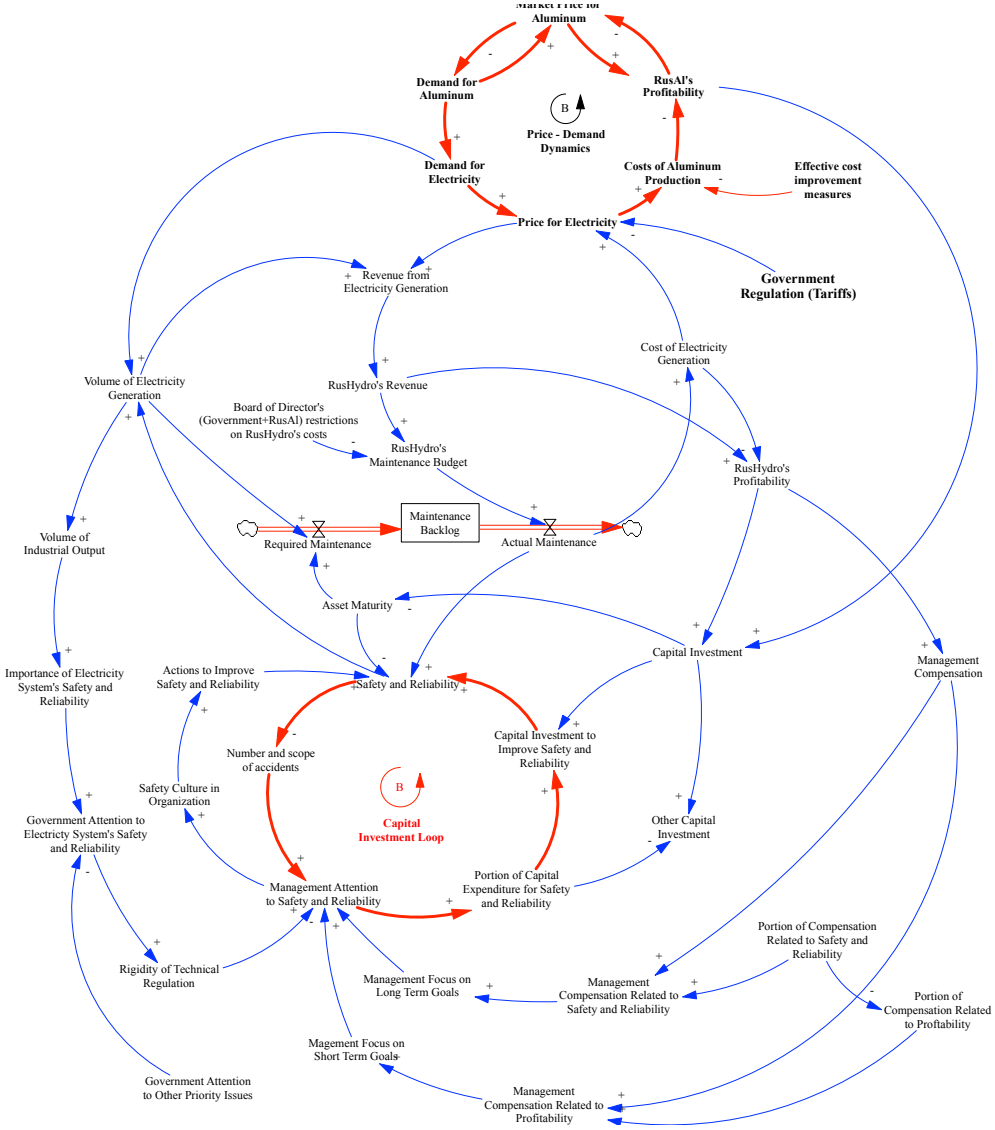

Figure 17: Hybrid System of Russia's Electricity Sector

Dynamics of Electricity Price

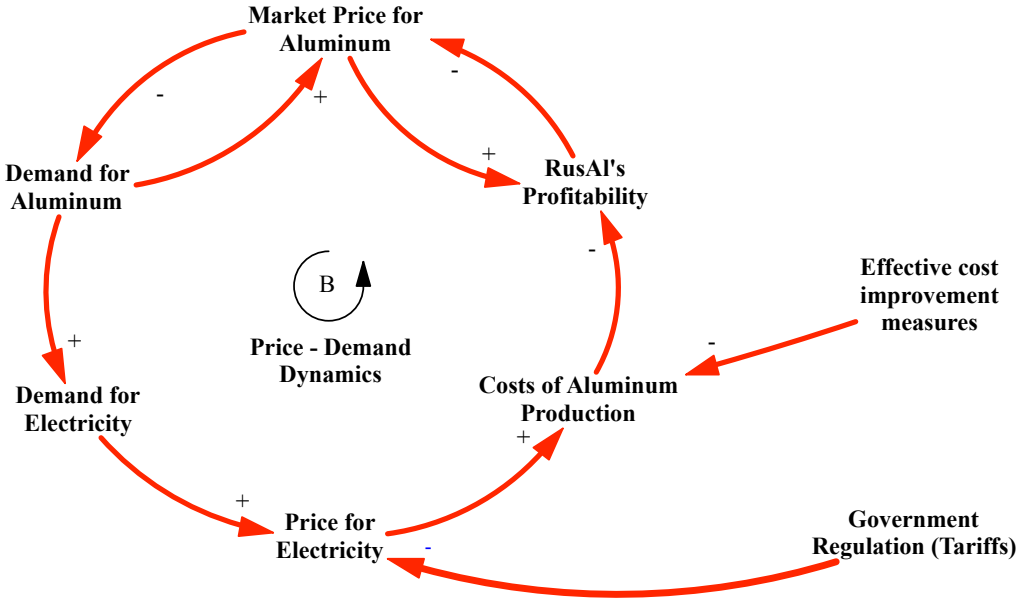

Figure 18: Dynamics of the Electricity Price

In our model Price for Electricity is one of the critical elements of the equation. Electricity generated by the hydroelectric station plays a critical role in the cost structure of the aluminum production—the lower is the price of electricity, the more competitive aluminum is on the global market. Aluminum cost is directly connected to *RUSAL's Profitability.*

Another important (but external to our model) variable that can decrease the *Cost of Aluminum Production* is *Effective Cost Improvement Measures.* However, improvements are usually costly and time-consuming vis-à-vis water discharge at a hydropower plant.

Market Price for Aluminum and *Demand for Aluminum* are two interdependent variables. In a market economy *Demand for Aluminum* dictates *Demand for Electricity*, in its turn electricity demand determines *Price for Electricity*.

In the Hybrid Model we have the co-existence of market and non-market factors. In this particular loop, we have *Government Regulation* in the form of tariffs for electricity generation and transmission that cap the price for electricity for its own reasons, which could range from goals such as increasing GDP or the employment of workers at aluminum smelters.

Capping the cost of electricity actually helps to increase RUSAL's profits, which in its turn could help RUSAL achieve its investment obligation towards the Russian government to build new Boguchansk HSP (RIA Novosti, August 2, 2010).

Capital Investment Loop

In the Hybrid Model, the state steps down from maintaining *Safety and Reliability*. It now becomes the responsibility of the semi-governmental/semi-private holding (RusHydro).

RusHydro management paid attention to issues of safety based on their awareness of the *Number and Scope of Accidents*, i.e. the higher the number of accidents and the larger the scope of such accidents, the greater the *Management Attention to Safety and Reliability.*

RusHydro is a young holding (established in 2004) which manages 20 branches and 48 other subsidiaries spread across Russia's climatic zones. These sites are different in capacity, technological maturity and their numbers of electricity consumers. The holding has integrated different entities that were never part of a single technological process. As a result, the holding's Moscow-based headquarters have a short institutional memory when it comes to safety and reliability. Lack of attention from headquarters resulted in low *Capital Expenditure for Safety and Reliability* vis-á-vis *Other Capital Investments.*

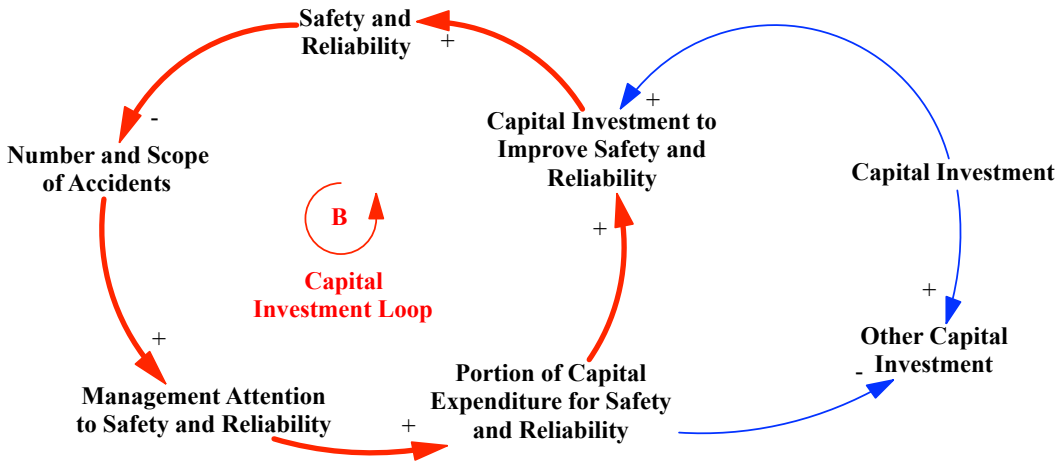

Figure 19: Capital Investment Loop

Maintenance Backlog

One of the key concepts of the model is *Maintenance Backlog*. As technology matures, it requires more maintenance. For example, Rostekhnadzor in its Official Investigation Report stated that the lifetime of each turbine is 30 years. After 20 years of operation, the average of operating time of each SSHPS turbine is about 85,000 working hours. When a turbine reaches its 50,000-hour horizon, the necessary maintenance work has to be repeated after every 9,000-10,000 hours (Rostekhnadzor, 2009).

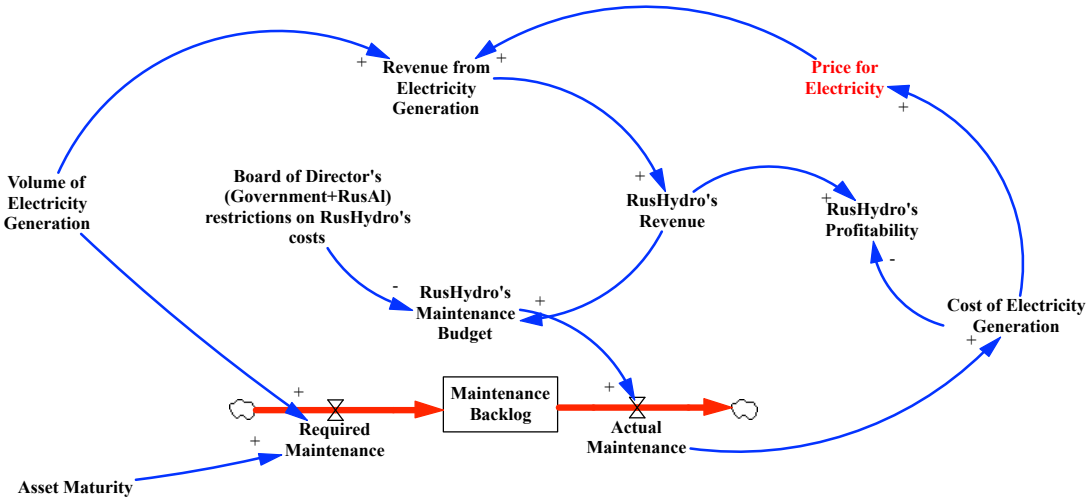

Figure 20: Maintenance Backlog

In this diagram we see that time (*Asset Maturity*) and electricity volume increase *Required Maintenance*, which results in increased stock that we named *Maintenance Backlog*. If *Asset Maturity* is an external variable, in some sense a legacy that the company has to deal with, *Volume of Electricity Generation* is a variable that can be externally controlled by the holding, which can actually generate economic gains and thus funds for maintenance.

In our model we connect *Volume of Electricity Generation* to revenues and eventually to *RusHydro's Revenues.* In order for backlog to decrease, RusHydro has to allocate more funds for its *Maintenance Budget*.

However, there is also an important variable that we call the *Board of Director's Restriction on Cost.* A board of directors that represents both government and private (RUSAL) interests has its own expectations of RusHydro's operating costs. Moreover, at the end of 2008, the board made a financial decision to mitigate possible and/or emerging engineering problems by purchasing civil liability insurance for operators of hazardous industrial facilities and owners of hydro generating installations. (RusHydro, December 24, 2008)

Moreover, increase in *Actual Maintenance* inevitably leads to increased *Cost of Electricity Generation*, which in its turn leads to a drop in profit margins for RusHydro and requires the *Price for Electricity* to go up.

Connecting Maintenance Backlog with Safety and Reliability

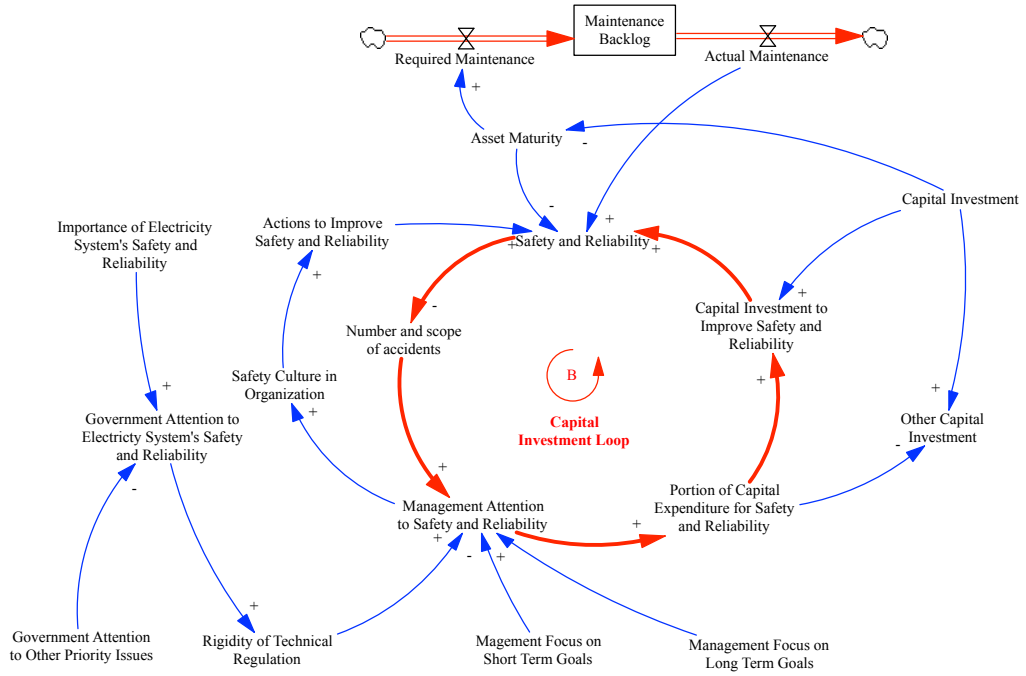

Figure 21: Connecting Maintenance Backlog with Safety and Reliability

Asset Maturity and *Actual Maintenance* are two variables that connect *Maintenance Backlog* with *Safety and Reliability*. Decrease in capital investment over time results in higher maturity of the infrastructure. The higher the maturity, the lower the *Safety and Reliability*. *Asset Maturity* is the cause for *Required Maintenance* to increase over time.

If we assume that *Maintenance Backlog* is a bathtub with inflow (*Required Maintenance*) and outflow (*Actual Maintenance*), there must be a critical level of maintenance work that will not allow any more accumulation of the backlog. At this point in my research I understand that this is a critical issue for which I do not have a clear and convincing explanation. However, it seems that an organization's migration from a safe to an unsafe state takes place with the increase of maintenance backlog.

As *Government Attention to Electricity System's Safety and Reliability* decreases so does the *Rigidity of Technical Regulations*. From Chapter 3 we know that the Law on Technical Regulations has not yet established a follow-up regulatory framework, while the old Soviet technical regulations were reclassified from "required" to "recommended" mode. In the next diagram I will also illustrate the difference between short- and long-term management goals. Together with the *Number and Scope of Accidents*, these four variables define *Management Attention to Safety and Reliability.*

Short Term vs. Long Term Goal of the Management

Management Attention to Safety and Reliability is affected by management's goals. But let us first start with RusHydro's profitability, which defines *Management Compensation*. Portions of this compensation can be related to financial performance and safety. The ratio of compensation to profitability and safety is another important differentiator.

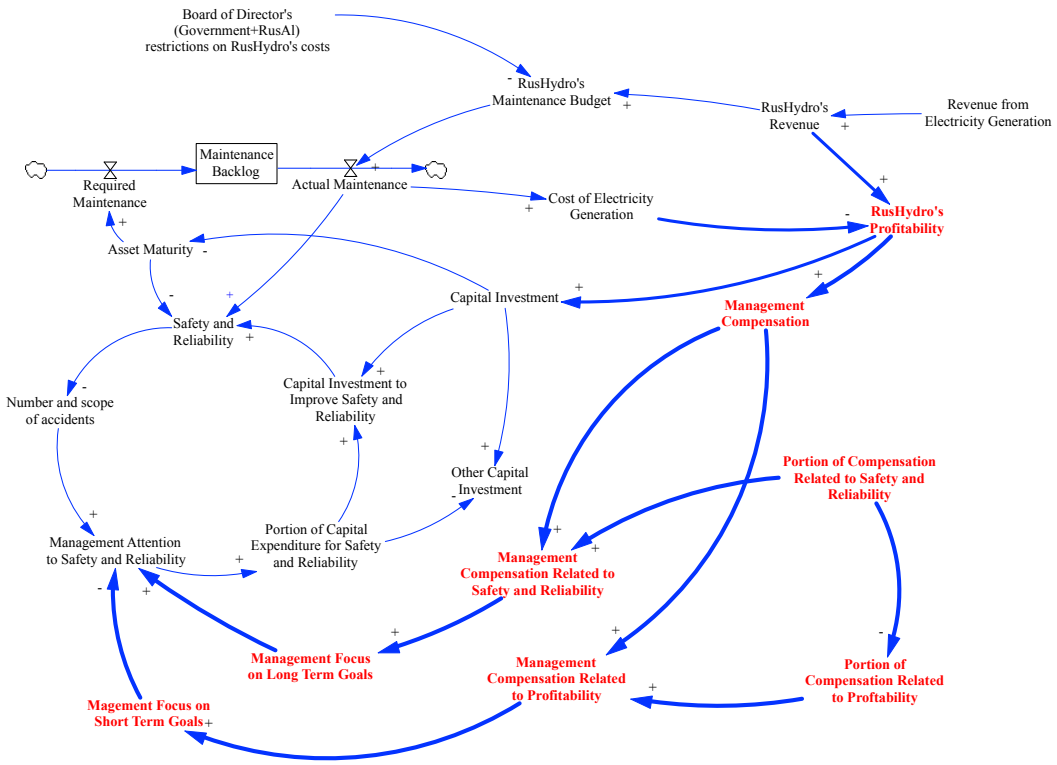

Figure 22: Short Term vs. Long Term Goal of the Management

As we saw in Chapter 3, RusHydro's KPI policy was, until 2010, focused on the company's financial and economic effectiveness; it did not include reliability and safety issues (Council of Federation, 2009b).

In this diagram I argue that the higher the proportion of compensation related to safety and reliability, the higher the *Management Compensation Related to Safety and Reliability,* the result being that management tends to focus on longer-term goals. On the contrary, the lower the portion of compensation related to safety and reliability, the higher the *Management Compensation Related Profitability,* the result being management focus on short-term goals. Management focus on long-term goals tends to increase the *Management Attention to Safety and Reliability*, and vice versa.

Summarizing key characteristics of the Hybrid System's causal-loop diagram we can conclude that this system's price dynamics are defined by a demand for electricity that drives prices up and government regulations that caps prices at levels reflecting government interest in the national economy.

Capital investment and maintenance are two crucial dynamics that can keep the number and scope of accidents at a low level. Continuous capital investment increases safety and reliability. Maintenance Backlog is stock with *Required Maintenance* as inflow and Actual Maintenance as outflow. High-level backlog is the result of slow outflow of actual maintenance, which results in decreased levels of safety and reliability.

It seems that the migration of an organization from a safe to an unsafe state takes place with an increase in maintenance backlog. Additional analysis has to be conducted to prove this conclusion.

5.3 Brief Overview of the Transition Period

"In the 1990s electricity production in Russia declined significantly because of the shut-down of several nuclear reactors, the fall in demand following the 1998 financial crisis and the consequent drop in the country's power generating capacity. However, the subsequent economic recovery contributed to an increase in total electricity consumption from approximately 809 terawatt-hours in 1998 to approximately 1,001 terawatt-hours in 2007. Today, thermal power (oil, natural gas and coal) accounts for roughly 63 per cent of Russia's electricity generation, followed by hydropower (21 per cent) and nuclear (16 per cent)" (Doeh, Wood, Popov, Fominykh, & Mouratova, 2008).

Russia's economic recovery contributed to an increase in total electricity consumption, from 715 billion kWh in 1998 to 980 billion kWh in 2007. Fossil-fuel power (oil, natural gas, and coal-fired) accounts for about 63% of electricity generation, followed by hydropower (21%) and nuclear (16%), according to the U.S. Energy Information Administration. According to state data, these plants produced 913 billion kWh in 2007.

Russia's power sector has a total generation capacity of 217 GW and includes over 440 thermal and hydropower plants, 77 of which are coal-fired, and 31 nuclear power stations. Some capacity in the far-eastern part of the country is not connected to the power grid.

Post-liberalization, the state retains ownership of system operator and transmission controller, Federal Grid Company, through its stake of 75% or more. It also maintains total ownership of the nuclear sector through the existing state agency RosAtom and its mining, fuel handling, construction and operating arms. The Interregional Distribution Company and the Hydro OGK remain under the government's control by virtue of its minimum 52% ownership of each, a similar position to that of the supply companies in which it always retains a minimum 51% stake.

The Russian electricity market is, in my opinion, one of the most complex electricity markets due to its geographical distribution and historical background. The big picture is further complicated by two additional factors:

1. The combined generation of electricity and heating energy, which adds a social component to the operating systems.

2. Unsystematic privatization of the electricity sector on the regional and municipal levels between 1991 and 1998. By social component I mean harsh climate and coupling of the electricity and thermo power infrastructures.

It took 10 years for the RAO UES to consolidate its transmission assets as federal property using complicated swaps in assets and equity with privately owned companies.

In Russia the loss of energy accounts for 40% of total consumption—a fact that is to a great extent caused by very low energy prices, which make energy-saving efforts unprofitable. Energy price increases, and the introduction of more severe energy saving regulations, remain politically unpopular. The Ministry of Industry and Energy of the Russian Federation estimates the investments needed for energy saving projects up until 2010 to be worth USD 50-70 billion (Swiss Business Hub Russia, 2008).

As a result, optimization of network losses is not high on the priority list of the Russian energy sector management. Currently the biggest and most visible loss to local power generators is that of heating energy supplied to municipalities at "social" cost. The Federal regulator and its regional offices regulate the price of heating. The heating infrastructure (mainly hot water pipelines) is on the balance sheets of generating companies. Social price caps imposed by regulators make the modernization of this infrastructure economically infeasible for generating companies.

In short, the public's deep sensitivity to price increases, as well as its distrust of sector management (the belief that that additional surpluses will be directed by the management towards modernization) makes any price increase politically unpopular. Regulators in turn resort to administrative methods of capping electricity prices. .

Transmission and Distribution

There are seven separate regional power systems in the Russian electricity sector: Northwest, Centre, Middle Volga, North Caucasus, Urals, Siberia, and Far East. The Far East region is the only one not connected to an integrated power system. Until 2007/8 UES, which is 52% owned by the government (Gazprom has a 10% stake), owned 96% of the T&D system, the central dispatch unit, and the federal wholesale electricity market (FOREM). The grid comprises almost 2 million miles of power lines, 93,000 miles of which are high-voltage cables over 220 kV. The former UES structure passed to the NGC in July 2008

Legal base for the Electricity market in Russia

The legal framework of Russia's electricity policy and the power sector's institutional structure is defined by the Federal Law on the Electricity Industry (the Electricity Law) dated 26 March 2003. In 2003 and 2007 amendments to the Electricity Law were introduced to expedite power industry reforms, introduce market instruments in the sector and reorganize Russia's state-owned electricity monopoly RAO UES. On the level of state monopoly, RAO UES adopted a restructuring plan called "The Concept of RAO UES Strategy

for 2003–2008" (the "5+5" Plan; May 29, 2003) (RAO UES), with the strategic goal of completing market deregulation by 2008. As of July 1, 2008 RAO UES ceased to exist.

Article 3 of the Electricity Law separates *consumers of electricity and heat energy* (both individual consumers and business) from *consumers of capacity* (entities that acquire capacity for its internal needs and/or onward sale).

Among other elements of the market, the article also defines:

- *Load-controlled electric power consumers:* significant consumers that influence the quality of electricity and reliability of Russia's United Energy Power System.
- *Co-generation of electric and thermal power:* a mode of operation of thermoelectric power plants in which electric power generation is directly related to simultaneous generation of thermal power. This is a key characteristic of the social impact of the electricity infrastructure.
- *Guaranteeing electric power supplier* (guaranteeing supplier): a commercial organization that is obligated in accordance with this Federal Law, or voluntarily-assumed obligations, to make an electric power purchase contract with any customer who requests it to do so, or with a person acting on behalf of and in the interests consumers who desires to purchase electric power;

Distributed generation: Separation into Wholesale and Retail Markets

Article 35 of the Electricity Law defines the requirement for legal entities to participate in the Wholesale market. According to the article, electricity consumers can participate in both Wholesale and Retail markets.

Key components of the Wholesale market:

- Bilateral Contract market
- Day-ahead Spot Market
- Intra-day Balancing Market

The Wholesale market is self-regulated by the Market Council (a non-profit organization), which decides on granting and/or depriving the right to trade on the Wholesale market, as well as defining trading rules and regulations (Article 33 of the Electricity Law). The representative of the Executive branch of the Federal Government in the Market Council has a veto power. The Council has 8 members from the Legislative and Executive branches of the Federal Government, four representatives from each of the three groups – (1) sellers of electricity, (2) buyers of electricity, and (3) representatives of commercial and technological infrastructures.

The Wholesale market is made up of three energy generation levels:

1. Generating capacities that provide reliability of the power system and nuclear power plants.
2. Thermal power stations with combined electricity and heating production. Hydropower plans that require the generation of certain levels of electricity due to their technological and environmental requirements.

3. Other participants of the Wholesale market that assumed legal obligations to provide electricity to wholesale consumers.

Retail market (Article 37):

- Consumers of electricity
- Suppliers of electricity: electricity retail organizations, guaranteed suppliers, electricity generating companies that are not permitted to participate in the Wholesale market
- Regional (territorial) transmission companies responsible for electricity transmission
- Organizations that provide operational & dispatching functions at the Retail market level.

Commercial law is the legal basis for the Retail market's daily operation. The Government regulates the rules for guaranteed suppliers, their standard contract procedures and operational/geographic limits.

Article 40 of the law requires the supplier of services to provide their end-consumers with a list of unbundled costs (cost of electricity generation, cost of transmission, cost of other services).

This Page Intentionally Left Blank

Chapter 6. Conclusion

"False conceptions are exaggerated modes of thought that do not accord with the facts. Even if an object - an event, a person, or any other phenomenon - has a slightly favorable aspect, once the object is mistakenly seen as existing totally from its own side, true and real, mental projection exaggerates its goodness beyond what it actually is" (Dalai Lama).

In my conclusion I will elaborate three major topics: (1) abstract description of the accident, (2) comparison of traditional vs. System Theory Approach, (3) summarizing and understanding the accident from system theory approach.

6.1 Abstract concept of the accident

A straightforward recitation of the events leading to the Sayano-Shushenskaya Hydroelectric Power Station accident gives us an incomplete picture of its causes. And while the System Theory approach provides a nuanced and informative explanation for the accident, its complexity of detail does not lend itself easily to quick summary. So rather than relying on either approach to give the reader an overview of the accident, let me briefly abstract the accident, mapping five key components that can help us understand the accident. These five components are Water, Structure, Machine, Power, and Human.

Water

The seasonal flooding that had previously caused three major accidents at the station was not the cause of this particular accident. However, during the accident, headwater spinning from the turbine rotor destroyed the turbine room, flooded the station, and drowned personnel. After the accident, the water level rose, requiring emergency discharge from the SSHPS and its sister Mainsk HPS downstream. Absence of an emergency discharge spillway created long-term challenges for the station as ice build-up increased pressure on the SSHPS's structure.

Structure

The structure of the station's dam remained intact immediately after the accident and through the cold winter following the accident, when water from emergency discharge created ice build-up on the dam. The strength of the structure—historically a source of station management concern—was not an issue at that time. However, the station's original design did not include an alternative power source to allow closing the upper valve automatically. This feature would have allowed for discharge of water from the flooded station several hours sooner. There were no emergency exits below the watermark in the foundation's structure to allow station personnel to evacuate safely. Turbine room design does not historically provide a separate compartment for each turbine.

Machine

The station's turbines were almost 30 years old. Average operating history of each turbine was about 85,000 working hours. The oldest turbine had a flaw in its original design; it received an inadequate overhaul six months prior to the accident (March 2009). The turbine's design flaw included an intermediate unsafe generation mode between two safe modes on each side of the spectrum. The two safe zones were: Load Zone 1: from 0 to 265Megawatt and Load Zone 3: from 570 to 640 Megawatt. The unsafe zone was Load Zone 2: from 265 to 570 megawatts. Operation in unsafe mode led to increased turbine vibration. The turbine's design flaw required the operator to pass unsafe mode as quickly as possible. Between March and August of 2009, Turbine 2 operated outside the accepted limits 210 times, for a total of 2520 seconds.

Turbine modernization in early 2009 included introduction of a management system of individual servomotors, which provided individual hydraulic actuators for individual turbine blades. Vibration sensors on the turbines, however, were inserted inadequately, and did not provide operators with complete information. None of the three layers of "turbine defense" – their 31 safety functions - were directly related to increases in turbine vibration and did not cause emergency shutdown of the turbine. As a result of the accident all 10 turbines of the station were damaged to different degrees.

Power

The design purpose of the SSHPS was to generate reliable power and maintain the stability of a large regional grid system. Two basic methods to ensure a high quality of electrical supply are:"(1) proper use of automatic voltage and frequency control methods and (2) employing large, interconnected, power systems which, by their very nature, are less susceptible to load variation and other disturbances" (Machowski, Bialek & Bumby, 2008).

There was a power disruption on the regional grid level that had to be stabilized by increased power generation at SSHPS. The operator at the Siberian Unified Grid System Dispatch had an incomplete picture of the dispatch process at the time when he sent dispatch commands to the SSHPS. The load fluctuation he assumed was to be taken by the 6.4-gigawatts power station was sent to the oldest - and defective - turbine, with one tenth of the station's installed capacity. During the last eight hours of operation (August 17, 2009), the load at Turbine 2 fluctuated between 0 and 610 MW. It operated in the Load Zone 2 between 07:46 and 08:13 (from 610MW to 605MW, to 575MW, to 475MW) (Rostekhnadzor, 2009).

Turbine 2 had been experiencing vibration anomalies, but such anomalies had become a commonly accepted risk, especially at the time of power disturbance on the regional grid level. Despite frantic attempts to slow the Turbine 2, at the moment of the accident it was generating 475 MW.

Human

There were about 300 hundred people at the station at the time of the accident. 75 people (25% of those present at the station) died. The population of Cheryomushki, hometown to the station's employees, was just 9000 people. In other words, there were for 8 funerals for

every thousand residents. The combined population of the closest cities and villages downstream from the station was 50,000. Had a broken dam resulted in a tidal wave casualties would have been enormous. This is the human scale of the accident.

Could the lives of these 75 people been saved? In my opinion, the lives of at least 65 non-core personnel that did not have to be at the station could have been saved had station management ordered a partial evacuation. Management attempt to avoid "airing dirty linen in public" was obvious even right after the accident, when federal emergency services received an initial report of only minor flooding of the station.

Interface between Machine, Power and Human

Of the five key components, the most intense interaction was between Machine, Power and Human. On the abstract level, the interaction of these three components is a source of complexity. In our case, the interface that allowed such interaction to occur was the Group Regulator for Active and Reactive Powers (GRARM). GRARM had two major goals (1) Active power regulation, which represented power actually transmitted and (2) Reactive power and voltage regulation, which was related to power going back and forth without any net energy.

At the time of GRARM development, the system requirement of GRARM did not include (1) criteria to form functional priorities for turbines operating under GRARM, (2) individual load limits and unsafe mode regimes for each turbine, (3) individual characteristics and structure of each turbine. GRARM had no safety functions. The system was not mandatory, and SSHPS could have operated with GRARM turned off.

6.2 Traditional view

Now that we've reviewed the accident's five key components, and identified its source of complexity, let us review the traditional framework through which this accident was perceived and assessed. On the left side of the graph below we have Mental Models, Changing Borders of the System and System Legacy. This is the baggage of knowledge and experience that we usually carry when we assess an accident. In the middle we have a Chain of Events, the logical and chronological flow of facts. On the right side we have a list of actions and reactions that we typically take in the aftermath of an accident. In this particular case, I've identified: Culture of Blame, Focus on Reliability and Responsibility and Modernization.

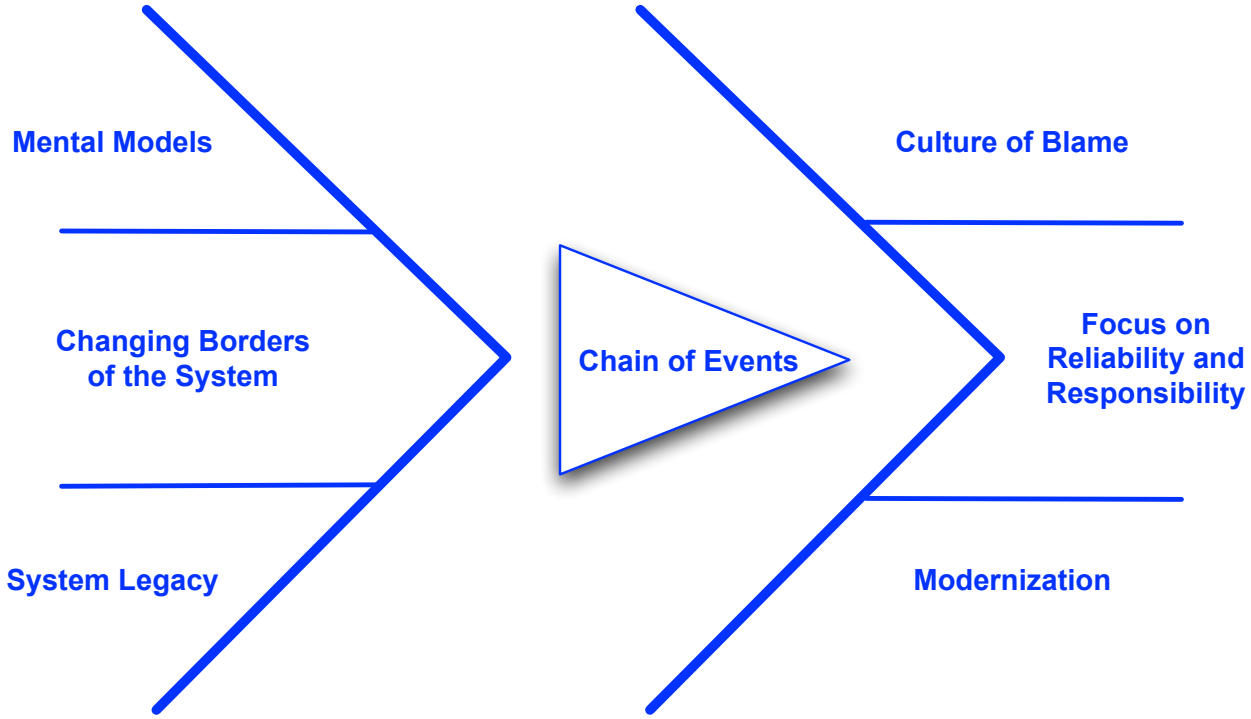

Figure 23: Traditional View of Accidents

Mental models

Traditionally we approach any accident with the baggage of previous knowledge and experience. Very often such baggage is built upon a theoretical approach. In accidents, such theoretical approach has long been the Reliability Theory, which focuses solely on internal characteristics of individual sub-components of a system.

Changing borders of the system

The system border changes over time due to its evolution and adjustment to the external environment. What was once safe may no longer be safe due to external factors. In the case of the SSHPS, continuous reform of Russia's electricity sector (which included chaotic privatization, partial price liberalization and, later, different forms of corporate consolidation) presented a long list of factors affecting station safety and reliability. Moreover, such structural challenges were among the first causes that both the investigators and the public were quick to blame for the accident.

System Legacy

System legacy presents recorded, irrefutable facts. Together with our mental models, system legacy is at the core of our assessment of a system. At the SSHPS, system legacy was a critical factor. SSHPS's integration within the Siberian Regional Energy Grid System, and importance to two aluminum-processing plants, defined the behavior of SSHPS owners and managers. Moreover, the unique legacy of the Soviet electricity system, including its

coupling with thermo energy sources due to Russia's harsh weather conditions, was a key driver behind government regulation of electricity prices.

Chain of Events

As we investigate an accident, a specific sequence of events shapes post-factum interpretation. It connects events in a specific post-factual manner—what Sidney Dekker calls "tunnel vision" (Dekker, 2006). The tunnel-vision explanation oversimplifies the history of the accident with linear logical flow and binary (right and wrong) choices. It oversimplifies the causality of events as well. As a result, hindsight prevents us from differentiating between what was known after the accident and what was known prior to and during the accidents.

Culture of Blame

In the aftermath of an accident, blame is a natural element of human and organizational behavior. The chain-of-events explanation requires people and organizations to comprehend and simplify an event, as well as identify a cause or an error, intentional or unintentional, to serve as a logical explanation. Whether it's a fire at a neighboring power station, a defective turbine, a flawed managerial decision or ill-conceived economic reforms, the culture of blame focuses attention on particular errors, rather than the systemic failures, as an explanation for an accident (Dekker, 2006).

Focus on Reliability and Responsibility

What lessons does an organization take away from assigning blame for an accident? Its management wants to increase the reliability of machinery and infrastructure. Lack of time and financial resources frequently preclude the necessary drastic changes. Perfunctory changes only reinforce complacency and a state of denial.

Punishment of the unlucky few who happened to be in close proximity to an accident nurtures fear, mistrust and indecision within an organization. This dynamics demands reflective reevaluation and a clarification of responsibilities within an organization.

Modernization

In those instances when lessons learned from an accident lead to deeper reevaluation, issues of modernization seem to address the problem in the long-term. In the three months following the SSHPS accident the Russian government signed decrees on Russia's Energy Strategy 2030; Design and Programs for the Perspective Development of Electricity; Appraisal of the Cost and Payments for Services of Operational Dispatch Management; and Amendments to Regulation of the Wholesale Market.

However, some scholars believe that "under specific Russian circumstances today, a modernization today may lead to negative results. This is because none of the modernization programs currently being discussed take into account the real causes of Russia's backwardness" (Gaddy & Ickes, 2010). They are: [1] spatial allocation of physical and human capital over a vast and cold territory and [2] rent addition to Russia's commodities export, namely oil and gas, but aluminum as well. "Russia's problem – its potential bear trap - is that rent addiction serves to sustain the dinosaurs [income from oil

and gas revenue that allows to maintain Russia's inefficient infrastructure]" (Gaddy & Ickes, 2010).

6.3 System Theory Approach

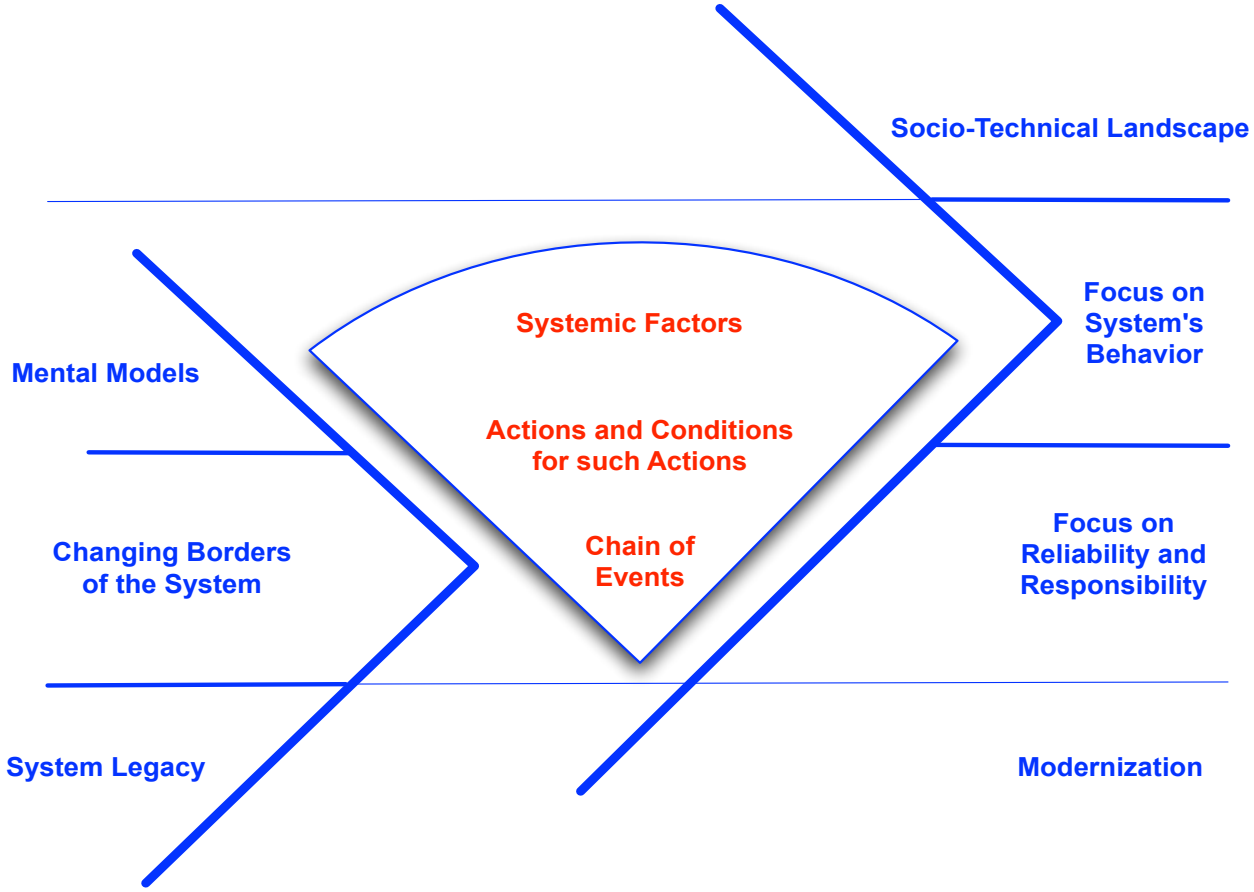

Figure 24: System Theory Approach

The System Theory approach gives us a broader understanding of a situation. This approach categorizes and structures numerous facts in a broader picture, bridging every fact with an appropriate level of analysis. What makes the SSHPS accident case interesting and complex is that there are multiple factors that occurred on different hierarchical levels, and in different points of time, that directly and indirectly steered SSHPS towards the accident.

On the events level

As the situation emerged, there was an intersection of issues of negligence, lack of proper training, indecisiveness and shock. Each individual action taken by station personnel made

sense and was part of the routine. It is when one combines these steps that they give us a more complete picture of the emerging disaster. Turbine 2 was turned into GRARM despite its known limitations. Personnel did not react to increased vibration, which after six months of operation became a "routine" anomaly. As the situation emerged, engineers on duty decided to wait for the Chief Engineer rather than make their own decisions and take necessary actions to address the problem. The Chief Engineer, who arrived 98 minutes before the accident, did not order non-essential personnel to evacuate the station. Even as vibration and control of Turbine 2 became an obvious problem, and personnel attempted to slow the turbine, 300 people were starting their workday. At the time of the accident, the alarm system did not signal the emergency situation and or the need to evacuate. Management was in a state of denial immediately after the accident, and did not inform authorities about the accident's full extent.

On the Conditions Level

The Conditions Level introduces additional context into our description of the accident. It can help explain why and how routine decisions by station personnel led to such disastrous results. Let us review the conditions that I've constructed in this thesis:

- Complex and over-centralized structure of RusHydro, with major focus on corporate profitability rather than reliability and safety,
- Lack of authority and responsibility on SSHPS managerial level,
- Maturity of station machinery,
- Unstructured and fragmented approach toward modernization and overhaul of hardware and software at SSHPS,
- System requirement gaps and design flaws of the GRARM,
- Introduction of new feature into overhauled Turbine 2,
- Lack of communication between SSHPS and Siberian Unified Grid System Dispatch,
- Absence of aggregated vibration data and its integration with safety features,
- Outsourcing of maintenance functions at SSHPS,
- Lack of training for SSHPS's personnel.

These and other conditions that emerged over time were part of daily life at the station. They produced uncertainties, dilemmas and complexities for station personnel. However, these conditions over time became an intrinsic feature of the station's daily operation.

On Systemic Factors Level

The SSHPS accident presents an opportunity to look at an existing system from a fresh perspective. Crisis and its aftermath shed new light on a system's structure. The moment of an accident alters our subjective sense of time as we begin dividing events into "before" and "after " categories. Events may be recorded and become part of the "historic record." Conditions may change and adjust to the situation. Systemic factors, however, are most likely to remain intact.

These are the systemic factors that were critical in this accident:

- Flaws in the initial design of the SSHPS, particularly of its turbines,

- Rigidity and historical inefficiencies of the Soviet economy and infrastructure, that advanced spatial misallocation of people and capital in Siberia,
- Reforms of the electricity sector (1992-2008), and segmentation of the integrated Siberian Energy System into several independent systems, without substantial capital investment and reevaluation of the operational environment for these systems,
- The hybrid nature of Russia's electricity sector, which allows co-existence of elements of both planned and market economies,
- Decrease in the direct role (economic planning) of the government and subsequent increase in government's indirect (regulatory) obligations for state property management, market regulations, technical and safety regulations, etc.
- Continuous reliance on old models of economic growth (export of commodities, i.e. aluminum) and cheap electricity as main engine for competitiveness, without substantial capital investment into infrastructure,
- Maturity of the infrastructure and accumulation of maintenance work.

Focus on System's Behavior

A broader understanding of this accident widens the scope of lessons that we can take from it. Rather than solely focusing our attention on improving reliability and responsibility, we can step one level up and ask how the system will behave in an environment shaped by given conditions and systemic factors. This system could be RusHydro, SSHPS or any other larger HPS.

If the operational environment for such hydropower stations does not change, we cannot expect that fragmented actions will prevent potentially dangerous scenarios. Demand for cheap electricity as a main cost component of competitive export commodities, generated by deteriorating infrastructure with limited capital investment, in a hybrid electricity sector regulated by old Soviet- and market-driven regulations, will inevitably lead to systemic errors. Such errors might manifest themselves in a form similar to that of the SSHPS accident. Or they may take other, unexpected, forms.

Socio-technical landscape

In a hybrid socio-technical landscape the roles of government, state enterprise, private business and civil society are not clearly defined. Their roles fluctuate depending on formal and informal interests, availability and competition for limited resources, direct and indirect financial benefits, and internal and external agendas. For example, a hybrid landscape allows the Russian Prime Minister to use both formal and informal channels to pressure leadership of Russia's private companies to meet investment obligations. In the same manner, Russia's private sector may influence the state to regulate price caps for electricity.

Russia's leadership would like the nation to become a modern and competitive global player. On one hand, the same leadership sticks to old economic models and perceptions. If the hybrid nature of Russia's social-technical landscape is a permanent state, government, private sector and society have to face this reality and work on defining each party's

responsibilities. Clarity on the socio-technical landscape level will eventually help define lower-level issues that both the state and private sector have to face in their daily operations. It can help systems such as RusHydro or RUSAL, and entities such as SSHPS or Bratsk HPS, adapt to a changing environment.

Bibliography

Beskhmelnitsyn, M. (2009). *Analiz resultativnosti investitsionnykh program razvitiya electroenergeticheskoi otrasli (Analysis of the electric power industry development investment program implementation).* Accounts Chamber of the Russian Rederation, Bulletin No. 5 (137). Retrieved from http://www.ach.gov.ru/userfiles/bulletins/10-buleten_doc_files-fl-1782.pdf

Council of Federation (2009a). *Itogovyi doklad parlamentskoi komissii po rassledovaniyu obstoyatel'stv, svyazannyh s vozniknoveniem chrezvychainoi situatsii tehnogennogo haraktera na Sayano-Shushenskoi GES 17 avgusta 2009 goda (Final report of the Parliamentary Commission on investigation of circumstances related to the man-caused emergency at Sayano-Shushenskaya HPS on August 17, 2009).* The Council of Federation of the Federal Assembly of the Russian Federation. Retrieved from http://council.gov.ru/journalsf/cat9/journal52/2009/number327.html

Council of Federation (2009b). *Prilozheniye 1: Vyvody i rekomendatsii ekspertnoi gruppy pri parlamentskoi komissii po rassledovaniyu obstoyatel'stv, svyazannyh s vozniknoveniem chrezvychainoi situatsii tehnogennogo haraktera na Sayano-Shushenskoi GES 17 avgusta 2009 goda (Appendix 1: Conclusions and recommendations of the expert group of the Parliamentary Commission on investigation of circumstances related to the man-caused emergency at Sayano-Shushenskaya HPS on August 17, 2009*). The Council of Federation of the Federal Assembly of the Russian Federation. Retrieved from http://council.gov.ru/files/journalsf/item/20100113174656.pdf

Crawley, E. (2007, January 30). *System architecture: IAP lecture 6.* Retrieved from MIT OpenCourseWare Web site: http://ocw.mit.edu/courses/engineering-systems-division/esd-34-system-architecture-january-iap-2007/lecture-notes/lec6.pdf

Dekker, S. W. A. (2006). *The field guide to understanding human error*. Aldershot, UK: Ashgate Publishing Co.

Doeh, D., Wood, C., Popov, A., Fominykh, S., & Mouratova, N. (2008). Reform of the Russian electric industry. *Law in transition online, October 2008*. European Bank for Reconstruction and Development. Retrieved from http://www.ebrd.com/downloads/research/law/lit082.pdf

Fleming, D. (2009, October 8). *Catalogue of failure led to Russian hydro plant disaster.* Retrieved from New Civil Engineer: http://www.nce.co.uk/home/energy/catalogue-of-failure-led-to-russian-hydro-plant-disaster/5209117.article

Gaddy, C. & Ickes, B. (2010). *Bear Trap: Can Russia Avoid Pitfalls on the Road to Sustainable Economic Growth?* Center for Research on International Financial and Energy

Security, Pennsylvania State University. Retrieved from http://crifes.psu.edu/papers/bearcrifes.pdf

Gnedenko, B., Belyaev, Y., & Solovyev, A. (1969). *Mathematical methods of reliability theory.* New York: Academic Press.

Goncharenko, A. (2010, June 02). *Dopolnitelnyi vodosbros Sayano-Shushenskoi GES sdan v ekspluatatsiyu (Additional spillway at Sayano-Sheshenskaya HPS commissioned).* Retrieved from Vesti: http://www.vesti.ru/doc.html?cid=17&id=365132

Hybrid (n.d.). In *Dictionary.com*. Retrieved from http://dictionary.reference.com/browse/hybrid

Interfax News Agency (2009, October 29). *Putin allocates 115m dollars to complete Siberian power plant's dam spill-way*.

International Water Power and Dam Construction (2009, July 08). *Expanding RusHydro lists GDRs on London Stock Exchange.* Retrieved from http://www.waterpowermagazine.com/story.asp?storyCode=2053529

IrkutskEnergo (2007). *About our company.* Retrieved from http://en.irkutskenergo.ru/qa/about.html

Ispolatov, S. (2010, June 29). *En+ ne knochet peremen (En+ does not want changes).* Retrieved from RBC Daily: http://www.rbcdaily.ru/2010/06/29/tek/490203

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety.* (book draft). Retrieved from http://sunnyday.mit.edu/safer-world/index.html, to be published by MIT Press in 2011.

Machowski, J., Bialek, J.W. & Bumby, J.R. (2008). *Power system dynamics: stability and control*. Oxford: Wiley. Retrieved from http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470725583.html

Ministry of Energy (2003). *Pravila tehnicheskoi ekspluatatsii elektricheskih stantsii i setei Rossiiskoi Federatsii (Rules for technical maintenance of electric power stations and networks of the Russian Federation).* No. 229 dated June 29, 2003. Retrieved from http://docs.cntd.ru/document/901865958#3H1742526C0EJO0V29NOO2KGMLF8000032I0000NM703OHGBD2863L37

RAO UES (n.d.). *Concept of RAO UESR's strategy*. Retrieved from http://www.rao-ees.ru/en/reforming/conc/show.cgi?concept.htm

Rasmussen, J., & Svedung, I. (2000). *Proactive risk management in a dynamic society.* Karlstad, Sweden: Swedish Rescue Services Agency.

RIA Novosti (2009, September 8). *Na remont SSGES vydelyat 10 mlrd rub (10 billion rubles to be allocated for SSHPS reconstruction).* Retrieved from http://uefaeuro08.ru/news/lenta/2010/02/24/n_1461575.shtml

RIA Novosti (2010, August 2). *Putin orders RusHydro, RUSAL to launch Boguchansk hydro-electric plant on time.* Retrieved from http://en.rian.ru/business/20100802/160042110.html

Rostekhnadzor (2009). *Akt tehnicheskogo rassledovanija prichin avarii, proisshedshej 17 avgusta 2009 goda v filiale Otkrytogo Aktsionernogo Obschestva «RusGidro» - «Sayano-Shushenskaya GES imeni P.S. Neporozhnego» (Technical investigation report on causes of the accident occurred on August 17, 2009 in the branch of the open joint-stock company RusHydro – Sayano-Shushenskaya HPS named after P.S.Neporozhnii)*. Prepared by the Accident Investigation Commission. Retrieved from RusHydro: http://www.rushydro.ru/file/main/global/press/news/8526.html/Act6.pdf

RusHydro (2008, December 24). *Board of Directors meeting: Minutes No. 69*. Retrieved from http://www.eng.rushydro.ru/company/governance/board/minutes/6388.html

RusHydro (2009). *Annual report 2008*. Retrieved from http://www.eng.rushydro.ru/file/main/english/investors/reports/annual-reports/RusHydro_Annual_Report_2008.pdf

RusHydro (2009, March 23). *Gidroagregat No.2 Sayano-Shushenskoi GES snova v stroyu (Turbine 2 of Sayano-Shushenskaya HPS is back in service).* Retrieved from http://www.sshges.rushydro.ru/press/news/6394.html

RusHydro (2010). *Company.* Retrieved from http://www.eng.rushydro.ru/company

RusHydro (2010, June 16). *JSC RusHydro: Strategic Plan for the period till 2015 and towards 2020*. Retrieved from http://www.eng.rushydro.ru/company/strategy

RusHydro (2010, September 28). *Na Sayano-Shushenskoi GES nachalis ispytaniya beregovogo vodosbrosa (Testing of the shore spillway started at Sayano-Shushenskaya HPS).* Retrieved from http://www.rushydro.ru/press/sshges/12569.html

RusHydro (2010, November 3). *JSCRusHydro recognized as one of the world's most rapidly developing energy companies* . Retrieved from http://www.eng.rushydro.ru/press/news/13039.html

RuStocks.com (2010, September 3). *Regular meeting of JSC RusHydro's Board of Directors*. Retrieved from http://www.rustocks.com/index.phtml/Pressreleases/20/8/24371?filter=2010-09

Russian Rederation (1997). *Federalnyi zakon O promyshlennoi bezopasnosti opasnykh proizvodstvennykh ob'ektov (Federal law on industrial safety of hazardous production*

facilities). No. 116-F3 dated July 21, 1997 with latest amendments of August 7, 2000. Retrieved from PortNews Information Agency: http://portnews.ru/laws/law/12/

Russian Federation (2003). *Federalnyi zakon "Ob electroenergetike" (Federal law on electric energy).* No. 35-F3 dated March 26, 2003 with latest amendments of November 4, 2007. Moscow, Russia. Retrieved from http://www.fas.gov.ru/legislative-acts/legislative-acts_16377.html

RuStocks.com(2008, October 31). *Code of corporate governance of open joint-stock company RusHydro.* Retrieved from http://www.rustocks.com/put.phtml/shGIDR_GovernanceCode.pdf

RuStocks.com (2010, September 3). *Regular meeting of JSC RusHydro's Board of Directors*. Retrieved from http://www.rustocks.com/index.phtml/Pressreleases/20/8/24371?filter=2010-09

Sagers, M., Freedenberg, P., & Mahnovski, S. (2009, August 21). Accident at Russia's Sayano-shushenskaya hydroelectric plant. *IHS CERA Alert*.

Standard&Poors (2008). *Corporate Governance Score: RusHydro (OJSC).* Retrieved from http://www2.standardandpoors.com/spf/pdf/equity/RusHydroexecutivesummary_Eng3.pdf

Swiss Business Hub Russia (2008). *Russia: Equipment for the Electricity Sector*. Retrieved from http://www.osec.ch/internet/osec/de/home/export/countries/ru/export/economic_report.-RelatedBoxSlot-15131-ItemList-57316-File.File.pdf/Russia-Electricity-Equipment-new.pdf

Ushakov, I. (2000). Reliability: Past, present, future. Keynote opening lecture at the conference on *Mathematical Methods in Reliability*. Bordeaux, France.

Voropai, N. (n.d.). *Vstupitelnoye slovo direktora instituta (Foreword of the Institute Director).* Institut sistem energetiki imeni L.A.Melentiev (Institute of Energy Systems named after L.A.Melentiev). Retrieved from http://www.sei.irk.ru/enterword.jsp

Weinberg, G. (1975). *An introduction to general systems thinking.* New York: Wiley.