RESILIENT CONTROL FOR CRITICAL INFRASTRUCTURES AND SYSTEMS

Yaguang Yang and Russell Sydnor
Office of Research, US Nuclear Regulatory Commission
21 Church Street, Rockville, 20850 USA
yaguang.yang@nrc.gov; russell.sydnor@nrc.gov

ABSTRACT

For critical infrastructures and systems, it is imperative that the infrastructures and/or the systems can survive the most severe incidents, such as component (hardware, software, or power supply) degradations and failures, natural disasters, human errors, malicious attacks, and environmental changes. This paper presents our opinions on the general overarching design considerations for resilient control systems. The actual resilient control implementation depends on what unfavorable scenarios may be addressed. The mitigation actions that should be considered will be in accordance with the design bases scenarios. We will also discuss the enabling technologies that will be needed for these mitigation actions; and why an integrated system approach will be able to increase the survivability. A literature review related to these enabling technologies will support our judgment that the real challenge faced by resilient control system designers and regulatory organizations is not the availability of the individual technologies, but instead, is a lack of precedent and successfully proven design that integrates many state-of-the-art technologies into a single first-of-the-kind system. Besides the complexity of the resilient control system design, another hurdle in the design is that the technologies successfully used in one industry may not be directly applicable to another industry because the systems may be significantly different. For example, mathematical models successfully used in control system design in the aerospace industry are not the same as the ones in nuclear power plants. Therefore, rigorous design reviews at different design stages, extremely aggressive testing performed by independent teams, and thorough license reviews by regulatory organizations will be necessary.

Key Words: Resilient control, critical infrastructures and systems, system survivability

1 INTRODUCTION

For critical infrastructures and systems, such as nuclear power plants, power grid systems, and critical space systems, it is imperative that the infrastructures or the systems can survive the most severe accidents. The necessity of this requirement has been seen from the consequences of notable incidents such as the Chernobyl nuclear power plant accident, the Challenger space shuttle explosion, the Yuma power blackout, and the recent Fukushima nuclear reactor accident triggered by the earthquake and the tsunami. To support meeting these challenging requirements, the concept of resilient control system design has been proposed [1-2]. The ultimate goal of resilient control system design is to maximize the survivability of the critical infrastructures and systems when they are subject to the adverse operating conditions, such as component (hardware, software, or power supply) degradations and failures, natural disasters, human errors, malicious attacks, and environmental changes. Although resilient control design has been considered and discussed by many researchers, and several conferences have been held in the last few years, different researchers consider different scenarios and propose using different technologies to mitigate different adverse conditions. For example, [2] discussed resilient control with the emphasis on modeling uncertainty and focused on H_2 and H_∞ design methods; [3-4] proposed resilient control based on prognostics technology; [3,5] discussed resilient control design to mitigate the effect of cyber attacks. [6]

suggested a different perspective on resilient control, which involves complex networks, cyber awareness, data fusion, and human-machine interface. [7] considered the decentralized agent-based control in the resilient control design. While these researchers, based on their previous experience, considered different adverse operational conditions and suggested solutions for the different aspects of the goals of resilient control design, in our opinion, a complete solution for the resilient control system design should consider a broader range of possible incidents and needs and adopt a broader spectrum of technologies at the same time. While actual implementation may be determined by the scenarios desired to be considered, we believe that resilient control system design is neither a single technology nor a new technology; it is a complex integrated system of systems based mostly on a variety of well developed technologies related to the feedback control, computer systems, and the information theory.

In this paper, we will present our perspectives on resilient control system design. By the term of resilient control system, we mean that these systems are able to work robustly to the modeling uncertainties and under measurement sensor inaccuracies in the normal operational and accident conditions; to take preventive actions when some incipient failures are predicted or when some failures are actually detected; to recover from failures of instrument, actuator, communication link, and power; to return to a safe status after a severe accident; to survive from natural disasters (such as earthquake, tsunami, hurricane, tornado), unexpected human errors, and malicious threats; to mitigate the negative impacts after a beyond design accidents. We refer to a control system with at least some of these features as a resilient control system. We will discuss technologies that may be used in resilient control design to achieve these goals; how these technologies will be used in which scenarios; why an integrated system will be a better design than the traditional control systems design that use only part of the technologies; and what are the challenges of resilient control system design.

The remainder of the paper is organized as follows. Section 2 explains that a resilient control system is a system of coupled systems. Section 3 discusses the importance of system awareness in a resilient control system. Section 4 discusses the potential use of networked control systems in resilient control system design. Section 5 is about hierarchical structure and supervisory control of the resilient system. Section 6 addresses reliable design principles such as redundancy, diversity, and defense in depth and their uses in resilient design. Section 7 discusses the necessity of protection and recovery systems. Section 8 discusses the use of multi-input multi-output (MIMO) methods and robust control in resilient system design. Section 9 discusses adaptive and reconfigurable designs for resilient systems. Section 10 focuses on cyber security in the resilient system. Section 11 considers sensor noise suppression techniques such as signal processing and statistical estimation. Section 12 addresses the importance of the post-accident information collection. Section 13 considers the role of regulatory organizations. The last section summarizes conclusions.

2 A RESILIENT SYSTEM CONTROLS COUPLED SYSTEMS

A critical infrastructure or system that needs a resilient control design is typically a high cost complex system. It normally includes physically distributed but operationally coordinated subsystems. Examples of these systems are Nuclear Power Plants (NPP), electrical power grid systems, satellites in formation fly, etc. As an example, the next generation nuclear power plant (NGNP) will have a nuclear reactor system, steam generator system, turbine generator system, intermediate heat exchange system, heat transport system, hydrogen production system and/or chemical heat process system (such as oil refinery system), etc [8]. Each sub-system is physically distributed but these sub-systems are connected (the distance between hydrogen production and reactor system may be at least 500 meters, but they are connected by the heat transport system). The NGNP control system has to control these coupled subsystems in a coordinated way to balance the overall plant heat generation, transmission, and consumption. For the satellites in formation fly [9], a set of satellites are physically separated in space, but their relative locations and attitudes have to be controlled in a coordinated way so that these satellites

can work as a group to achieve their scientific missions. Though each satellite has its own instruments and attitude control system, these satellites are linked by the communication system to share the information on their positions and attitudes so that all satellites' positions and attitudes are controlled as a group.

This coordination among sub-systems is very important and it requires communication systems to share information among subsystems during normal and abnormal operating conditions; information sharing makes it possible that supervisory control will be able to coordinate the distributed subsystems to set goals for individual control sub-systems. Information sharing, diagnostics, prognostics, and distributed control design also make it possible that the intact subsystems may be immune from failure propagation of the damaged system(s). We will discuss this in more detail in the following sections.

3 SELF AWAERNESS IS CRITICAL FOR RESILIENT CONTROL SYSTEMS

Several design considerations require that resilient control systems have the capability of detecting failures and/or predicting incipient failures with sufficient confidence so that it can take preventive actions to prevent the situation from getting worse. Fortunately, fault detection, diagnostics and prognostics technologies have been studied for many years, and numerous successful applications have been reported [10][11].

[10] discussed the use of historical data stored in the computer system to monitor instrument channel health condition, including static surveillance testing and dynamic testing of process instruments in nuclear power plants. For the static method, several techniques, such as averaging techniques, empirical modeling techniques, physical modeling techniques, and fault detection techniques are explained. For the dynamic method, sensor response time and noise analysis in frequency domain and time domain are presented. These techniques can be used to examine sensor drift, sensor failure, and quality assurance, etc.

In [11], some real applications of diagnostics and prognostics are described with fairly deep details. For example, using the fact that most machine components exhibit symptoms prior to a failure event, one can identify these symptoms by several types of nondestructive testing such as oil analysis, wear particle analysis, thermography and vibration analysis. Among these tests, vibration analysis is applied most frequently to rotating machinery. Manufacturers typically collect the vibration characteristics, such as vibration spectrum, vibration modes and eigenfrequency of the important components and save this information into computer systems. Accelerometers are mounted on these components and the instruments continuously monitor these characteristics. The measured signal is processed and then compared to the database and libraries of typical signatures for the malfunction of bearings, misalignment and other problems, as well as normal operational signal modes to determine the health of rotational machines. This type of technique has been developed and used in various diagnostic and prognostic applications in light water cooled nuclear reactors [11-12]. When a moderate, serious or extreme fault is detected, experts are involved on the analysis and follow-up actions.

Another example is "acoustic monitoring" [11, 13] which has been used in the chemical and nuclear industries to detect leakage. The audible spectra obtained through acoustic monitoring in normal operation and leakage conditions are different. This measurement, for example, can be used to detect if a valve is nearly closed but not completely closed as required. Cavitation may occur in pumps which may cause serious damage to the component, cavitation noise can be detected using acoustic methods. Rotational machines also have narrow band, high amplitude peaks in the measured acoustic spectrum. Deviations of these peaks from their baseline location, shape or magnitude give a warning of changing conditions. These changes are well classified, such as temperature change or speed change, etc. With the aid of computer systems and newly developed technology, engineers have made this kind of fault detection system more reliable and accurate.

There are many other reports on the applications of diagnostics and prognostics. For example, [14] used accelerometers (in the audible frequency range and acoustic emission detection in ultrasonic range) to detect and localize the moving of loose parts and to estimate their size and potential damage. [15] used signal noise analysis (auto-spectra and cross-spectra) and correlation function (auto-correlation and cross-correlation) of the measured process signals, together with linear system theory, to diagnose the motion of nuclear reactor core barrel and core barrel support assembly.

In summary, the technologies such as fault detection, diagnostics, and prognostics, have shown their capability to detect and/or predict incipient faults. Together with other design features, such as redundancy, defense in depth, reconfigurable design, networked information sharing, and supervisory control (which will be discussed later), the capability of detection and predication will enable the resilient control systems to mitigate the effects of various incidences. Therefore, these technologies should be adopted in resilient control systems.

4 A RESILIENT CONTROL SYSTEM IS A NETWORKED CONTROL SYSTEM

For a resilient control system, fault detection and accident warning is the first step to take the right action at the right time. A fault or accident happening in one subsystem may require another subsystem to take appropriate action. This means that the resilient control system should be a networked control system so that various subsystems and supervisory control system can share critical information in real time. Clearly, the state-of-the-art networked digital control system should consider information delay and other effects such as packet drops discussed in [16]. As a result, mathematical models for networked control systems are significantly different from the ones used in traditional control systems; and the design methods are more complex than the ones developed for traditional control systems.

An important feature of a networked control system is that information (reference input, plant output, control input, etc.) of measurements and control decisions is exchanged using a network among subsystems. The insertion of the communication links in the feedback control loops makes the analysis and design of the networked control system more complex because the information traffic uses packets that may not be synchronized and cause significant information (constant or more likely time varying) delay; even worse, some packets can be lost during the transmission and therefore the received information may be incomplete. These phenomena do not meet the assumptions made for the conventional control systems. However, significant progress has been made in the analysis and design of networked control systems [17]. Appropriate models are developed to account for the network delays. Non-networked feedback system design methods have been extended to the design of networked control systems. For example, one can compute an upper bound on the maximum allowable transfer interval such that stability of the closed-loop system is preserved. This bound can be used to design the network sampling rate to guarantee the stability when the control loop is closed over the network. Compensation for network-induced delay is also proposed. Though the networked control system is still a dynamic research area, the existing methods may be useful for the practical design of networked control systems. However, real design and implementation of a networked control system to fulfill the requirements of the resilient control system is still challenging due to the lack of successful experience.

A realistic and critical design consideration related to networked control system is the separation of communication links of control systems and the communication links of protect systems. As the protection systems have to be extremely reliable that do not allow packet loss and long time delays.

Networked control systems are essential for information sharing in resilient control. Together with the other design considerations such as diagnostics, prognostics, fault detection, and redundancy, it makes supervisory control more powerful in decision-making process to take preventive actions to avoid using

faulted components and/or subsystems to mitigate the effects of component and/or subsystem failures, to recover from the failures of instruments, actuators, communication links, and power.

5 HIERARCHICAL AND DISTRIBUTED STRUCTURE

Because of the information sharing capability provided by the networked control system, resilient control systems should be designed as a hierarchical control system [18] to coordinate the responses of the subsystems to the changes of various operational conditions. The supervisory control system is on the top of the distributed control subsystems. Each distributed control system controls a subsystem, such as a single satellite of a group of satellites in formation fly, or a turbine generator system in a nuclear power plant. Each distributed control system is relatively independent but is connected to the supervisory control system via communication networks. Each subsystem sends, via communication networks, the information important to the entire system to the supervisory control system and receives the commands from the supervisory control system. The supervisory control system, after receiving the information from the distributed control subsystems, makes decisions and sends the commands to the distributed control subsystems. This structure has been used in some traditional nuclear control systems, for example, the Babcock and Wilcox Pressurized Water Reactor [19], to balance the plant so that each subsystem knows its target of heat generation, heat transmission, and heat conversion.

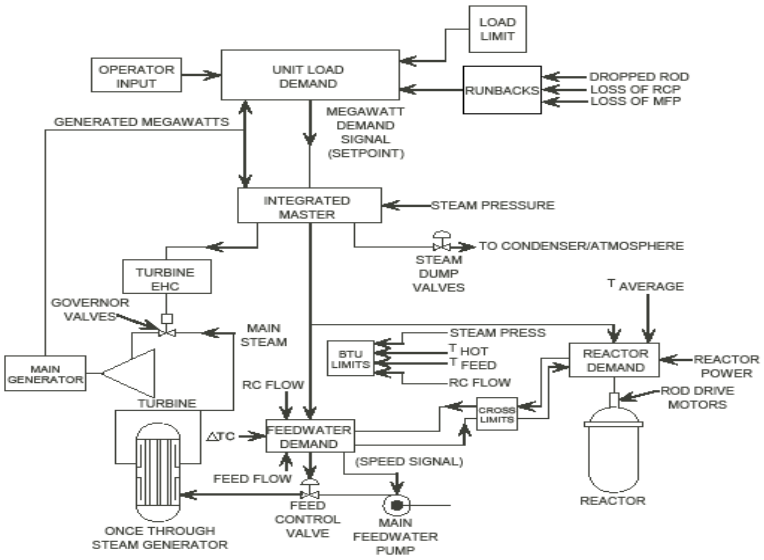

Figure 1. Simplified integrated control system of B&W pressurized water reactors

For a resilient control system, with the aid of fault detection, diagnostics and prognostics, we expect the supervisory control system can make more complicated decisions than traditional integrated control system designs, such as selecting appropriate sensors and actuators from redundancy when sensor or actuator failure is detected; reconfiguring the entire system when some severe accident happens; using a different set of control parameters when system reconfiguration occurs. These decisions are crucial for resilient control systems to achieve most design requirements, such as taking preventive actions when some incipient failures are predicted or when some failures are actually detected; recovering from failures of instrument, actuator, communication link, and power; returning to a safe state after a severe accident; surviving from natural disasters (such as earthquake, tsunami, hurricane, tornado), unexpected human errors, and malicious threats; and mitigating the negative impacts after a beyond design accident.

6 REDUNDANCY, DIVERSITY, AND DEFENSE IN DEPTH

Redundancy, diversity, and defense in depth are required general design criteria for all nuclear power plants [20]. With added features in resilient control, however, the design team may better use the redundancy, diversity, and defense in depth to achieve higher survivability than the traditional control system designs in nuclear reactors. Since all critical sensors, actuators, and components in control and protection systems have redundancy in nuclear power plant; by incorporating features such as prognostics, diagnostics, networked information sharing and supervisory control, adaptive and reconfigurable resilient control systems, the integrated resilient control system is able to detect and identify the failed sensors and/or actuators, to select intact sensors and actuators, and to reconfigure the system so that the reconfigured system does not involve any problematic components, thereby increasing the overall system's survivability. Besides the traditional sensors, actuators, and components, redundancy in resilient control systems should be extended to more subsystems. For example, the redundancy of the communication network systems should be considered as it may experience environment disturbances or natural disasters, and information sharing is very critical for resilient control systems. The redundancy of communication network systems may also mitigate the negative effect of packet drops. As more than one link transfers the same information, one may also use the redundant links to detect the failure of some communication network systems by cross checking the received information. Physical separation of the communication network systems among critical subsystems may be another required feature because it increases the survivability of the communication network systems when facing accident such as fire, earthquake, hurricane, or malicious intrusion.

Although redundancy may mitigate the effect of single failures, using several identical sensors (or actuators) for the same measurable parameters (or control parameters) does not eliminate common mode failures since identical product may fail at the same time in a similar situation. To prevent such a common cause failure, it is imperative to use different types of redundant sensors (or actuators) for the same measurement (or for the control of the same parameter). This is the philosophy of diversity. Diversity in resilient control system design becomes even more important because digital sensors and actuators are expected to be used in resilient control system and redundant identical software in these digital components may not enhance the reliability as redundant identical hardware does [21].

Defense in depth is another general design criteria required for nuclear power plants by [20]. To prevent radioactive material leakage, several protection layers are designed; fuel rods, pressure boundary, and containment. To mitigate loss of power effects, the reactor systems first use power coming from the turbine generator; then from the electrical power grid; then from, if grid fails, the diesel generator; and then from, if diesel generator fails, the battery. This idea can be extended further. For example, if any accident, or serious problem or threat is detected in the main control room, the communication connection between the main control room and the needed subsystems should be disabled and the alternative remote control room should be used to control the plant until the problem or the threat is resolved. The resilient control systems may have additional layers and broader spectrums of protection to handle various incidents.

7 PROTECTION AND/OR RECOVERY SYSTEMS

The final barrier of defense in depth in resilient control systems is the protection and/or recovery system. It is worthwhile to discuss the features of this system in a separate section because of its importance to the system survivability. The protection and/or recovery system is designed for the worst case. Unlike other subsystems in resilient control design, the protection or recovery system must be

logically and physically *simple* so that it is extremely reliable because the protection or recovery system is the last barrier to prevent the entire critical asset from disastrous failures. Examples are the safe mode control in spacecraft attitude control system [22] and reactor protection systems in nuclear reactors [23]. The former works when the normal mode control system fails to stabilize the spacecraft. The safe mode control normally uses only earth magnet field (which is always available) and magnet torque bar to stabilize the spacecraft using extremely simple PID control. This strategy has saved numerous satellites and brings them back to the normal attitude control modes. The reactor core protection system works when the normal reactor control systems fail to control some safety critical parameters or some subsystems fail to maintain normal operating conditions. The reactor protection system also uses very simple logic, has redundant and diverse instruments, and is designed to be "fail safe".

It is expected that the resilient control system will transmit most information using shared digital communication links and multiplex/demultiplex technology which is significantly different from analog communication links which are mostly dedicated point to point links. Although, sharing communication networks has many advantages, the information transmission protocols in this form are more complex and this may cause signal delay and package drop. All these features contradict the simplicity and reliability requirements on protection/recovering systems. Therefore, separate and independent communication systems for protection/recovery systems should be considered.

In summary, a well designed and implemented protection/recovery system should be logically and physically as simple as possible and extremely reliable so that it will be always available to protect the system when severe accident happens, to mitigate the adverse effects when beyond design accident occurs.

8 ROBUST DESIGN OF RESILIENT CONTROL SYSTEMS

To enhance the overall resilience of critical infrastructures and systems, besides adding layers in defense in depth, resilient control systems should be designed to improve the robustness of each defensive layer so that it will minimize the chance to challenge the next defensive layer. This requires that the control system be robust to the modeling uncertainties (which we will discuss in this section) and the measurements reliable in the presents of sensor noise (which we will discuss later).

Since a resilient control system controls multiple coupled subsystems, each subsystem has at least a controlled variable and redundant sensors and actuators; a resilient control system is a MIMO system. This means that classical control system design methods used in most existing nuclear power plant control system design may be improved because the classical control theory was introduced to analyze and design the single input and single output (SISO) systems. Although classical control theory is still useful if the designers consider each subsystem independently except that each subsystem receives input reference from the supervisory control system; a better practice is to view the entire resilient control system as a large coupled system and to design the resilient control system using MIMO control system design methods, such as robust pole assignment [24], optimal control [25], and H_∞ control [26] design methods. By using the extra degree of freedom of MIMO systems, robust design makes the closed-loop system insensitive to the modeling uncertainty and unpredicted disturbances.

It is worthwhile to note that the resilient control system has redundancy for important sensors and actuators, which means that even if some sensors and/or actuators failed and the system is reconfigured based on what sensors and actuators are available, the reconfigured system may still be a MIMO system. Therefore multiple control laws may be designed and stored in the computer control systems. When some sensors and/or actuators fail and the system is reconfigured, the corresponding control law for the reconfigured system should be used.

In summary, robust control design mitigates the adverse effects of modeling error and unpredicted disturbance in normal operating condition, thereby reducing the chance of challenging multiple defensive layers, and thereby improving the survivability of resilient control systems.

9 A RESILIENT CONTROL SYSTEM IS ADAPABLE AND RECONFIGURABLE

We have touched on reconfiguration of the resilient control system in the previous section. Since a resilient control system has the feature of fault detection, diagnostics, and prognostics, it can detect component failure and malicious threat or even predict incipient faults of different components, this information is also shared with the supervisory control system in real time via the reliable communication networks. Also, since the resilient control system has redundancy, the supervisory control system can make real time decisions to avoid using faulted components/subsystems by reconfiguring the entire system. This decision results in a series of commands that are sent to all the relevant subsystems. The subsystems execute the reconfiguration commands; the entire system is reconfigured into a different new system. The control laws designed for the default system may not be suitable for the reconfigured system; therefore a set of pre-designed control laws for this new system are stored in the computer system and automatically used to replace the previous control laws.

Reconfigurable system design has a long history in spacecraft design (autonomous control) and has been very successful [27]. Our opinion is that the same design principle is directly applicable in nuclear power plant control system design. Special attention should be paid to the switch of the control laws, that is, the state transients must be in the safety envelop of normal operation. Therefore, when designing the control law for the reconfigured system, the control engineers need to minimize the transient effects so that the entire system can be stabilized from this incident.

An adaptable and reconfigurable feature provides the resilient control system additional layers of defense in depth. The preventive actions should significantly reduce the adverse effects such as sensor and actuator failures caused by aging, natural disasters, human errors, and malicious attacks.

10 CYBER SECURITY DESIGN TO MITIGATE MALICIOUS THREATS

Besides equipment failures and human errors, the resilient control system is required to counteract malicious threats. This is particularly important in a resilient control system which is based on digital systems that are more vulnerable to cyber attacks. For example, [28] reported coordinated covert and targeted cyber attacks against global oil, energy, and petrochemical companies starting in November 2009; [29] reported and analyzed W32.Stuxnet. The report concludes that W32.Stuxnet is “an incredibly large and complex threat to industrial control systems”. These examples demonstrated the importance of taking cyber security into consideration in the control system design. Many research works are recently proposed to incorporate cyber security into resilient control system design. In [30], deceptive defense mechanisms are proposed; in 2007, the National Institute of Standards and Technology (NIST) published “Guide to industry control system security” [31]. Cyber security is a very dynamic, important, underdeveloped, and challenging technical area [32]. We expect more serious research will be conducted. We also expect that the resilient control system design will use extensively real time data and possibly plant models to identify degradations, incipient failures, deviation from normal operations, and cyber intrusions by comparing information from redundant measurement, model based predictions, statistical and historical trend analysis, etc.

We believe that taking cyber security into the design consideration will be necessary for resilient control systems.

11 SIGNAL PROCESSING FOR SENSOR NOISE SUPPRESSION

Sensor noise has been found to cause erroneous responses in nuclear power plant control and protection systems [33]. Similar to the modeling errors and unexpected disturbances, measurement errors always exist in engineering systems. There are two types of measurement errors, systematic errors and random errors. In general, a systematic measurement error is a biased error which is constantly larger or smaller than the actual value of the measured parameter. This error may be related to calibration process or material aging or environment changing, etc. A random error is associated with the fact that when a measurement is repeated, it will generally provide a measured value that is different from the previous value. It is random in that the next measured value cannot be predicted exactly from the previous value. For example, some sensors are very sensitive to thermal noise; some sensors are very sensitive to electromagnetic interference; and some sensors are very sensitive to radiation. In extreme cases, the sensor response to the combination of the environments may be greater than the response to the desired measurand. The measurement error may become so severe that the signal to noise ratio is so high that the measured value cannot be directly used.

Improving sensor performance is important to resilient control. Fortunately, many statistical estimation methods have been developed to estimate measurement bias and true measurement value under the noise environment. These methods have been proven very effective in real applications. For example, Kalman filtering [34] has been successfully used in spacecraft attitude determination for this purpose. Another efficient tool is the digital signal processing methods which have been widely used in many industrial applications to suppress random noises, thereby enhancing the accuracy and reliability of the measurement [35]. These methods, such as low pass filters, Butterworth filter, and Chebyshev filter have been fully discussed in [36].

For resilient control system design, we believe that both signal processing methods and statistical estimation methods can significantly improve measurement accuracy and reliability. Therefore, incorporating signal processing methods into the resilient control system design should reduce the chance of entering next defensive layer, thereby increasing the survivability of critical infrastructures and systems.

12 POST ACCIDENT INFORMATION COLLECTION

One of the important lessons learned from Fukushima accident is that nuclear power plants need robust instrumentation and control systems against severe accident [37]. The Fukushima plant computer system was damaged by the Tsunami and could not record plant status data. Important data about plant status after the tsunami were lost. Engineers had to make decisions while lacking key information and researchers have lost opportunity to reexamine the accident and gain insight to prevent similar accidents in the future.

We believe that higher physical protection standards for the critical instrumentation should be considered so that reliable post accident information collection will be available. This design consideration should mitigate negative impacts after a beyond design accident.

13 ROLE OF REGULATORY ORGANIZATIONS

Given the complexity of resilient control system designs described above and the safety critical implications of resilient control system designs, it is clear that the design, implementation, testing, operation, and retirement of resilient control systems need to be strictly scrutinized. The regulatory

organizations, such as NRC and FAA, may need to be involved in the entire life cycle of the resilient control systems. In the United States, Nuclear Regulatory Commission (NRC) is a designated agent that regulates all activities of nuclear power plants from site selections to decommissioning based on 10 CFR [20]. It is likely that the Next Generation Nuclear Power plants (NGNP) will adopt some design features of resilient control design described in this paper [38]. NRC does not have the experience of licensing resilient control system design. We expect that there will not only be challenges ahead for the design team to develop the first-of-the-kind resilient control system in the nuclear industry and for the testing team to validate the design, but there will also be challenges for the regulatory organization to license the design via extensive and critical reviews.

14 CONCLUSIONS

In this paper, we presented our opinion on the overarching principles of a fully developed resilient control system which is designed for critical infrastructures or systems. Based on these required design principles, we discussed methods that may be used to achieve these required design features. These methods involve many technical disciplines and systems. Therefore, a resilient control system is a system of systems. Unlike traditional control systems, the design work cannot be done by one control engineer anymore; it will involve an engineering team with expertise in many different fields. Based on many papers we reviewed in these technical areas, we believe that most technologies are matured for engineers to successfully design and implement resilient control systems. However, to design and build the first-of-the-kind of resilient control system still needs a lot of detailed work and can be very challenging because of the ambitious goals. Therefore, it is possible that the first-of-the-kind of resilient control system design will adopt only some of the overarching principles based on the scenarios analysis and risk assessment of a particular system.

15 REFERENCES

1. E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing. Aldershot Hampshire, UK, (2006).
2. M. S., Mahmoud, *Resilience Control of Uncertain Dynamical Systems*, Springer-Verlag, Berlin Heidelberg, (2004).
3. L. M. Stevens, "Next generation nuclear plant resilient control system functional analysis," *Idaho National Laboratory Technical Report*, INL/EXT-10-19359, (2010).
4. K. Ji, Y. Lu, L. Liao, Z. Song, and D. Wei, "Prognostics enabled resilient control for model-based building automation systems", *Proceeding of building simulation 2011,* Sydney Australia, November 14-16, pp.286-293 (2011).
5. N. Kottenstette, G. Karsai, J. Sztipanovits, "A passivity-based framework for resilient cyber physical systems", *Proceeding of 2nd International Symposium on Resilient Control Systems*, Idaho Falls, ID, September 18, pp. 43-50, (2009).
6. C. G. Rieger, D. I. Gertman, and M.. A. McQueen, "Resilient control system: next generation design research", *Proceeding of 2nd Human System Interactions,* Catania, June 23, pp632-636, (2009).
7. M. B. Kane, J. P. Lynch, and A. T. Zimmerman, "Decentralized Agent-based Control of Chilled Water Plants using Wireless Sensor and Actuator Networks", *Proceeding of 2nd International Symposium on Resilient Control Systems*, Idaho Falls, ID, September 18, pp. 131-136, (2009).
8. General Atomics, "Pre-conceptual engineering services for the next generation nuclear plant (NGNP) with hydrogen production," https://inlportal.inl.gov/portal/server.pt/community/ngnp_public_documents (2007).

9. F.H. Bauer, Hartman, H. Kate J. Bristow, D. Weidow, J. How, and F. Busse, "Enabling spacecraft formation flying through spaceborne GPS and enhanced autonomy technologies," *Proceedings of the 12th International Technical Meeting of the Satellite*, Nashville, TN, 14-17 Sept. pp. 369-383, (1999).
10. Ø. Berg, et al., *On-line monitoring for improving performance of nuclear power plants, part 1: instrument channel monitoring*, IAEA Nuclear Energy Series, Technical Report, No. NP-T-1.1, Vienna, (2008).
11. Ø. Berg, et al., *On-line monitoring for improving performance of nuclear power plants, part 2: process and component condition monitoring*, IAEA Nuclear Energy Series, Technical Report, No. NP-T-1.2, Vienna, (2008).
12. H. R. Smith, E. Wiedenbrug, and M. Lind, "Rotating element bearing diagnostics in a nuclear power plant: comparing vibration and torque techniques", *Proceedings of IEEE International Symposium on Diagnostics for Electric Machines, Power Electronics and Drives*, Cracow, December 4, pp. 17-22, (2007).
13. S. Shimanskiy, T. IIjima, and Y. Naoi, "Development of acoustic leak detection and localization methods for inlet piping of Fugen nuclear power plant", *Journal of Nuclear Science and Technology*, **Vol. 41**, pp. 183-195, (2004).
14. S. J. Vahaviolos, S. E. Kattis, M. F. Carlos, D. A. Kourousis, A. A. Anastasopoulos, J. W. Dong, "Loose parts and valve flow monitoring in nuclear power plants using integrated digital systems", *Proceedings of 17th World Conference on Nondestructive Testing*, Shanghai, China, Oct. 25-28, (2008).
15. D. N. Fry, R.C. Kryter, and J.C. Robinson, "Analysis of neutron-density oscillations resulting from core barrel motion in a PWR nuclear power plant", Annals of Nuclear Energy, **Vol. 2**, pp. 341-351, (1975).
16. W. Zhang, M. S. Branicky, and S. M. Phillips, "Stability of Networked Control Systems." *IEEE Contr. Syst. Mag.*, **Vol. 21**, pp. 84-99, (2001).
17. J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems", Proceedings of the IEEE **Vol. 95**, pp. 138-162, (2007).
18. H. E. Garcia, A. Ray, and R. M. Edwards, "A reconfigurable hybrid system and its application to power plant control", *IEEE Transactions on Control System Technology*, **Vol. 3**, pp 157-170, (1995).
19. Bobcock and Wilcox Cross Training Manual, Chapter 9, Integrated control system, United States Nuclear Regulatory Commission, (2011).
20. "10 Code of Federal Regulation, part 50", Office of the Federal Register, Revised as of January1, (2011).
21. J. Salewski, W. Ehrenberger, F. Saglietti, J. Gorski, and A. Kornecki, "Safety of computer control systems: challenges and results in software development", *Annal Reviews in Control*, **Vol. 27**, pp. 23-37, (2003).
22. J. Lafontaine, J. Côté, A. Kron, P. Vuilleumier, S.Santandrea, P. V. Braembussche, "Validation of innovative state estimation and control techniques on PROBA-2", *Proceedings of the 6th International ESA Conference on Guidance, Navigation and Control Systems,* Loutraki, Greece, October 17-20 (2005).
23. W.R. Corcoran, N.J. Porter, J.F. Church, M.T. Cross, and W.M. Guinn, "The critical safety functions and plant operation", *Nuclear Technology*, **Vol. 55**, pp. 690-712, (1981).

24. A.L. Tits, and Y. Yang, "Globally convergent algorithms for robust pole assignment by state feedback," IEEE. Trans. on Automatic Control", *IEEE Transactions on Automatic Control*, **Vol. 41**, pp. 1432-1452, (1996).

25. J. A. E. Bryson, and Y.C. Ho, *Applied optimal control: optimization, estimation and control*. Hemisphere Publishing Corporation, (1975).

26. K. Zhou, J. C. Doyle and K. Glover, *Robust and Optimal Control*. Prentice Hall, New Jersey, (1996).

27. F. H. Bauer, J. Bristow, D. Folta, , K. Hartman, D. Quinn, and J.P. How, "Satellite Formation Flying Using an Innovative Autonomous Control System (AUTOCON) Environment," Proceedings of AIAA GN&C Conference, Dan Diego, August, pp. 1-9, (1996).

28. McAfee Foundstone Professional Services and McAfee Labs, "Global energy cyberattacks: night dragon", http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

29. Nicolas Falliere, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier," Version 1.4, (2011). http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

30. M.A. McQueen and W.F. Boyer, "Deception used for cyber defense of control systems", *Proceedings of Human System Interface,* Catania, Italy, May 21-23, pp. 624-631, (2009).

31. K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control system (ICS) security", *NIST* Second public draft, Gaithersburg, MD, (2007).

32. E.A. Lee, "Cyber physical systems: design challenges", *Proceedings of 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing*, Orlando, FL, May 5-7, pp. 363-369, (2008).

33. D. A. Copinger and D.L. Moses, "Fort Saint Vrain Gas Cooled Reactor Operational Experience", NUREG/CR-6839, U.S. Nuclear Regulatory Commission, Washington D.C., (2003).

34. E.J. Lefferts, F.L. Narkley, and M.D. Shuster, "Kalman filtering for spacecraft attitude estimation", *Journal of Guidance, Control and Dynamics*, **Vol. 5**, pp. 417-429, (1982).

35. W. Hernandez, "A survey on optimal signal processing techniques applied to improve the performance of mechanical sensors in automotive applications", *Sensors*, **Vol. 7**, pp. 84-102, (2007).

36. A. V. Oppenheim, and R. W. Schafer, *Discrete-Time Signal Processing*. Prentice Hall Press, Upper Saddle River, NJ, USA, 2009.

37. T. Fujie, "Keynote speeches: Nuclear safety development in the Japanese nuclear industry", *ICI 2011*, Daejeon, August 21-25, (2011).

38. L. M. Stevens, "HTGR resilient control system strategy", *INL/EXT-10-19645*, Idaho National Laboratory, (2010).