Integrated Robust and Resilient Control of Nuclear Power Plants for Operational Safety and High Performance

Xin Jin, *Student Member, IEEE*, Asok Ray, *Fellow, IEEE*, and Robert M. Edwards

***Abstract*—This paper presents an integrated robust and resilient control strategy to enhance the operational safety and performance of nuclear power plants. The objective of robust control is to minimize the sensitivity of plant operations to exogenous disturbances and internal faults while achieving a guaranteed level of performance with a priori specified bounds of uncertainties. On the other hand, the role of resilient control is to enhance plant recovery from unanticipated adverse conditions and faults as well as from emergency situations by altering its operational envelope in real time. In this paper, the issues of real-time resilient control of nuclear power plants are addressed for fast response during emergency operations while the features of the existing robust control technology are retained during normal operations under both steady-state and transient conditions. The proposed control methodology has been validated on the International Reactor Innovative & Secure (IRIS) simulator of nuclear power plants.**

***Index Terms*—Emergency operation, nuclear power plant, operational safety, resilient control, robust control.**

ACRONYMS

BIBO	Bounded-input bounded-output.
FSM	Finite state machine.
IRIS	International reactor innovative & secure.
LFT	Linear fractional transformation.
LOFA	Loss-of-flow accident.
MIMO	Multi-input multi-output.
RCP	Reactor coolant pump.
SISO	Single-input single-output.

NOMENCLATURE

The variables that are used in the controller design procedure, described in Sections II and IV-B, are listed below.

$C(s)$	Low pass filter.
$\mathbb{C}, \mathbb{R}$	Field of complex and real numbers.
d	Disturbances and uncertainties.
e	Tracking error.
$Fl(P,K)$	Lower LFT of plant P and controller K.
$G(s)$	Strictly proper transfer function.
$K(s)$	Robust controller.
$M(s)$	Minimum-phase stable transfer function matrix.
$P_0(s)$	Nominal plant.
$P(s)$	Augmented plant.
$\tilde{P}$	Solution of algebraic Lyapunov equation.
r, w_r	Reference Signals.
T	Temperatures of the nuclear power plant.
T_s	Sampling time.
u	Controller outputs.
u_{rob}, u_{res}	Outputs of robust and resilient controllers.
w_d	Disturbances.
w_n	Sensor noise.
w_u	Uncertainty input of $P(s)$.
W_c	Control action weighting function.
W_n	Sensor noise weighting function.
W_e	Tracking error weighting function.
W_u	Uncertainty in plant modeling.
$y, \hat{y}$	Measurement of plant output and its estimate.
$\tilde{y}$	Output estimation error
y_d	Desired plant output following a desired model.
z_c	Weighted control action.
z_e	Weighted tracking error.
z_u	Uncertainty output of $P(s)$.
γ	H_∞-norm of a transfer matrix operator.

Manuscript received November 12, 2009; revised January 24, 2010. Current version published April 14, 2010. This work was supported in part by the U.S. Department of Energy under NERI-C Grant DE-FG07-07ID14895 and by NASA under Cooperative Agreement NNX07AK49A. Any opinions, findings and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the sponsoring agencies.

The authors are with the Department of Mechanical and Nuclear Engineering, The Pennsylvania State University, University Park, PA, 16802 USA (e-mail: xuj103@psu.edu; axr2@psu.edu; rmenuc@engr.psu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TNS.2010.2042071

δ	State transition function of the FSM.
Δ	Set of all possible uncertainty $(diag\{\Delta_u, \Delta_p\})$.
Δ_u	Block structure of plant uncertainties.
Δ_p	Block structure of performance objectives.
μ	Structured singular value.
$\sigma, \hat{\sigma}$	Vector of adaptive parameters and its estimate.
τ	Time constants.

I. Introduction

NUCLEAR power plants are complex dynamical systems with many variables that require dynamical adjustments to achieve safety and efficiency over the entire operational envelope because their stability and performance could be severely limited by a wide variety of safety requirements, operating conditions, internal faults, and exogenous disturbances. To achieve the specified goals, multiple control variables are simultaneously manipulated for generating the required power and enabling the plant to exploit alternate decision and control strategies. These strategies are often dictated by economy and safety of plant operations. For example, feedback regulation of nonlinear dynamics (e.g., control of reactor power and thermal hydraulics in the balance of plant) could lead to static bifurcation, which is linked to degeneracy in the system's zero dynamics [1].

When faced with unanticipated situations, such as equipment failures or large exogenous disturbances to the plant control system, the human operators are required to carry out diagnostic and corrective actions. Even experienced operators could be overwhelmed by the sheer number of display devices and sensor outputs to be monitored. An intelligent decision and control system with a large degree of autonomy could enhance the operational safety and performance of nuclear plants by alleviating the burden of human operators and simultaneously mitigating the adverse consequences at an incipient stage.

Several researchers have reported intelligent decision and control methods (e.g., optimal control [2], fuzzy logic [3], neural networks [4], and model predictive control [5]) to enhance operational safety and performance of nuclear power plants. Along this line, robust control techniques have also been investigated [6], [7], where the role of a robust controller is to achieve disturbance rejection by reducing sensitivity of the plant control system (i.e., plant plus controller) to exogenous disturbances and internal faults. The task is to synthesize a robust decision and control law on an infinite-time horizon by:

- Mitigation of the detrimental effects of uncertainties and exogenous disturbances;
- Trade-offs between plant stability and performance within specified bounds of uncertainties [8].

However, stability and performance robustness of such control algorithms may not be assured beyond the a priori specified bounds of uncertainties and disturbances; usually larger are the bounds, lower is the plant performance and plant instability is less likely. Therefore, the bounds of structured and unstructured uncertainties are usually specified design parameters for trade-off between stability and performance, and are often based on nominal and off-nominal plant operations that may include at most a few anticipated abnormalities. In the event of a plant accident, the deviations from the nominal plant operating conditions may significantly exceed these uncertainty bounds. Hence, immediate actions beyond the regime of robust control are needed for operational safety and subsequent restoration of normalcy to the original operational mode or to a gracefully degraded mode.

Guo *et al.* [9] have investigated resilient propulsion control of aircraft to determine on how engine control systems can improve safe-landing probabilities under adverse conditions. The key idea is as follows: In emergency situations, the conservative procedure of engine control may not be suitable for aircraft safety; it may be advantageous to compromise the engine health to save the aircraft. The aim of their research is to develop adaptive engine control methodologies to operate the engine beyond the normal domain for emergency operations to enhance safe landing at the expense of possibly partial damage in the aircraft. Motivated by this idea, resilient controllers can be designed for nuclear power plants to ensure the operational safety by "sacrificing" performance under adverse conditions. Recently, Hovakimyan and coworkers [10] have reported a control algorithm called $\mathcal{L}_1$-adaptive control to address the issues in Integrated Resilient Aircraft Control (IRAC) that is an active area of research in National Aeronautics and Space Administration (NASA). It is noted that the notion of resilience, introduced in the present context, is entirely different from being non-fragile or insensitive to some errors in the nominal state-space matrices of controller during implementation [11].

The role of the proposed resilient control in a nuclear power plant is to enhance recovery of the control system from unanticipated adverse conditions and faults as well as from emergency situations by altering its operational envelope in real time [12]. Resilient decision and control laws are synthesized on a finite-time horizon as augmentation of robust decision and control with the objectives of:

- Reliable and fast recovery from adverse conditions and emergency situations;
- Restoration of the control configuration upon returning to normalcy or upon graceful degradation within design specifications.

This paper addresses the issues of real-time resilient control of nuclear power plants for fast response during emergency operations while the features of the existing robust controller are retained during normal operating conditions. The goal is to formulate and validate resilient and reconfigurable control algorithms toward deployment of real-time controllers for emergency recovery of nuclear plants from expected and unexpected adverse conditions.

The integrated robust and resilient control strategy, developed in this paper, has been tested on the International Reactor Innovative & Secure (IRIS) simulator [13], [14] that is built upon one of the next generation nuclear reactor designs for a modular pressurized water reactor with an integral configuration. Currently, IRIS is in the stage of pre-application licensing with Nuclear Regulatory Commission (NRC); its safety testing for

Design Certification (DC) is expected to be completed by 2010 with deployment in the 2015–2017 time frame.

The major contributions of the paper are delineated below:

- Introduction of the innovative concept of resilient control in nuclear plant control for fast recovery from unanticipated adverse conditions and emergency situations.
- Extension of the concept of robustness by integration with resilience for control of nuclear power plants under both normal operations and emergency situations.
- Validation of the concept of integrated robust and resilient control of nuclear power plants on the IRIS simulator.

The paper is organized in five sections including the present one. Section II presents underlying principles of robust control and resilient control. Section III addresses integration of robust control and resilient control strategies. Section IV presents testing and validation of these strategies on the IRIS simulator. The paper is summarized and concluded in Section V.

II. Robust and Resilient Control

This section introduces the underlying principles of multivariable robust control and resilient control for nuclear power plants, where robust controllers are designed by the H_∞-based μ-synthesis method [8] and resilient controllers are designed by $\mathcal{L}_1$-adaptive output feedback algorithm [10]. A finite state machine is then used to integrate the above two controllers for normal operation and emergency recovery from both expected and unexpected adverse conditions while bumpless transfer between the control modes is assured by usage of smoothing filters.

A. Robust Multivariable Control Using μ-Synthesis

In this paper, a μ-synthesis robust control approach is used to synthesize the feedback controller. The plant uncertainties, including the effects of unmodeled dynamics, linearization, and model reduction, are characterized and estimated. Based on the specified uncertainties, robust multivariable controllers are designed using D-K iteration [8] based on the stability and performance specifications. The order of the synthesized controllers is then reduced to an acceptable level by Hankel norm approximation [15].

1) Uncertainty Modeling: Uncertainties due to the inability to model relevant dynamics in an actual plant and the simplification to achieve a mathematical representation, including linearization and model reduction, are taken into consideration for synthesis of robust controllers. Consequently, robustness of the synthesized controller is dependent on the type and size of the uncertainties.

In the controller design for nuclear power plants, Shyu and Edwards [7] considered three types of uncertainties due to unmodeled dynamics, linearization, and model reduction, respectively. These uncertainties contribute to the deviation between the real plant and its reduced-order linear model, based on which the robust controller is synthesized. The unmodeled uncertainties are obtained from the modeling process where the governing equations are derived to represent the plant dynamics including the errors induced by linearization and model reduction.

Unstructured uncertainties, represented by the difference of the magnitude of input-output frequency response at each frequency point, are used in this paper. This bound is defined by the norm of the uncertainty matrix. The overall uncertainty bound is chosen to cover the summation of all uncertainties considered above, i.e.,

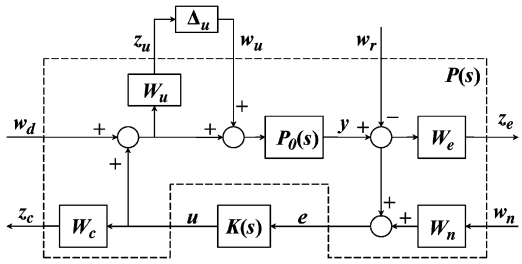

Fig. 1. Closed-loop system interconnection diagram.

$$|\Delta_u| \geq |\Delta_M| = |\Delta_{Lin}| + |\Delta_{Red}| + |\Delta_{Umd}| \tag{1}$$

where Δ_u is bound of the overall uncertainty, Δ_M is the overall uncertainty which is the summation of the magnitudes of linearization uncertainty Δ_{Lin}, model reduction uncertainty Δ_{Red}, and unmodeled uncertainty Δ_{Umd}.

The uncertainty bounds are defined as in (2) in a diagonal matrix form to cover the overall uncertainty. For the purpose of robust controller design, it is advantageous to normalize uncertainty with a frequency dependent weighting function $W_u(s)$:

$$\Delta_u = diag\,(\Delta_{u1}(s), \ldots, \Delta_{un}(s)) = W_u(s)\delta_u \tag{2}$$

where $W_u(s) = diag(W_{u1}(s), \ldots, W_{un}(s))$, and $\delta_u = diag(\delta_{u1}, \ldots, \delta_{un})$.

2) Performance Specifications: Selection of weighting functions and interconnection of the closed-loop system is an essential step in the synthesis of a robust controller. The weighting functions that specify the plant uncertainty and performance specifications invariably need to be adjusted iteratively. Fig. 1 shows the block diagram of closed-loop control system with performance specifications, as explained below.

- The uncertainty weighting function W_u represents the integrated uncertainty bound.
- The tracking error weighting function W_e specifies the performance requirements, which is chosen in such a way that the steady-state tracking errors in both channels should be small (e.g., on the order of 0.01 or less).
- The control action weighting function W_c is used to attenuate the control action efforts. That is, if the control action is excessive, W_c is tuned offline to penalize the control efforts, and conversely if the plant response is sluggish.
- The sensor noise weighting function W_n represents the frequency-dependent effects to filter the measurement noise.

Upon selection of the above weighting functions, the nominal plant model $P_0(s)$ can be interconnected with the weighting functions (i.e., W_u, W_e, W_c, and W_n) to generate the augmented plant $P(s)$, as shown in Fig. 1, where the input and output of $P(s)$ are:

$$w = \begin{bmatrix} w_d \\ w_n \\ w_r \\ w_u \end{bmatrix} \begin{matrix} -\text{disturbance} \\ -\text{noise} \\ -\text{reference} \\ -\text{uncertainty} \end{matrix} \qquad z = \begin{bmatrix} z_c \\ z_e \\ z_u \end{bmatrix} \begin{matrix} -\text{weighted control} \\ -\text{weighted error} \\ -\text{uncertainty} \end{matrix}$$

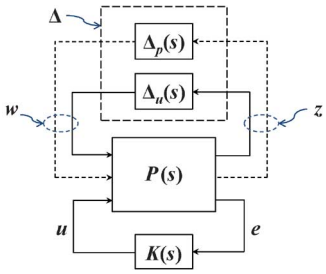

Fig. 2. LFT description of the robust control problem.

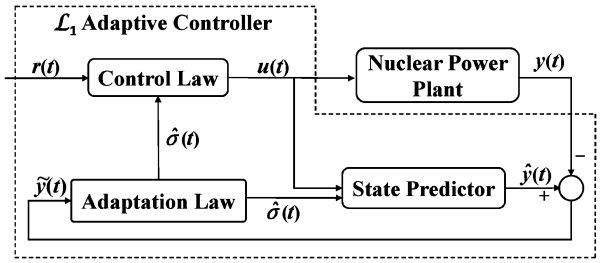

Fig. 3. Closed-loop system with the $\mathcal{L}_1$-adaptive controller.

u is the control input from controller, y is the measurement of plant output, and e is the tracking error.

The robust control problem is formulated in a two-port framework using linear fractional transform (LFT) [8], as shown in Fig. 2. Let n_{z_1} and n_{w_1} denote the numbers of outputs and inputs of the uncertainty weighting function, respectively, and n_{z_2} and n_{w_2} denote the numbers of output and input of the performance specification weighting functions, respectively. Then, the block structure Δ of the uncertainty model is defined as:

$$\Delta=\left\{\begin{bmatrix}\Delta_u & 0\\ 0 & \Delta_p\end{bmatrix}:\Delta_u\in\mathbb{C}^{n_{z_1}\times n_{w_1}},\Delta_p\in\mathbb{C}^{n_{z_2}\times n_{w_2}}\right\} \quad (3)$$

The first block of the uncertainty matrix corresponds to the uncertainty block Δ_u, used in modeling the plant uncertainty. The second block Δ_p includes the performance objectives in the framework of the μ-synthesis [8]. The inputs to the second block are the weighted control action z_c and weighted tracking error z_e, and the outputs are the reference w_r, disturbance w_d and sensor noise signals w_n.

3) Controller Design Using μ-Synthesis: To meet the control objectives, a stabilizing controller K is synthesized such that, at each frequency $\omega\in[0,\infty]$, the structured singular value satisfies the following condition:

$$\mu_{\Delta_p}\left[F_L(P,K)(j\omega)\right]<1 \quad (4)$$

where $F_L(P,K)$ represents the linear fractional transformation (LFT) [8] of P and K. The fulfillment of this condition guarantees robust performance of the closed-loop control system. The μ-synthesis can be accomplished by using the D-K iteration tool in MATLAB [15]. For faster computation, the controller order could be reduced by eliminating the insignificant states by balanced realization and Hankel norm approximation [8], [15].

B. Resilient Control

The role of resilient control is to enhance recovery of the control system from unanticipated adverse conditions and faults as well as from emergency situations. Therefore, the resilient controller should be re-configurable to accommodate wide-range operations and faulty conditions, and this requires the resilient controller to be both robust and adaptive. Recently, Hovakimyan *et al.* [10] have developed a novel control algorithm, called $\mathcal{L}_1$-adaptive control, to address the issues in Integrated Resilient Aircraft Control (IRAC). The advantages of $\mathcal{L}_1$-adaptive controller are: (i) guaranteed fast adaptation, and (ii) simultaneous tracking of the input and output signals that are uniformly bounded. Since the $\mathcal{L}_1$-controller is both robust and adaptive, it is suitable for resilient control.

1) $\mathcal{L}_1$-Adaptive Output Feedback Control: The $\mathcal{L}_1$-adaptive control architecture was first presented by Cao and Hovakimyan [10] using a state feedback approach in systems with constant unknown parameters. Later, the $\mathcal{L}_1$-adaptive control has been extended to nonlinear time-varying systems in the presence of multiplicative and additive unmodeled dynamics [16]. Its extension to output feedback control has been presented for a class of uncertain systems [17] that allows for tracking arbitrary reference with guaranteed time-delay margin. In the work reported in this paper, the $\mathcal{L}_1$-output feedback adaptive control architecture has been employed to address the challenge of resilient control of nuclear power plant, as shown in Fig. 3. While details on the $\mathcal{L}_1$-adaptive controller are reported in recent literature [10], [16], [17], the salient features are explained in terms of the following single-input single-output (SISO) system model.

$$y(s)=G(s)\left(u(s)+d(s)\right) \quad (5)$$

where $u(t)\in\mathbb{R}$ is the control input, $y(t)\in\mathbb{R}$ is the system output, $G(s)$ is a strictly proper unknown transfer function of unknown relative degree n_{ar} for which only a known lower bound $1<n_r\leq n_{ar}$ is available, and $d(t)$ is the time-dependent disturbances and uncertainties. With a slight abuse of notation, Laplace transforms of $u(t)$, $y(t)$, and $d(t)$ are respectively denoted as $u(s)$, $y(s)$, and $d(s)$.

Let $r(t)$ be a given bounded continuous reference input signal. The control objective is to design an adaptive output feedback controller giving $u(t)$ such that the system output $y(t)$ tracks the reference input $r(t)$ following a desired model:

$$y_d(s)=M(s)r(s) \quad (6)$$

where $M(s)$ is a minimum-phase stable transfer function of relative degree $n_r>1$. The system equations in terms of the desired model are rewritten as:

$$y(s)=M(s)\left(u(s)+\sigma(s)\right) \quad (7)$$

where $\sigma(s)=M^{-1}(s)(G(s)-M(s)u(s)+M(s)G(s)d(s))$ is the disturbance.

Closed-Loop Reference System: Let $u_{ref}(s)$ and $\sigma_{ref}(s)$ be the reference control input and reference disturbance, respectively, of the closed-loop reference system that defines an achievable control objective for the $\mathcal{L}_1$-adaptive controller such that:

$$\begin{aligned} y_{ref}(s) &= M(s)\left(u_{ref}(s)+\sigma_{ref}(s)\right) \\ \sigma_{ref}(s) &= \left(\left(G(s)-M(s)\right)u_{ref}(s)+G(s)d_{ref}(s)\right)/M(s) \\ u_{ref}(s) &= C(s)\left(r(s)-\sigma_{ref}(s)\right) \end{aligned} \tag{8}$$

where $C(s)$ is a low pass filter with DC gain $C(0)=1$ and $d_{ref}(t)=f(t,y_{ref}(t))$ is a (possibly) time-varying function of the reference output $y_{ref}(s)$.

The transfer matrices $C(s)$ and $M(s)$ are selected such that

$$H(s)=G(s)M(s)/\left(C(s)G(s)+\left(1-C(s)\right)M(s)\right) \tag{9}$$

is stable and that the $\mathcal{L}_1$-gain of the cascaded system is upper bounded as:

$$\left\|H(s)\left(1-C(s)\right)\right\|_{\mathcal{L}_1}<1 \tag{10}$$

Then, the reference system in (8) is stable.

Referring to Fig. 3, individual components of the $\mathcal{L}_1$-adaptive controller are described next.

State Predictor (Passive Identifier): Let ($A_m\in\mathbb{R}^{m\times n}$, $b_m\in\mathbb{R}^n$, $c_m\in\mathbb{R}^n$) be the minimal realization of the stable transfer matrix $M(s)$. Hence, (A_m,b_m,c_m) is controllable and observable with A_m being Hurwitz. Then, the system in (5) is rewritten in the state-space setting as:

$$\begin{aligned} \dot{x}(t) &= A_m x(t)+b_m\left(u(t)+\sigma(t)\right) \\ y(t) &= c_m^T x(t) \end{aligned} \tag{11}$$

and the associated state predictor is given by:

$$\begin{aligned} \dot{\hat{x}}(t) &= A_m\hat{x}(t)+b_m\left(u(t)+\hat{\sigma}(t)\right) \\ \hat{y}(t) &= c_m^T\hat{x}(t) \text{ and } \tilde{y}(t)=\hat{y}(t)-y(t) \end{aligned} \tag{12}$$

where $\hat{\sigma}(t)\in\mathbb{R}^n$ is the vector of adaptive parameters. Notice that, in the state predictor equation $\hat{\sigma}(t)$ may not belong to the space spanned by b_m, while $\sigma(t)$ does belong to the space spanned by b_m in (11).

Adaptation Law: Let $\tilde{P}$ be the solution of the following algebraic Lyapunov equation:

$$A_m^T\tilde{P}+\tilde{P}A_m^T=-Q \tag{13}$$

where $Q>0$. From the properties of $\tilde{P}$ it follows that there always exists a nonsingular $\sqrt{\tilde{P}}$ such that

$$\tilde{P}=\sqrt{\tilde{P}}^T\sqrt{\tilde{P}} \tag{14}$$

Given the vector $c_m^T(\sqrt{\tilde{P}})^{-1}$, let D be the $(n-1)\times n$-dimensional nullspace of $c_m^T(\sqrt{\tilde{P}})^{-1}$, i.e.,

$$D\left(c_m^T(\sqrt{\tilde{P}})^{-1}\right)^T=0 \tag{15}$$

and let

$$\Lambda=\begin{bmatrix} c_m^T \\ D\sqrt{\tilde{P}}\end{bmatrix}\in\mathbb{R}^{n\times n} \tag{16}$$

The update law for $\hat{\sigma}(t)$ at sampling instant (with $T_s>0$ being the sampling time) as:

$$\hat{\sigma}(iT_s)=-\Phi^{-1}(T_s)\mu(iT_s),\quad i=1,2,\ldots \tag{17}$$

where the state transition matrix

$$\Phi(T_s)\triangleq\int_0^{T_s}e^{\Lambda A_m\Lambda^{-1}(T_s-\tau)}\Lambda d\tau \tag{18}$$

and

$$\mu(iT_s)\triangleq e^{\Lambda^{-1}T_s}\underline{1}_1\tilde{y}(iT_s),\quad i=1,2,\ldots \tag{19}$$

where $\underline{1}_1$ denotes a Cartesian basis vector in $\mathbb{R}^n$ with its first element equal to 1 and other elements being 0.

Control Law: The control law is defined via the output of the low-pass filter:

$$u(s)=C(s)r(s)-\frac{C(s)}{M(s)}c_m^T(s\mathbb{I}-A_m)^{-1}\hat{\sigma}(s) \tag{20}$$

The complete $\mathcal{L}_1$-adaptive controller consists of the state predictor in (12), the adaptation law in (17), and the control law in (20), subject to the $\mathcal{L}_1$-gain upper bound in (10). The performance bounds of the $\mathcal{L}_1$-adaptive output feedback controller are given by the following theorem:

Theorem 2.1 (Theorem 1 and Lemma 3 in [17]):

$$\begin{aligned} \lim_{T_s\to 0}\left(\|\tilde{y}\|_{\mathcal{L}_\infty}\right)&=0 \\ \lim_{T_s\to 0}\left(\|y-y_{ref}\|_{\mathcal{L}_\infty}\right)&=0 \\ \lim_{T_s\to 0}\left(\|u-u_{ref}\|_{\mathcal{L}_\infty}\right)&=0 \end{aligned} \tag{21}$$

where $\|\bullet\|_{\mathcal{L}_\infty}$ denotes the $\mathcal{L}_\infty$ norm (i.e., essential supremum of the absolute value) of the function $\bullet$.

III. Integration of Robust and Resilient Control

This section describes how the robust controllers and resilient controllers are integrated. A finite-state machine (FSM) [18] has been adopted for discrete decision-making, which monitors the conditions of the nuclear power plant via a fault detector and controls the bumpless transfer between the robust and resilient

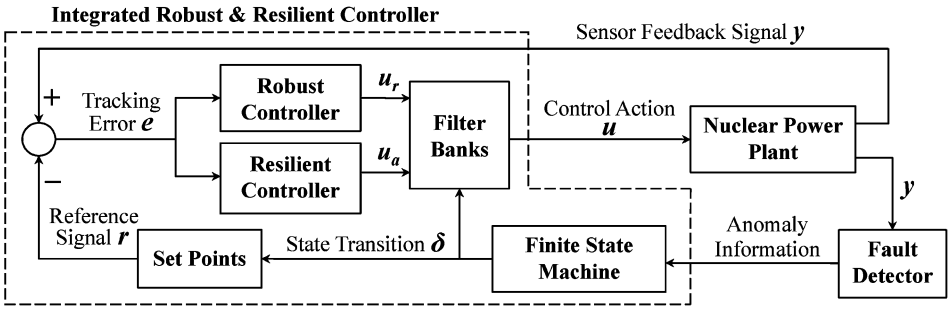

Fig. 4. Layout of the integrated robust and resilient control system.

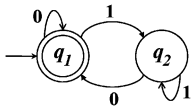

Fig. 5. Example of a finite state machine (FSM).

controllers. Fig. 4 depicts the layout of an integrated robust and resilient control system that includes the robust controller, resilient controller, fault detector, finite state machine (FSM), a set of reference points, and a filter bank for bumpless transfer. The fault detector is extrinsic to both robust and resilient controllers.

A. Finite State Machine

A finite state machine (FSM) [18] is a 5-tuple $(Q, \Sigma, \delta, q_0, F)$, where Q is a finite set called the states, Σ is a finite set called the alphabet, $\delta : Q \times \Sigma \rightarrow Q$ is the state transition function, $q_0 \in Q$ is the start state, and $F \subseteq Q$ is the set of accepted states or final states.

Fig. 5 shows an example of a finite state machine (FSM) $S = (\{q_1, q_2\}, \{0, 1\}, \delta, q_1, \{q_1\})$ that consists of two states q_1, q_2, representing the normal operating condition and an anomalous condition, respectively. The alphabet in this FSM is selected as $\Sigma = \{0, 1\}$, where the symbol 0 represents the normal condition, and the symbol 1 represents the detection of anomaly (e.g., abrupt temperature change in primary coolant flow). A brief explanation of the FSM's operation is presented below.

When the nuclear power plant is in the normal operating condition (i.e., the symbol of the alphabet is 0), the FSM is in state q_1. When an anomaly occurs in the plant, the symbol changes from 0 to 1, and the FSM makes a transition to the anomalous state q_2. Accordingly, the control system takes necessary actions (e.g., change of the feed water flow set point) are taken to keep the nuclear power plant safe according to the above procedure. The FSM stays in state q_2 until the plant is restored to the normal condition when the symbol changes back to 0, and thus the FSM makes the transition back to the normal state q_1. The role of resilient control is to make the transition from state q_1 to state q_2 as quickly and safely as possible to recover from unanticipated adverse conditions/faults and emergency situations by altering its operational envelope in real time. The control configuration is restored upon returning to normalcy if the plant is not damaged, or to a gracefully degraded condition if the plant is partially damaged but still operable within specified safety and performance criteria; this is achieved by returning to state q_1 from state q_2.

B. Bumpless Transfer

Switching from one controller to another should entail as little agitation (i.e., occurrence of undesirable transients) as possible. By parallel operation of a non-active controller one could try to drive its output signals towards the "correct" amplitude, so that the resulting transients of the closed loop due to a transfer of authority are as small as possible. This is known as the *bumpless transfer* problem for transition from one operating mode to another.

Many bumpless transfer techniques have been developed for application in scenarios with different constraints, such as switching between manual and automatic control, filter and controller tuning, scheduled and adaptive controller [19]. In this paper, a piecewise linear filter is constructed to mitigate the transients during switching between the robust controller and the resilient controller. The key idea is explained below.

While the robust controller is active to perform in both steady state and transient conditions under normal operation, the resilient controller becomes active to provide safety and recovery to the plant during adverse conditions and emergency situations. In order to achieve bumpless transfer from robust control to resilient control and avoid abrupt changes in control actions, piecewise linear filters are added to the controller outputs. The resulting control action $u(s)$ is formulated as:

$$u(s) = G_{res}(s)\, u_{res}(s) + G_{rob}(s)\, u_{rob}(s) \qquad (22)$$

where u_{res} and u_{rob} are outputs of the resilient controller and robust controller, respectively, and G_{res} and G_{rob} are the filter transfer functions for the respective control actions.

C. Integrated Robust and Resilient Control Strategy

Following Fig. 4, the next task is to incorporate the finite state machine (FSM) and filter banks within the plant control system for bumpless transfer between the robust and resilient controllers. For example, upon detection of a loss-of-flow accident (LOFA), as the primary coolant temperature crosses a specified threshold, this information activates the transition between states of the FSM. The state transition function δ provides inputs to both blocks, namely, set points and filter banks, as seen in Fig. 4. If a significant fault or emergency situation is detected in the plant, the state transition in the FSM initiates a bump-

less transfer between the two controllers and may also alter the thresholds in the set points module. The altered thresholds are then used as the new set points for the controller under the abnormal condition. Upon return to normalcy, robust control with the original set points are resumed. In practice, a fault detection system is needed to identify an abnormal incident as early as possible, which necessitates incorporation of a fault detection scheme within the integrated robust and resilient system. This is a topic of future research.

IV. Testing and Validation on the IRIS Simulator

The proposed integrated robust and resilient control strategy has been tested and validated on a simulator of nuclear plants. The results of simulation are presented and further experimental validation is planned on research reactors (e.g., Penn State's TRIGA research reactor [20]) in the future.

A. The International Reactor Innovative & Secure Simulator

The International Reactor Innovative & Secure (IRIS) simulator of nuclear power plants is based on the design of a next-generation nuclear reactor. It is a modular pressurized water reactor (PWR) with an integral configuration of all primary system components. Fig. 6 shows the layout of the primary side of the IRIS system that is offered in configurations of single or multiple modules, each having a power rating of 1000 MWt (about 335 MWe) [14]. The nominal reactor core inlet and outlet temperatures are 557.6°F (292°C) and 626°F (330°C), respectively. The pressurizer, eight steam generators, and the control rod mechanism are integrated into the pressure vessel with the reactor core. There is no huge pipe used to connect these components. This design avoids the large loss of coolant accident (LOCA). The whole control rod mechanism is mounted inside the pressure vessel to avoid failures of the control rod head penetration.

As shown in Fig. 6, the integral design of the primary side also makes the containment vessel much smaller than the traditional pressure vessel of a PWR. The IRIS reactor coolant pumps are of the spool type, and are located entirely within the reactor vessel; only small penetrations for the electrical power cables are required. The spool pump geometric configuration provides high inertia/coastdown and high run-out flow capability that contributes to minimize or even mitigate the negative consequences of loss-of-flow accidents (LOFAs).

A simulation testbed for testing and validation of control algorithms has been developed under the project of Nuclear Energy Research Initiative (NERI). The testbed is built using MATLAB/SIMULINK. This SIMULINK model includes a reactor core model, a helical coil steam generator (HCSG) model. The turbine is not explicitly modeled in the testbed since the reactor's operational safety is the major focus of this paper. The simulation testbed is implemented on a Quad Core 2.83 GHz CPU 8 GB RAM Workstation in the laboratory of Penn State. Another two workstations with the same configuration are also available for simulating a twin-unit plant operation scenario, in which two workstations host an individual IRIS module, and the third one hosts the controller to coordinate the plant modules through a local network. This testbed is capable of

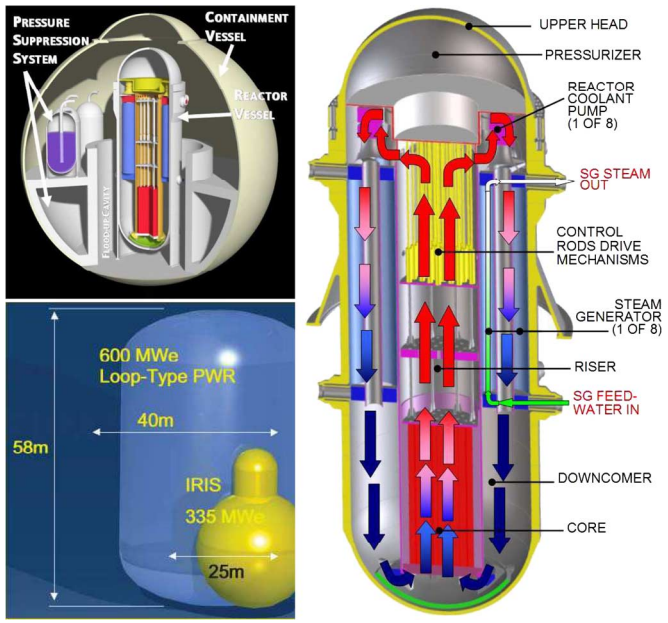

Fig. 6. Layout of the primary side of the IRIS system [14].

simulating normal operation conditions at different operational modes as well as various faulty scenarios including:

- Actuator failures: Feedwater pump trip, malfunctions of reactor coolant pump and control rod mechanism;
- Sensor failures: Malfunctions of temperature, pressure, and flow-rate sensors;
- Internal faults: Uncertainties in fuel temperature coefficient of reactivity, coolant heat capacity, and feedwater heat capacity.

B. Design of the Integrated Robust and Resilient Control System

The details of the integrated control system design are introduced in this section.

1) Robust Controller Design: The design of a robust controller requires judicious selection of the uncertainty weighting function (W_u) and the performance weighting functions, W_e, W_c and W_n. These weighting functions essentially serve as user-selected performance specifications.

The uncertainty weighting function $W_u(s)$ is selected to capture the frequency-dependent uncertainties as:

$$W_u(s) = \begin{bmatrix} \frac{0.1(s+60)}{s+600} & 0 \\ 0 & \frac{0.1(s+60)}{s+600} \end{bmatrix} \tag{23}$$

In order that the plant output y tracks the given reference signal r, the tracking error weighting functions with respect to each plant output are chosen and put into a form of the diagonal matrix $W_e(s)$ as:

$$W_e(s) = \begin{bmatrix} \frac{100(s+1)}{1000s+1} & 0 \\ 0 & \frac{100(s+1)}{1000s+1} \end{bmatrix} \tag{24}$$

This weighting function indicates that the steady-state (i.e., low-frequency) tracking errors due to reference step-inputs in either

TABLE I
RESULTS OF THE μ-SYNTHESIS

Iteration #	Controller Order	γ-value	μ-value
1	30	2.441	1.515
2	30	1.030	1.021
3	30	0.979	0.984
4	30	0.986	0.988
5	30	0.978	0.981
6	30	0.984	0.986

TABLE II
ORDER REDUCTION OF CONTROLLER #5

Reduced Order	μ-value after reduction
30	0.9812
10	0.9812
8	0.9826
7	0.9828
6	0.9877
5	1.0311

channel should be on the order of 0.01 or smaller. This performance requirement becomes less stringent at high frequencies.

The control action weighting function W_c is included to tune the control action effort. For example, if the time response of the controlled system displays excessive control action, the weighting function serves to penalize the energy of the oscillation; on the other hand, if the response is sluggish, the weighting function has a more benign role with a significantly reduced penalty. The control action weighting function is selected as:

$$W_c(s) = \begin{bmatrix} \frac{0.0068(10s+1)}{s+1} & 0 \\ 0 & \frac{0.0068(10s+1)}{s+1} \end{bmatrix} \tag{25}$$

In the closed-loop interconnection, effects of frequency-dependent sensor noise are represented by the weighting function diagonal matrix $W_n(s)$ as:

$$W_n(s) = \begin{bmatrix} \frac{0.0001(10s+1)}{s+1} & 0 \\ 0 & \frac{0.0001(10s+1)}{s+1} \end{bmatrix} \tag{26}$$

An increased sensor noise weight makes the controller more robust to sensor noise possibly at the expense of relatively slow response.

The μ-synthesis design of the robust controller is accomplished by using the D-K iteration tool in MATLAB [15]. For the IRIS plant, the results of D-K iterations are shown in Table I, where γ is the H_∞-norm of the transfer matrix operator that is a measure of the controller's robust stability, and μ is the structured singular value that is a measure of the controller's robust performance. For controllers with $\gamma < 1$ and $\mu < 1$, the robust stability and robust performance are guaranteed. The controller is selected after five D-K iterations as it yields the smallest γ and μ values. The resulting robust controller of order n with m (sensor) inputs and ℓ (control action) outputs in the state space form, where $\ell = m = n = 2$, is shown below:

$$K = \begin{bmatrix} A_{n\times n} & B_{n\times m} \\ C_{\ell\times n} & D_{\ell\times m} \end{bmatrix} \tag{27}$$

As seen in Table I, the synthesized controller yields the closed-loop $\mu = 0.981$ after five iterations and the robust performance of the control system is guaranteed for the prescribed uncertainty and performance. For faster computation, the controller order is reduced by eliminating the insignificant states, where balanced realization and Hankel norm approximation [8], [15] has been used; the results of controller order reduction are listed in Table II. It is seen in Table II that the μ-values do not increase significantly after order-reduction until the controller order is reduced below 10. There is a clear increase in μ as the controller order is reduced from 7 to 6, and the value of μ for controller order less than 6 is greater than 1. Therefore, the controller of reduced order 7 is selected.

2) Resilient Controller Design: The resilient control algorithm in Section II-B is derived for a single-input single-output (SISO) system. However, the plant dynamics of the IRIS model are coupled in two sensor channels, steam pressure and reactor power, which require an extension of the SISO $\mathcal{L}_1$-adaptive output feedback controller to multi-input multi-output (MIMO) systems. The components of the MIMO control system are described below.

Desired System: The matrix transfer function of the desired control system is selected in the following form:

$$M(s) = \begin{bmatrix} M_1(s) & 0 \\ 0 & M_2(s) \end{bmatrix} \tag{28}$$

where $M_1(s)$ and $M_2(s)$ are the scalar transfer functions for corresponding channels of secondary steam pressure and reactor power, where zero non-diagonal elements of the matrix transfer function imply decoupling of the channels in the desired transfer function. In the current design, minimum-phase stable transfer functions of relative degree $n_r = 2 > 1$ are selected as:

$$M_1(s) = M_2(s) = \frac{\omega_M^2}{s^2 + 2\xi_M\omega_M s + \omega_M^2} \tag{29}$$

where $\omega_M = 0.35$, $\xi_M = 2$. The parameter ω_M and ξ_M are chosen in such a way that the frequency response of the desired system is close to that of the linearized IRIS model.

Low-Pass Filter: Following Fig. 4, the low-pass filter bank is selected as:

$$C(s) = \begin{bmatrix} C_1(s) & 0 \\ 0 & C_2(s) \end{bmatrix} \tag{30}$$

$$C_1(s) = C_2(s) = \frac{\omega_C^2}{s^2 + 2\xi_C\omega_C s + \omega_C^2} \tag{31}$$

where $\omega_C = 6$, $\xi_c = 1.6$. The structure and parameters of the low-pass filter are chosen in such a way that system $H(s)$ in (9) is stable and the $\mathcal{L}$-stability condition in (10) is satisfied. Consequently, the closed-loop reference system in (8) is stable.

3) Smoothing Filter Design for Bumpless Transfer: Bumpless transfer between the robust and resilient controllers is

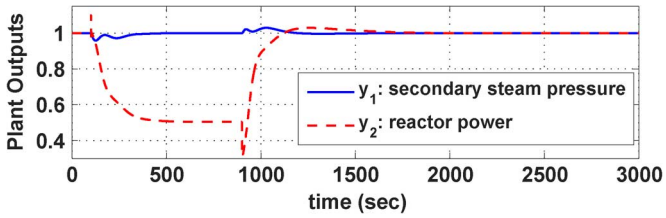

Fig. 7. Normalized plant outputs.

achieved by incorporating smoothing filters. During the transition from a normal condition (i.e., state q_1) to an abnormal condition (i.e., state q_2), the filter transfer functions are chosen as:

$$G_{res}(s) = \frac{1}{s(\tau_1 s + 1)} \text{ and } G_{rob}(s) = \frac{\tau_1}{\tau_1 s + 1} \tag{32}$$

and, during the transition from an abnormal condition (i.e., state q_2) to an normal condition (i.e., state q_1), the filter transfer functions are chosen as:

$$G_{res}(s) = \frac{\tau_2}{\tau_2 s + 1} \text{ and } G_{rob}(s) = \frac{1}{s(\tau_2 s + 1)} \tag{33}$$

such that the control actions during transition stages are actually a linear combination of time-dependent weighted outputs from the controller actions, u_{res} and u_{rob} of the resilient and robust controllers and vice versa. The respective time constants τ_1 and τ_2 are chosen according to performance specifications based on the following rationale: While a large time constant yields slow and smooth transition, a small time constant ensures fast response. In this study, the time constants τ_1 and τ_2 are chosen as 2 sec and 200 sec, respectively. The smaller value of τ_1 represents relatively rapid response that is needed for transition to resilient control to deal with emergency situations. The larger value of τ_2 represents relatively slow response for transition back to robust control as normalcy is restored.

A μ-analysis test confirms that bounded-input bounded-output (BIBO) stability of the augmented closed-loop system is retained after the addition of the filters, G_{res} and G_{rob}. Synthesis of a more advanced filter is a topic of future research.

C. Results of Testing and Validation on the IRIS Simulator

A scenario of loss-of-flow accident (LOFA) for the (closed loop) system has been simulated on the IRIS to evaluate the performance of integrated robust and resilient control algorithm. Example of causes for LOFA are loss of off-site power, pump failure, heat exchanger blockage, pipe blockage, and faulty valve closure. In this simulation, the LOFA is caused by reactor coolant pump (RCP) failure of 4 out of 8 reactor coolant pumps, which is a Condition IV accident. Although this accidental event can be mitigated by the "Safe-by-Design" feature of IRIS [14] (i.e., natural circulation of coolant removes decay heat from the core even when the coolant pump fails), the plant could still be damaged if appropriate control actions are not taken.

In the first 100 sec of the simulation exercise, the nuclear power plant is in a normal operating condition with full output power load and steam pressure load. In the simulated scenario, when four of the eight primary flow pumps fail, the LOFA is detected at $t = 100$ sec and the resulting anomaly information is generated as seen in Fig. 4. The fault detection system is extrinsic to both the robust and resilient controllers, and its incorporation within the integrated control system is a topic of future research.

Upon detection of the LOFA incident, the control output is switched quickly from the robust controller to the resilient controller that promptly reduces the set points of output power load and feedwater flow by half. The plant is brought back to normalcy at $t = 900$ sec when all primary flow pumps become functional. To make the plant return to normalcy, the output power load and feedwater flow set points are reset to their respective nominal values, and the control output is switched bumplessly from the resilient controller back to the robust controller. Note that this bumpless transfer is ensured by the choice of a relatively large filter time constant ($\tau_2 = 200$ sec) relative to the tenure of the LOFA.

Fig. 7 shows the normalized plant outputs, steam pressure y_1 and reactor output power y_2. Under normal conditions, both plant outputs are at their nominal values, which are normalized to 1. When four of the eight primary reactor coolant pumps fail, the plant is not able to generate 100% power, and thus the output power load is reduced to 50% by resilient control actions. Upon returning to normalcy, the output power gradually returns to 100%. Note that there exist spikes in the reactor power y_2 when the anomaly occurs and it is removed. Those spikes are generated due to temperature feedback from the reactor as a consequence of the abrupt change in primary flow when four of the eight pumps fail. Note that, in practice, a change in the feedwater flow may not occur as a step, but may have a relatively more gradual but sufficiently fast profile. Furthermore, if the output power in the control system is taken to be the turbine output power instead of the reactor core output power, the spikes would be averaged out due to the mechanical inertia of the turbine. In the future work, a turbine model will be integrated into the nuclear plant model.

Fig. 8 shows the responses of the control actions, feedwater flow u_1 and rod reactivity u_2, after occurrence of the LOFA. When the plant is operated under normal conditions, the control efforts are indicated as 0% implying zero deviations from the nominal values of u_1 and u_2. Upon detection of the LOFA at $t = 100$ sec, in order to "save" the plant, the feedwater flow is gradually increased by 10% of the nominal value and the rod reactivity is reduced by more than 80% of the nominal value.

Fig. 9 shows the temperatures (i.e., primary coolant inlet, primary coolant outlet, and secondary coolant steam temperatures) monitored by sensors inside the plant, and ΔT is the temperature difference between the primary coolant inlet flow and outlet flow, which is used to activate the FSM (see Figs. 5 and 4). Upon detection of the LOFA, the control system reduces the rod reactivity by more than 80%. Consequently, the primary coolant inlet temperature drops.

As seen in Fig. 10, switching of the symbols (i.e., 0 and 1) of the alphabet are controlled by the FSM. When the plant is working in normal conditions, the symbol is 0, the FSM stays in normal state q_0, and the output power reference point is 1.

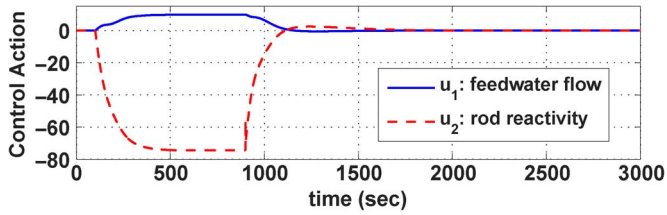

Fig. 8. Control actions of integrated robust and resilient controller.

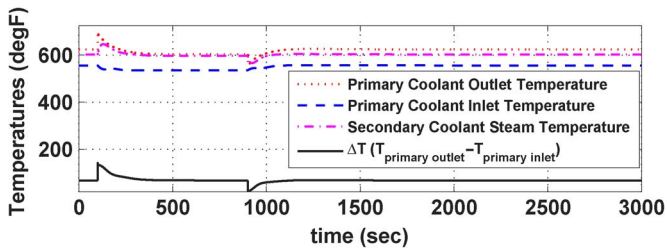

Fig. 9. Temperatures of steam, primary inlet and outlet flows.

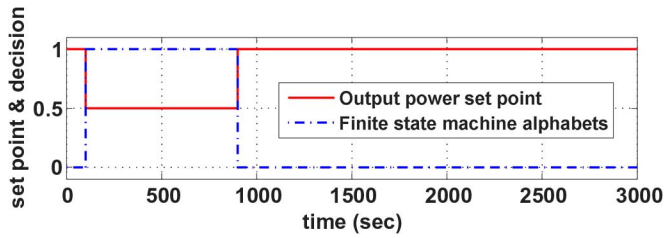

Fig. 10. Finite state machine alphabets and output power set point changes.

When the anomaly occurs, the symbol changes to 1 immediately, which causes the FSM to transit from state q_1 to q_2 and the output power reference point to change from 1 to 0.5.

V. Summary, Conclusions & Future Work

This paper investigates a new concept of integrated robust and resilient control for enhancement of the operational safety and performance of nuclear power plants. The robust controller is designed by using the μ-synthesis tools with D-K iteration [15]. The optimal Hankel approximation is used to reduce the order of the robust controller [15]. The concept of resilient control in nuclear plants is derived from Integrated Resilient Aircraft Control (IRAC) [9] that is an active area of research in National Aeronautics and Space Administration (NASA); this is a direct transfer of technology from aeronautics to nuclear engineering. The resilient control is implemented by $\mathcal{L}_1$-adaptive output feedback controller, which guarantees fast adaptation, uniformly bounded transient and asymptotic tracking for both input and output signals of the control system simultaneously. The robust and resilient controllers are integrated by utilizing a finite state machine and smoothing filters to ensure bumpless transfer from robust to resilient control modes and vice versa. In the simulation example of nuclear power plant control, the finite state machine is designed to switch between normal and abnormal states and activate related control actions by monitoring plant coolant temperatures. The filters ensure bumpless transfer between robust controller and resilient controller and avoid impact to the nuclear reactor during transition stage.

A simple scenario of loss-of-flow accident (LOFA) has been investigated on the International Reactor Innovative & Secure (IRIS) simulator [14]. Simulation results based on this LOFA scenario show that the proposed controller recovers from the emergency situation with a fast response, while the characteristics of the standard robust controller are retained during normal operating conditions. Further analytical, simulation and experimental research is necessary before this novel concept of integrated robust and resilient control can be considered for application to commercial nuclear power plants. The following are a few examples of future research in integrated robust and resilient control of nuclear power plants:

- Incorporation of fault detection schemes within the integrated control system;
- Filter design for fast and stable switching between robust and resilient control modes;
- Construction of finite-state machines for incorporation within the integrated control system to represent various failure states and interstate switching;
- Demonstration of safe recovery from various real-life emergency situations by including balance of plant components in the IRIS simulator;
- Experimental validation of safe recovery under selected accident scenarios on research reactors (e.g., Penn State's TRIGA research reactor [20]).

Acknowledgment

The authors would like to thank Prof. Naira Hovakimyan of the University of Illinois at Urbana Champaign for her technical support in developing the resilient controller. The authors are also grateful to the thoughtful and meticulous comments of the anonymous reviewers.

References

[1] H. G. Kwatny, B.-C. Chang, and S.-P. Wang, "Static bifurcation in mechanical control systems," in *Bifurcation Control*. Berlin, Germany: Springer, 2004, vol. 293, pp. 67–81.

[2] R. M. Edwards, K. Y. Lee, and A. Ray, "Robust optimal control of nuclear reactors and power plants," *Nucl. Technol.*, vol. 98, pp. 137–148, May 1992.

[3] Z.-Y. Huang, R. M. Edwards, and K. Y. Lee, "Fuzzy-adapted recursive, sliding-mode controller design for a nuclear power plant control," *IEEE Trans. Nucl. Sci.*, vol. 51, no. 1, pp. 256–266, Feb. 2004.

[4] K. Hadad, M. Mortazavi, M. Mastali, and A. A. Safavi, "Enhanced neural network based fault detection of a VVER nuclear power plant with the aid of principal component analysis," *IEEE Trans. Nucl. Sci.*, vol. 55, no. 6, pp. 3611–3619, Dec. 2008.

[5] M. G. Na and B. R. Upadhyaya, "Application of model predictive control strategy based on fuzzy identification to an SP-100 space reactor," *Ann. Nucl. Energy*, vol. 33, no. 17–18, pp. 1467–1478, Nov.–Dec. 2006.

[6] R. N. Banavar and U. V. Deshpande, "Robust controller design for a nuclear power plant using H_∞ optimization," *IEEE Trans. Nucl. Sci.*, vol. 45, no. 2, pp. 129–140, Apr. 1998.

[7] S. S. Shyu and R. M. Edwards, "A robust multivariable feedforward/feedback controller design for integrated power control of boiling water reactor power plants," *Nucl. Technol.*, vol. 140, no. 2, pp. 129–140, Nov. 2002.

[8] K. Zhou, J. Doyle, and K. Glover, *Robust and Optimal Control*. Upper Saddle River, NJ: Prentice-Hall, 1996.

[9] T. H. Guo and J. S. Litt, "Resilient propulsion control research for the NASA Integrated Resilient Aircraft Control (IRAC) project," in *Proc. AIAA Conf. and Exhibit*, Rohnert Park, CA, May 7–10, 2007, AIAA-2007–2802.

[10] C. Cao and N. Hovakimyan, "Design and analysis of a novel $\mathcal{L}_1$ adaptive control architecture with guaranteed transient performance," *IEEE Trans. Autom. Control*, vol. 53, no. 3, pp. 586–591, 2008.

[11] M. S. Mahmoud, *Resilient Control of Uncertain Dynamical Systems*. Berlin, Germany: Springer, 2004.

[12] X. Jin, R. Edwards, and A. Ray, "Integrated robust and resilient control for nuclear power plants," in *Proc. 6th ANS Int. Topical Meeting NPIC & HMIT, Paper 3 Session I & C Grid Appropriate Reactor*, Knoxville, TN, Apr. 5–9, 2009.

[13] M. Carelli, "IRIS: A global approach to nuclear power renaissance," *Nucl. News*, vol. 46, no. 10, pp. 32–42, Sep. 2003.

[14] M. D. Carelli, "The design and safety features of the IRIS reactor," *Nucl. Eng. Des.*, vol. 230, pp. 151–167, 2004.

[15] G. J. Balas, J. C. Doyle, K. Glover, A. Packard, and R. Smith, *μ-Analysis and Synthesis Toolbox User's Guide*. Natick, MA: MathWorks, 2001.

[16] C. Cao and N. Hovakimyan, "$\mathcal{L}_1$ adaptive controller for systems in the presence of unmodeled actuator dynamics," in *Proc. 46th IEEE Conf. Decision and Control*, New Orleans, LA, Dec. 2007, pp. 891–896.

[17] C. Cao and N. Hovakimyan, "$\mathcal{L}_1$ adaptive output feedback controller for non strictly postive real multi-input multi-output systems in the presence of unknown nonlinearities," in *Proc. Amer. Control Conf.*, St. Louis, MO, Jun. 10–12, 2009, pp. 5138–5143.

[18] M. Sipser, *Introduction to the Theory of Computation*. Boston, MA: PWS Publishing, 1997.

[19] W. S. Levine, *Control Systems Fundamentals*. Boca Raton, FL: CRC, 2000.

[20] D. M. Fouquet, J. Razvi, and W. L. Whittemore, "TRIGA research reactors: A pathway to the peaceful applications of nuclear energy," *Nucl. News*, vol. 46, no. 12, pp. 46–56, Nov. 2003.