INL/CON-12-26847
PREPRINT

A Resilient Condition Assessment Monitoring System

5th International Symposium on Resilient Control Systems

Humberto E. Garcia
Wen-Chiao Lin
Semyon M. Meerkov

August 2012

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

A Resilient Condition Assessment Monitoring System

Humberto E. Garcia, Wen-Chiao Lin, and Semyon M. Meerkov

***Abstract*— An architecture and supporting methods are presented for the implementation of a resilient condition assessment monitoring system that can adaptively accommodate both cyber and physical anomalies to a monitored system under observation. In particular, the architecture includes three layers: information, assessment, and sensor selection. The information layer estimates probability distributions of process variables based on sensor measurements and assessments of the quality of sensor data. Based on these estimates, the assessment layer then employs probabilistic reasoning methods to assess the plant health. The sensor selection layer selects sensors so that assessments of the plant condition can be made within desired time periods. Resilient features of the developed system are then illustrated by simulations of a simplified power plant model, where a large portion of the sensors are under attack.**

***Index Terms*— Resilient systems, resilient monitoring, cyber-physical attacks, cyber/physical condition assessments, rational controllers, graceful degradation, measure of resiliency.**

I. Introduction

A. Motivation

Complex engineering systems need to be reliably monitored in order to ensure safety and proper operations. To this end, sensors are typically deployed within the monitored facility in order to observe the behavior of key process variables and access system conditions. Monitoring challenges include efficient processing of information and correct assessment of facility health despite possible natural or malicious disturbances. While natural disturbances can often be characterized reasonably well, malicious disturbances are ill-characterized. Regarding the latter, a significantly damaging disturbance to design against is the *cyber-physical coordinated attack*. In a cyber-physical coordinated attack, an attacker may cause a physical damage to the monitored facility and, furthermore, coordinately compromise the information layer via a cyber attack (e.g., by causing sensors to provide false readings of process variables) so as to confuse the operator of the actual plant health conditions. As intended by the attacker, a potential result may be that the operator, due to this confusion, takes a wrong decision, such as shutting down the monitored process or switching the plant to an inappropriate operating mode, while he/she otherwise could have gracefully maintained operations amid in a degraded mode, for example. Here, *coordinated* means that attacks occur at different locations of the monitoring system, while *cyber-physical* means that there are not only physical but also cyber attacks. A resilient monitoring system, which meets the above challenges, should possess the following properties:

- exhibit graceful degradation in performance, as opposed to sudden collapse, under severe disturbances;
- capable of effectively accommodating ill-defined or ill-characterized anomalies;
- capable of marshalling data according to assessed health condition of the monitored system;
- dynamically select active sensors for data collection in an untrackable manner that would complicate the task of an attacker in inflicting severe consequences;
- utilize prediction calculations regarding performance of solution alternatives when dynamically selecting sensors;
- capable of accommodating partial and unreliable sensory information;
- provide proper assessments of the monitored system within specified decision periods despite severe disturbances, such as cyber-physical coordinated attacks.

A monitoring system with the above properties should exhibit the behavior of resilient systems described in [1], [2]. This paper develops a monitoring system that satisfies these properties, being able to dynamically adapt based on assessed conditions not only of the monitored facility but also of its information infrastructure due to natural or malicious physical and cyber attacks.

B. Brief review of relevant literature on resilient systems

Research on resilient systems is a relatively new subject and recent work on resilient systems can be found in [1]–[11]. In particular, [3] provides collections of papers that treat resilience engineering as a paradigm for safety management that focuses on “how to help people cope with complexity under pressure to achieve success.” These papers explore different facets of resilience as “the ability to anticipate and adapt to the potential for surprise and failure.” Based on these work, [4] further identifies four cornerstones of resilience as knowing “what to do,” “what to look for,” “what to expect,” and “what has happened.”

Relations between resilience and robustness have been investigated. For example, [5] addresses different fire-prone ecological systems and suggests that robustness tradeoffs in these systems demonstrate resilience. In [6], resilient control systems that emphasize control design in an adversarial and uncertain cyber environment (as opposed to physical disturbances) are developed. This control design is viewed as pivoting on the tradeoff between robustness and resilience. Optimality criteria are proposed for tradeoff between robustness and resilience in modern industrial control systems.

Further developments of resilient systems with uncertain cyber environments can be found in [1], [7]. Specifically, [1] provides a conceptual framework and brief overview of the architectural considerations for designing systems that operate in hostile cyber environment with uncertainties in complex networks and human interactions. The work in [7] develops an intelligent resilient control algorithm for a

H.E. Garcia and W.-C. Lin are with the Idaho National Laboratory, P.O. Box 1625, Idaho Falls, ID 83415-3675, USA. Email: {Humberto.Garcia, Wen-Chiao.Lin}@inl.gov; S.M. Meerkov is with the University of Michigan, Ann Arbor, MI 48109, USA. Email: smm@eecs.umich.edu

978-1-4673-0162-6/12/$31.00 ©2012 IEEE

wireless networked control system based on quantification of the concept of resiliency in terms of quality of control. Here, resiliency maintains normal operations in the face of wireless interference incidents. Reference [12] further uses the quality of control for designing resilient control strategies for model-based building control, improving building automation systems.

Resilient systems have also been considered regarding security issues in, for example, [8], [9]. While [8] describes experiences and success in cyber security programs leading to more robust, secure, and resilient monitoring and control systems in industrial assets, [9] discusses security-related definitions for resilience, which includes integrity and confidentiality in addition to availability.

Developments of resilient systems for computer systems and for monitoring critical infrastructures can be found, for instance, in [10] and [11]. In particular, in [10], metadata-based resilience policies are enforced to design computing systems that can dynamically adapt in a predictable way to unexpected events. In [11], basic paradigms are proposed for integration of diverse fault detection and identification methods and control methods for achieving resilience in critical infrastructures.

Finally, we mention that, although the resilient monitoring structure in this work shares that developed in [2], the design approaches are different. In particular, the monitoring system designed here aims at selecting sensors to make plant health assessments within desired time periods despite cyber attacks, while that in [2] focuses on selecting sensor configurations to maximize plant health assessment confidence. Moreover, some advantages are also afforded by the approach considered here, such as faster computations of the monitored plant assessments.

C. Proposed monitoring system architecture

A resilient condition assessment monitoring (ReCAM) system, as illustrated in Fig. 1, is addressed in this paper that exhibits the properties envisioned in Section I-A. Natural or malicious disturbances may occur at each unit operation of the monitored system, while sensor data may not be trustworthy due to cyber attacks, for example. The goal is to dynamically collect and interpret sensor data and correctly assess the physical condition or health of the monitored system within desired timeliness requirements.

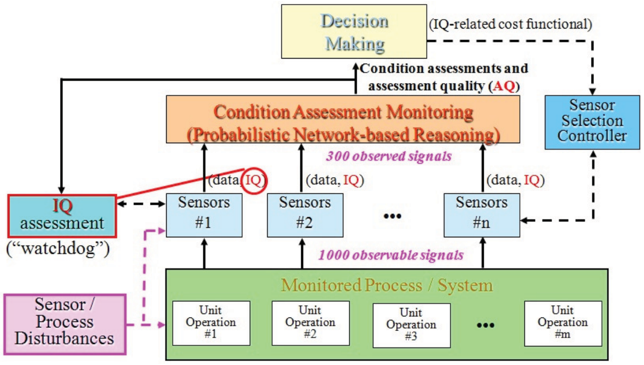
Decision Making
(IQ-related cost functional)
Condition assessments and assessment quality (AQ)
Condition Assessment Monitoring (Probabilistic Network-based Reasoning)
Sensor Selection Controller
300 observed signals
(data, IQ)
(data, IQ)
(data, IQ)
IQ assessment
("watchdog")
Sensors #1
Sensors #2
•••
Sensors #n
1000 observable signals
Monitored Process / System
Sensor / Process Disturbances
Unit Operation #1
Unit Operation #2
Unit Operation #3
•••
Unit Operation #m

Fig. 1. Architecture of proposed ReCAM system.

Within this architecture, the quality of sensor data is quantified by introducing the on-line assessed metric here called information quality (IQ), which includes both data quality (DQ) and data relevance (DR). While DQ quantifies the trustworthiness of a given sensor data, DR quantifies the importance of it. For example, consider two sensors associated to the same process variable (e.g., temperature in a given tank) in the monitored system. If one of the sensor is already reporting data with high DQ about this process variable, the DR associated with the other sensor may be assigned to a low value. In this paper, we do not explore DR further and only DQ is considered. In this regard, there are numerous methods that can be used to online compute sensor DQ, from techniques that rely on data- and model-driven calculations and probing mechanisms to detect data tampering to physical security procedures that rely on surveillance to infer breaches at data centers such as I/O boards, switches, programmable logic controllers (PLCs), and supervisory control and data acquisition (SCADA) installations. Classically, DQ may be generated by statistical analysis of sensor data. For example, suppose redundant sensors are associated with a certain process variable. An approach for generating DQ is investigating whether a sensor data in question is statistically significantly different to other redundant data. Voting techniques may also be used here. DQ may also be computed using calibration methods (e.g., kernel regression techniques [13]). Comparing results of state estimators and observed sensor data provides may yet be another way to generate DQ. From the domain of cyber security, monitoring network traffic around sensors may provide another way of generating DQ based on detection of suspicious and/or abnormal levels of message traffic, which may indicate a cyber attack, hence potential tampering of information. Finally, physical security violations (e.g., unlocked physical access points or observed breaches on security measures) may also be used to qualitatively quantify DQ for sensors located in suspected areas. In this work, DQ is thus assumed to be given by some sort of watchdog entity and interpreted via the notion of believability, defined in later sections.

At each time instant, a (different) subset of the sensor data (along with their IQ) may be active, which is chosen by a sensor selection controller for condition assessments. Although all sensor data may be available, only a subset of active ones are utilized for plant assessment at each time instant. The number of active sensors is accordingly selected based on the particular needs for marshalling data in order to meet observability requirements under varying conditions. Benefits of this dynamic sensor selection include:

- Suppose all available sensors are always utilized for plant condition assessment. Assume that a set of sensors are compromised. Using all the data may lead to confusion as sensor data may contradict with one another. Considerable effort may have to be consumed to filter out false sensor data.
- Due to selecting different subsets of active sensors at different time instances, health assessment is not tied to using only a particular set of sensor data. This feature also makes it more difficult for attackers to identify most important sensors to compromise.

- Since only a subset of sensors is selected at each time instant, information traffic is reduced and additional number of active sensor are selected only when merited to achieve required level of assessment quality.

In addition, since physical and cyber threats are typically ill-characterized (e.g., due to lack of attack samples and the intrinsic nature of malicious behaviors), thus limiting the use of model-based techniques relying on assumed disturbance characterizations, it is important to randomly search and explore in a rational manner time-varying subsets of sensors for selection, while exploiting sensors known to provide best data for health assessments under observed conditions. For this purpose, the theory of rational behavior (TRB) is utilized here to synthesize sensor selection algorithms [14]–[16]. Other work that introduce randomness to improve system performance includes simulated annealing [17]. The way sensors are selected avoids the so-called *observation stiffness*, which implies that only a specific set of sensors is used. While relying on a specific set of sensors may provide improved performance under well characterized disturbances, it is often an impediment to implementing graceful degradation under ill-characterized situations. Contrarily, by adaptively selecting different sets of sensors, observation stiffness is relaxed and the monitoring system becomes more flexible to handle disturbances. This is an example of duality between performance and flexibility. Observation stiffness provides optimal monitoring performance for well defined disturbances but poor performance under unconsidered conditions. Flexible observations, on the other hand, may yield adequate (but suboptimal) observational performance but may accommodate a variety of ill-defined situations.

In the proposed resilient monitoring architecture, data retrieved from the given set of active sensors is then processed by a health condition assessment monitoring module. Due to the time-varying mix of active sensors providing data for plant assessment and the possible presence of cyber attacks, the sensory information is partial and unreliable. To address this, the health assessment module needs to have a network-like topology capable to compute sufficiently accurate health assessments under possible missing and/or unreliable data. While Bayesian belief networks (BBN) are utilized in this work for conducting these calculations, other network-based probabilistic reasoning techniques may be used instead.

As illustrated in Fig. 1, the condition assessment monitoring algorithms output health assessments of the monitored plant for decision making, along with their associated assessment quality (AQ), the latter metric used to judge confidence on these assessments. This confidence is accordingly used as input for the sensor selection controller to select sensor configurations that meet expected levels of AQ.

D. Contributions and paper organization

By developing and evaluating the techniques discussed for the proposed ReCAM system illustrated in Fig. 1, the following contributions are achieved in this paper:

- formulation of a resilient monitoring approach for adaptively meeting observability requirements under severe disturbances, such as cyber-physical coordinated attacks, to complex engineering facilities;
- development of the building blocks associated with the proposed ReCAM system;
- demonstration of the resilient benefits associated with the proposed monitoring solution.

The rest of this paper is organized as follows. Section II provides a mathematical overview of the various layers of the ReCAM system, while Section III describes the monitored plant and sensors. The information, assessment, and sensor selection layers of ReCAM system are developed in Sections IV, V, and VI, respectively. The ReCAM system is applied to a simplified power plant model in Section VII and performance results are evaluated under non-resilient and resilient approaches. Finally, conclusions are briefly discussed in Section VIII.

II. ReCAM Structure

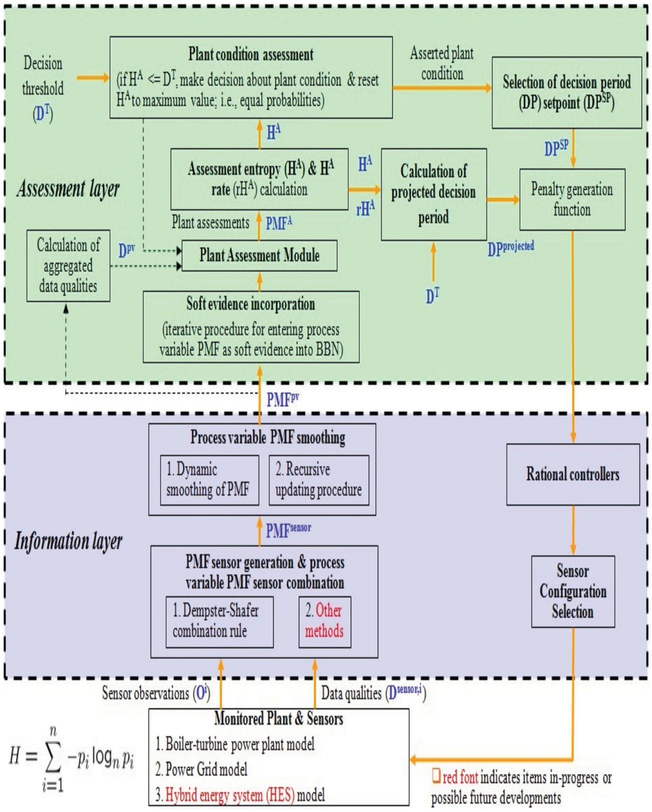
Decision threshold (D^T)
Plant condition assessment
(if H^A <= D^T, make decision about plant condition & reset H^A to maximum value; i.e., equal probabilities)
Asserted plant condition
Selection of decision period (DP) setpoint (DP^SP)
H^A
DP^SP
Assessment layer
Assessment entropy (H^A) & H^A rate (rH^A) calculation
H^A
rH^A
Calculation of projected decision period
Penalty generation function
Plant assessments
PMF^A
Calculation of aggregated data qualities
D^pv
Plant Assessment Module
DP^projected
Soft evidence incorporation
(iterative procedure for entering process variable PMF as soft evidence into BBN)
D^T
PMF^pv
Process variable PMF smoothing
1. Dynamic smoothing of PMF
2. Recursive updating procedure
Rational controllers
Information layer
PMF^sensor
PMF sensor generation & process variable PMF sensor combination
1. Dempster-Shafer combination rule
2. Other methods
Sensor Configuration Selection
Sensor observations (O^i)
Data qualities (D^sensor,i)
Monitored Plant & Sensors
1. Boiler-turbine power plant model
2. Power Grid model
3. Hybrid energy system (HES) model
H = Σ_{i=1}^{n} −p_i log_n p_i
□ red font indicates items in-progress or possible future developments

Fig. 2. Detailed structure of ReCAM implementation.

A detailed structure of ReCAM is shown in Fig. 2. In this structure, sensor observations from the monitored plant and their associated DQs are first processed in the information layer, which provides estimates of process variable PMFs, PMF^{pv}. These PMF estimates are then processed by a plant assessment module modeling the monitored plant. Note that instead of hard evidences (i.e., exact values of the observed process variables), soft evidences (i.e., probability distributions of the variables) are entered. The plant assessment module outputs PMF of plant assessment, PMF^{A}. Using PMF^{A}, the entropy of this plant assessment is calculated. If this entropy is less than a threshold, a definite decision is made about plant conditions. If the entropy is higher than this threshold, a projected decision period, $DP^{projected}$ is calculated. The value of $DP^{projected}$ is the estimated time period from the previous definite decision of plant conditions to the next definite decision. Based on the difference between $DP^{projected}$ and a user defined (set point) decision period, DP^{SP}, penalties are generated and communicated to rational controllers, which select sensor configurations that try to keep $DP^{projected}$ as close as possible to DP^{SP}.

Detailed descriptions of the constituent components of the information and assessment layers are shown in Fig. 3. We briefly describe the building blocks in Fig. 3 from bottom to top. To estimate the process variable PMF from each (active) sensor, sensor DQ (or D^{sensor}) is interpreted using the notion of *believability*. Demspter-Shafer Theory is employed to combine PMF estimates from sensors assigned to the same process variable. Smooth filtering, based on first order dynamics, of combined process variable PMF estimates is introduced so newly observed evidence for plant assessment is not entered abruptly. Modeling relations among process variables and plant conditions are used to assess plant conditions based on the estimated process variable PMFs. CPTs of BBNs are found assuming perfect sensor DQ and, hence, they need to be accordingly tuned using aggregated DQs of process variables. Aggregated DQ (or D^{pv}) is calculated based on current estimates of process variable PMF; the result often differs from D^{sensor}, especially when multiple sensors are utilized for one variable and at early phases of the PMF smooth filtering. When no sensor is activated for a given process variable, smooth transition of aggregated DQ (via first order dynamics) towards $D^{pv} = 1$ is introduced. An iterative procedure, which is a modification of the iterative proportional fitting procedure (IPFP), is used to enter estimated process variable PMF evidence into the BBN. Assessments of plant condition is then computed by the BBN. Implementation of the different components in the ReCAM structure is further discussed throughout this paper.

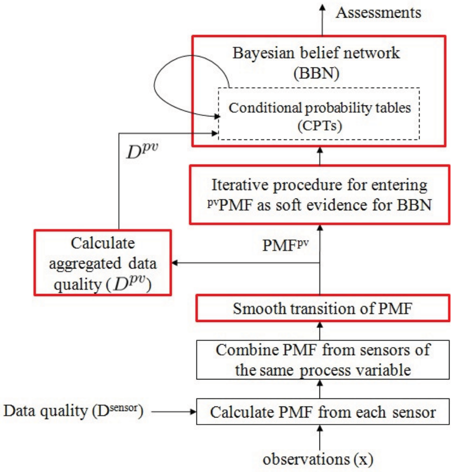
Assessments
Bayesian belief network (BBN)
Conditional probability tables (CPTs)
D^{pv}
Iterative procedure for entering pvPMF as soft evidence for BBN
PMFpv
Calculate aggregated data quality (D^{pv})
Smooth transition of PMF
Combine PMF from sensors of the same process variable
Data quality (Dsensor)
Calculate PMF from each sensor
observations (x)

Fig. 3. Details of ReCAM implementation.

III. Monitored Plant and Sensors

In this section, models of the monitored plant and sensor measurements of process variables are introduced. Specifically, let $V_1, V_2, \ldots, V_M$ denote random variables describing discrete states of M process variables and G denote a random variable describing plant state. The monitored plant is modeled as a set of conditional probabilities of process variables V_i, $i = 1, 2, \ldots, M$, given state of plant G and/or other process variables. For convenience, BBN is used to organize this information. In particular, the plant model is:

$$\begin{cases} [P(V_i|G)] & \text{for } i \in I \subseteq \{1, 2, \ldots, M\}, \\ [P(V_i|V_j)] & \text{for some pairs } i, j \in \{1, 2, \ldots, M\}. \end{cases} \tag{1}$$

Notice that some V_i do not directly depend on the state of plant G but on the state of certain process variable V_j. On the other hand, sensor measurements are computed by adding a given Gaussian noise to the true value of the process variable. To model cyber attacks, the mean value of the noise is accordingly modified based on the severity of the attack. Sensor outputs are then computed by discretizing measured process values into discrete quantities such as low, normal, and high. A DQ model is used to calculate the effects of the threat on the quality of the sensor measurements. The output, D_i, of this DQ model is the estimated sensor DQ.

IV. Information Layer

For a given process variable V, Figure 4 illustrates the operation of the information layer, which calculates the estimated process variable PMF, $\hat{P}(V)$, that is subsequently used as evidence at the assessment layer for computing plant condition assessments. Suppose the DQ of sensor S_i is D_i and that S_i observes $\sigma \in \Sigma$, where Σ is the set of states of V (e.g., Low (L), Normal (N), or High (H)). The notion of *believability* of a sensor is employed to interpret this observation in the form of PMF for V [2]. Formally, *believability* is defined as follows:

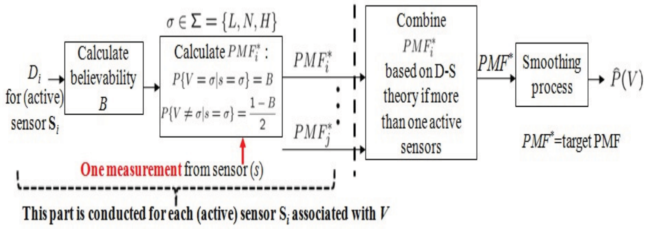
$\sigma \in \Sigma = \{L, N, H\}$
D_i for (active) sensor S_i
Calculate believability B
Calculate PMF_i^* :
$P\{V = \sigma|s = \sigma\} = B$
$P\{V \neq \sigma|s = \sigma\} = \frac{1-B}{2}$
PMF_i^*
PMF_j^*
Combine PMF_i^* based on D-S theory if more than one active sensors
PMF^*
Smoothing process
$\hat{P}(V)$
PMF^*=target PMF
One measurement from sensor (s)
This part is conducted for each (active) sensor S_i associated with V

Fig. 4. Information layer of proposed ReCAM system.

$$B = \frac{1}{|\Sigma|}\left[(|\Sigma| - 1)D_i + 1\right], \tag{2}$$

where $|\Sigma|$ is the cardinality of the process variable state space, Σ. Based on B, we calculate PMF_i^*, where $PMF_i^*(\sigma)$ denotes the probability of $V = \sigma$, used to determine the target PMF for the smoothing process. In particular, PMF_i^* based on the observation s of S_i is given by:

$$PMF_i^*(\delta) = P\{V = \delta|s = \sigma\} = \begin{cases} B & \text{if } \delta = \sigma, \\ \frac{1-B}{|\Sigma|-1} & \text{if } \delta \neq \sigma. \end{cases} \tag{3}$$

For example, suppose $\Sigma = \{L, N, H\}$ and observation s is N. Then PMF_i^* is given by

$$\begin{aligned} PMF_i^* &= \left[\begin{array}{ccc} PMF_i^*(L) & PMF_i^*(N) & PMF_i^*(H) \end{array}\right] \\ &= \left[\begin{array}{ccc} \frac{1-B}{2} & B & \frac{1-B}{2} \end{array}\right]. \end{aligned} \tag{4}$$

Note that the calculation of PMF_i^* results from only one measurement reported by S_i. If there is only one active sensor, say S_i, for V, we set $PMF^* = PMF_i^*$. If there are multiple (active) sensors observing V, Dempster-Shafer combination rule [2] is used to combine multiple PMFs. The formula for two sensors, say S_i and S_j, is as follows:

$$PMF_\sigma^* = \frac{PMF_i^*(\sigma)PMF_j^*(\sigma)}{\sum_{\delta\in\Sigma} PMF_i^*(\delta)PMF_j^*(\delta)}, \ \sigma\in\Sigma, \quad (5)$$

where $PMF_i^*(\delta)$ and $PMF_j^*(\delta)$ is calculated by (3) and PMF_σ^* is the probability for $V = \sigma$ in PMF^*. Extension of (5) to more than two sensors is straightforward. The combined PMF^* is used as a target for the smoothing process detailed below. The smoothing process serves as a low pass filter and prevents abrupt changes in $\hat{P}(V)$. To facilitate discussion, consider the following:

- measurements from all active sensors are synchronously collected at the same time;
- let k $(k = 1, 2, 3 \ldots)$ denote the time index when measurements from active sensors are collected.

For each time instant k, $PMF_i^*(k)$ for each active sensor is calculated, which is then combined with others to compute $PMF^*(k)$; notice that if $D_i(k)$ and $s(k)$ do not change within a given time window, $PMF^*(k)$ does not change either. At each time instant k, the smoothing process in Fig. 4 is executed using the calculated $PMF^*(k)$ as a target PMF. The dynamics for smoothing process is given by

$$\tau\frac{d}{dt}PMF(t) = PMF^*(k) - PMF(t), \quad (6)$$

where

- at time $t = 0$, $PMF(0)$ is uniform. For example, $PMF(0) = [\ \frac{1}{3} \quad \frac{1}{3} \quad \frac{1}{3}\ ]$ when $\Sigma = \{L, N, H\}$;
- for time instant k, dynamics are simulated with target $PMF^*(k)$ from t_{k-1} to $t_k = t_{k-1}+\Delta t$, where $t_0 = 0$;
- Δt and τ are design parameters;
- $PMF(t_k)$ is $\hat{P}(V)$ for time k;

To calculate $\hat{P}(V)$, ones does not have to wait first for the collection of a long sequence of measurements (from active sensors). The computation of $\hat{P}(V)$ is conducted as measurements are sequentially collected from active sensors. In the following, to quantify the information contained in $\hat{P}(V)$, the information entropy of $\hat{P}(V)$ is defined as

$$H^I = \sum_{\sigma\in\Sigma} -\hat{P}(V = \sigma)\log_{|\Sigma|}\hat{P}(V = \sigma). \quad (7)$$

V. Assessment Layer

The assessment layer estimates the monitored plant conditions based on the estimated process variable PMFs. Figure 5 shows the operations of the assessment layer, where V_i, $i = 1, 2, \ldots, M$ are the process variables and G represents the status of the plant. While other probabilistic reasoning methods may be used, the plant assessment module utilizes a BBN in the present work, where estimated PMFs are entered using a modification of the iterative proportional fitting procedure (IPFP) documented in [18]. The assessment algorithm is applied as $\hat{P}(V_i)$, $i = 1, 2, \ldots, M$ are calculated from sensor measurements sequentially collected at time $k = 1, 2, \ldots$. When using the assessment algorithm to compute the a posteriori belief of plant state $\hat{P}(G)$, the initial (a priori) belief of plant state is the result from the assessment computed at previous time step. That is, if the current time index is k, the a priori belief for the assessment algorithm is $\hat{P}(G)$ calculated at time $k-1$. When $\hat{P}(V_i)$, $i = 1, 2, \ldots, M$ at time k are consistent with $\hat{P}(G)$ calculated at time $k-1$, the assessment entropy of the plant, defined as:

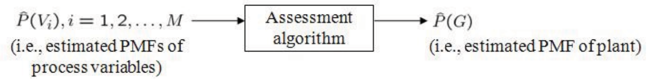
$\hat{P}(V_i), i = 1,2,\ldots,M$
(i.e., estimated PMFs of process variables)
Assessment algorithm
$\hat{P}(G)$
(i.e., estimated PMF of plant)

Fig. 5. Assessment layer of ReCAM system.

$$H^A = \sum_{\sigma\in\Sigma_G} -\hat{P}(G = \sigma)\log_{|\Sigma_G|}\hat{P}(G = \sigma), \quad (8)$$

decreases from its previous value calculated at $k-1$. Once the assessment entropy of plant decreases below a (user-defined) decision threshold, a definite decision is made about the plant state (e.g., whether the plant is normal, degrading, or down) and the belief of plant state is reset to complete ignorance (e.g., $P(G) = [\ 1/3 \quad 1/3 \quad 1/3\ ]$) for the subsequent assessment, and the assessment procedure repeats. Resetting here means resetting the roots of the BBN. Note that $\hat{P}(G)$ is used here as statistics for decision making and not reported to the user, but rather the definite decisions (e.g., whether plant is normal, degrading, or down). Moreover, the notion of decision period is of importance. It is defined as the time window that starts at the moment of resetting the plant belief to complete ignorance and ends when a decision on plant state is made. Decision period is the time needed to make a definite decision regarding the state of the monitored plant. During the decision period, no updated decision is available to a user (e.g., a plant operator) and the monitoring system reports/keeps the definite decision on plant state computed during the previous decision period.

A. Modification of CPTs and aggregated data quality

Because CPTs of BBNs are trained assuming perfect DQs, they need to be accordingly modified considering the estimated DQs. A method used in this work calculates the aggregated DQ corresponding to the estimated process variable PMF. Specifically, consider an estimated PMF for the process variable V, $\hat{P}(V)$ and calculate its entropy, H^I, via (7) to find:

$$\bar{x} = \arg\max_{\sigma\in\Sigma}\hat{P}(V = \sigma), \quad (9)$$

and find $\bar{D}$ such that

$$H^I = Entropy(\bar{x}, \bar{D}) \quad (10)$$

where $Entropy(x, D)$ is the entropy of the PMF calculated (by (2)–(3)) when a sensor measurement is x with DQ D. Once the aggregated DQ is computed, the CPT for the process variable is modified by

$$Prob_{modified}(V = \sigma|A) = Prob(V = \sigma|A) + (\frac{1}{n} - Prob(V = \sigma|A))(1 - \bar{D}) \quad (11)$$

for $\sigma \in \Sigma$, where n is the number of possible states of V and A represents parent nodes of V. Note that when $\bar{D} = 0$, the modified conditional probabilities become $\frac{1}{n}$ and when $\bar{D} = 1$, the modified conditional probabilities are the same as the original ones. Moreover, when modifying the CPT by (11), the conditional probabilities, $Prob(V = \sigma|A)$, are always obtained from the original CPT. Similar to the strategy used at the information layer, when no sensors for the given process variable are active, the first order dynamics shown below is employed to "fade" the aggregated DQ, thus preventing abrupt changes to the monitoring system.

$$\tau_{\bar{D}} \dot{\bar{D}}(t) = 1 - \bar{D}(t), \tag{12}$$

where

- at time $t = 0$, $\bar{D}(0)$ is the last aggregated DQ before all sensors associated with the process variable become inactive;
- for time instant k, dynamics are simulated from t_{k-1} to $t_k = t_{k-1} + \Delta t$, where $t_0 = 0$;
- Δt and $\tau_{\bar{D}}$ are design parameters;
- $\bar{D}(t_k)$ is the faded aggregated DQ at time k.

This computation continues until at least one sensor associated with the process variable becomes active. Then, the aggregated DQ is again calculated as described above.

VI. Sensor Selection Layer

The goal of the sensor selection layer is to meet a certain (user-defined) decision period. The goal is not to find an optimal sensor configuration (SC) per se, but rather to control selections of SCs so that the assessment entropy decreases as needed to meet decision period requirements. There is no need for plant operating conditions and sensor DQs (i.e., threats) to stay the same, but they can change. In this work, each sensor is equipped with a rational controller (RC) to select its operation mode. The RCs are designed to achieve monitoring objectives based on the penalties received.

A. Rational Controller

The RCs designed here are based on the ring element [14]. The state space of the ring element is $[0, 1)$. When the ring element is in $[0, 0.5)$, the sensor associated with it is inactive, thus reporting no data. Similarly, when the ring element is in $[0.5, 1)$, the sensor associated with it is active. When sensors switch to active (inactive), their RCs pick a state in $[0.5, 1)$ ($[0, 0.5)$) with uniform probability. The dynamics of the ring element is described as follows:

$$\dot{x} = \varphi^N(\{x\}) \tag{13}$$

where $\{x\}$ takes the fractional part of x, $\varphi(x)$ is the penalty associated with x, and N is a positive number referred to as the measure of rationality. The dynamics in (13) is approximated as

$$x(k+1) = x(k) + \Delta t \varphi^N(\{x(k)\}) \tag{14}$$

where k denoted the index of the measurement step and $\Delta t = 0.001$ in this work.

B. Penalty Function

Ring elements are penalized so that the desired decision period is achieved within some tolerance. To this end, the expected decision period is estimated based on the time elapsed since last decision and the current rate of assessment entropy change. That is, assume the current measurement step is k and the assessment module has just processed the soft evidences computed from measurements collected at k. The decision period is then estimated as follows:

$$\widehat{DP} = TE + \frac{(DT - H(k))}{(H^A(k) - H^A(k-1))}, \tag{15}$$

where DT is the decision threshold, TE is the time elapsed since last decision, $H^A(k)$ is the assessment entropy at time k, and $\widehat{DP}$ is the projected decision period. The assessment entropy is calculated using (8). Appropriate penalty functions can be found from numerical experiments following the rationale bellow:

- If projected decision period is longer than desired, penalize **inactive** sensors more;
- If projected decision period is shorter than desired, penalize **active** sensors more;
- Sensors with **high** D incur **less** penalty when active and more penalty when inactive;
- Sensors with **low** D incur **more** penalty when active and less penalty when inactive.

VII. Application

A. Simplified power plant

Application of ReCAM to a simplified power plant model is considered here, consisting of six unit operations and 16 process variables as shown in Fig. 6. The six unit operations are: main steam generator (MSG), reheat steam generator (RSG), high pressure turbine (HPT), low pressure turbine (LPT), feed water pump (FWP), and condenser (C). The 16 process variables considered are listed below.

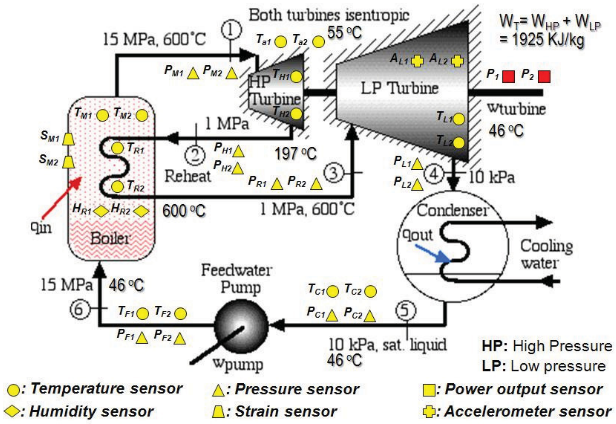

Fig. 6. Simplified power plant for demonstration.

- Twelve of the 16 process variables are temperatures and pressures at the six unit operations. These process variables are denoted by P_i and T_i, $i \in \{M, R, H, L, F, C\}$, for pressure and temperature, respectively, at the unit operation with i as the first letter

in its abbreviation. For example, temperature at LPT is indicated by T_L.
- The remaining four process variables are strain at boiler near MSG (S_M), humidity around RSG (H_R), temperature in atmosphere around HPT (T_a), and acceleration at LPT (A_L).

Two sensors are assigned to each process variable. We use the index j, $j = 1, 2$, to denote the jth sensor for a process variable. For example, T_{M1} and T_{M2} denote the first and second sensor for T_M, respectively.

Four types of physical anomalies are considered:

- Anomaly #1, in MSG: Low heat transfer;
- Anomaly #2, in RSG: Pipeline rupture;
- Anomaly #3, in HPT: Improper heat insulation;
- Anomaly #4, in LPT: Decreased efficiency;

Process variables not mentioned in the characterization of a particular anomaly may also be affected. For example, when MSG is malfunctioning, T_M is low. In this case, T_H will also be low due to physical association.

B. Sensor models

We consider two sets of redundant sensors, A and B, each associated with the sixteen process variables introduced above. Set A (or B) is the set of sensors with subscript 1 (or 2). Sensors are assumed to have additive Gaussian white noise with zero mean and variance $\sigma^2 = (m \times L)^2$, where L is the absolute value of the difference between the baseline value of the process variable corresponding to the given sensor and its high/low threshold. Moreover, m is tunable and chosen to be 0.2. If a sensor is attacked, the attacker adds bias according to whether true value of the measured process variable is:

$$\begin{cases} > \text{high threshold, add bias } -(TL) \times n \times L, \\ < \text{low threshold, add bias } (TL) \times n \times L, \\ \text{otherwise, add bias } -(TL) \times n \times L, \end{cases} \tag{16}$$

where $TL \in [0, 1]$ is the treat level of attack, chosen to be 0.7, and n is tunable, chosen to be 8. It is assumed that the assessed DQ of a sensor is given by $D = 1 - TL$, where $TL = 0$ if the sensor is not attacked. Equation (16) indicates that the attacker makes the sensor output low (high), while the true value of the process variable is high (low). Moreover, when the true value is between high and low, the attacker makes the sensor output low.

C. Comparison with non-resilient monitoring

In this subsection, we compare the performance of the proposed ReCAM system against a non-resilient approach. A non-resilient approach refers to a monitoring system that always uses all sensors deployed, without utilizing DQ information. Hard evidences from sensors are thus always directly entered into the plant assessment module. For simplicity, we assume that only sensors in set A are utilized for the non-resilient case.

In the experimental run here presented, the power plant is assumed to operate normal from 0 to 749 seconds. From 750 to 4000 seconds, Anomaly #2 is introduced. Moreover, two different cyber attacks are considered in coordination with this physical attack. Specifically, assume that no cyber attack is present from 0 to 1499 seconds. Then,

- Attack #1: From 1500 to 2499 seconds, 12 sensors compromised:
  - in set A, three sensors are attacked: P_{R1}, T_{R1}, and H_{R1};
  - three additional sensors in set A are randomly chosen to be attacked;
  - six sensors from set B other than P_{R2}, T_{R2}, and H_{R2} are randomly chosen to be attacked.
- Attack #2: From 2500 to 4000 seconds, 12 sensors compromised:
  - previously attacked sensors are restored;
  - similar procedure is followed to choose the sensors to be attacked.

Figure 7 shows the conditions assessed for MSG and RSG by ReCAM and the non-resilient system. Simulation results shown that for the cyber-physical attack considered here, the ReCAM system is able to correctly identify physical anomalies and assess the condition of the monitored system, while the non-resilient monitoring system is often confused, identifying incorrect anomalies and making wrong plant assessments. Table I shows that there is significant confusion in making a conclusive assessment under non-resilient monitoring case. Specifically, in period 4, the ReCAM system does not get confused as cyber attacks are injected, correctly assessing that only one device is malfunctioning, while the non-resilient system wrongly indicates three malfunctioning devices 77.37% of the time.

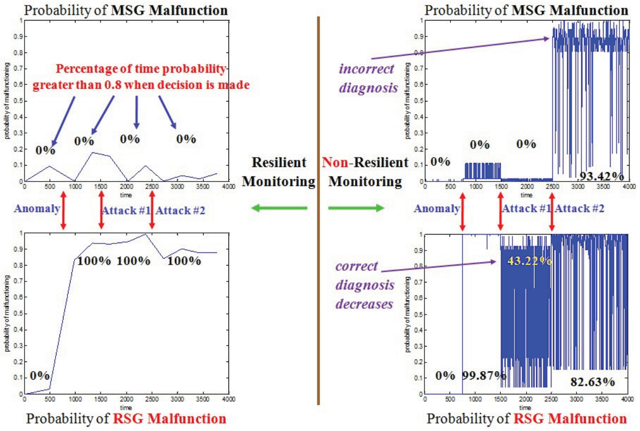

Fig. 7. Assessments for MSG and RSG.

TABLE I
NUMBER OF DEVICES CONSIDERED MALFUNCTIONING WITH CERTAINTY

# of Devices	**Period 1** (Normal)		**Period 2** (anomaly #2)		**Period 3** (attack #1)		**Period 4** (attack #2)	
	R	NR	**R**	NR	**R**	NR	**R**	NR
0	**100%**	100%	0%	0.13%	0%	0%	0%	**0.26%**
1	0%	0%	**100%**	**99.87%**	**100%**	**82.58%**	**100%**	**0.26%**
2	0%	0%	0%	0%	0%	**17.42%**	0%	**22.11%**
3	0%	0%	0%	0%	0%	0%	0%	**77.37%**

In order to compare the performance of ReCAM and non-resilient approach, we introduce the *measure of resiliency*, defined as the norm-2 distance, $\|T - \hat{T}\|$ with

$$T = \left[\, p_{MSG}\ p_{RSG}\ p_{HPT}\ p_{LPT}\ p_{FWP}\ p_{Condenser} \,\right] \quad (17)$$

and

$$\hat{T}=\left[\, \hat{p}_{MSG}\ \hat{p}_{RSG}\ \hat{p}_{HPT}\ \hat{p}_{LPT}\ \hat{p}_{FWP}\ \hat{p}_{Condenser} \,\right], \quad (18)$$

where p_i and $\hat{p}_i$ are, respectively, the true and estimated probabilities that component i is malfunctioning. We conduct a longer simulation with scenarios similar to those considered in Subsection VII-C. However, we assume that the RSG anomaly occurs starting from time 2100 and attacks 1 and 2 commence at 7500 and 12750, respectively. Note that, within this scenario, $p_i = 0$ for $i \neq RSG$, $p_{RSG} = 0$ for time < 2100, and $p_{RSG} = 1$ otherwise. Figure 8 compares the measures of resiliency for resilient and non-resilient systems. When sensors are not attacked, systems with and without resilient monitoring algorithms have similar $\|T - \hat{T}\|_2$ values. When cyber attacks occur, system without resilient monitoring algorithms performs much worse (with $\|T - \hat{T}\|_2 > 1$ most of the time) than system with resilient monitoring algorithm ($\|T - \hat{T}\|_2 < 0.8$).

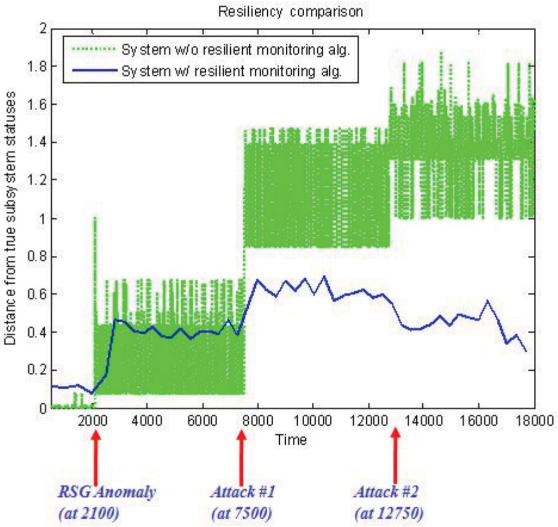

Fig. 8. Measures of resiliency for resilient and non-resilient systems

VIII. Conclusion

In this paper, a ReCAM system is proposed to meet resiliency challenges when monitoring complex engineering facilities. Chief among the challenges is the ability for the monitoring system to correctly assess facility health within desired decision period despite cyber-physical coordinated attacks. The proposed ReCAM system, which is comprised of information, assessment, and sensor selection layers, is able to meet the challenges considered. In particular, the ReCAM system exhibits resiliency and is able to dynamically adapt and reconfigure depending on assessed conditions not only on the monitored facility but also on the information infrastructure. Algorithms for the various ReCAM system layers were developed and benefits of the ReCAM system were demonstrated using a simplified power plant model. Although comparisons of the resilient monitoring system developed here to existing monitoring systems are not conducted in this paper, they will be addressed in the future. A number of scenarios will also be developed to further illustrate the effectiveness of the methods used here.

Acknowledgment

The research reported here was supported by the Instrumentation, Control, and Intelligent Systems (ICIS) initiative at Idaho National Laboratory under U.S. Department of Energy contract DE-AC07-05ID14517.

References

[1] C. G. Rieger, D. I. Gertman, and H. A. McQueen, "Resilient control systems: Next generation design research," in *Proceedings of the 2nd IEEE Conference on Human System Interaction*, Catania, Italy, May 2009, pp. 632 – 636.

[2] H. E. Garcia, N. Jhamaria, H. Kuang, W.-C. Lin, and S. M. Meerkov, "Resilient monitoring system: Design and performance analysis," in *Proceedings of the 4th International Symposium on Resilient Control Systems*, Boise, ID, 2011, pp. 61–68.

[3] E. Hollnagel, D. D. Woods, and N. Leveson, Eds., *Resilience Engineering: Concepts and Percepts*. Ashgate Publishing, 2006.

[4] E. Hollnagel, J. Pariès, D. D. Woods, and J. Wreathall, Eds., *Resilience Engineering in Practice: A Guidebook*. Ashgate Publishing, 2011.

[5] M. A. Moritz, M. E. Morais, L. A. Summerell, J. M. Carlson, and J. Doyle, "Wildfires, complexity, and highly optimized tolerance," in *Proceedings of the National Academy of Sciences*, vol. 102, no. 50, 2005, pp. 17 912–17 917.

[6] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference*, Orlando, FL, December 2011, pp. 4066–4071.

[7] K. Ji and D. Wei, "Resilient control for wireless networked control systems," *International Journal of Control, Automation, and Systems*, vol. 9, 2011.

[8] R. S. Anderson, "Cyber security and resilient systems," in *Proceedings of the 50th Annual Meeting of Institute of Nuclear Materials Management*, 2009.

[9] M. Bishop, M. Carvalho, R. Ford, and L. M. Mayron, "Resilience is more than availability," in *Proceedings of the 2011 Workshop on New Security Paradigms*, 2011.

[10] G. D. M. Serugendo, J. Fitzgerald, A. Romanovsky, and N. Guelfi, "A meta-based architectural model for dynamically resilient systems," in *Proceedings of the 2007 ACM Symposium on Applied Computing*, 2007.

[11] K. Villez, V. Venkatasubramanian, H. Garcia, C. Reiger, T. Spinner, and R. Rengaswamy, "Achieving resilience in critical infrastructures: A case study for a nuclear power plant cooling loop," in *Proceedings of the 3rd International Symposium on Resilient Control Systems*, Idaho Falls, ID, August 2010, pp. 49–52.

[12] K. Ji, Y. Lu, L. Liao, Z. Song, and D. Wei, "Prognostics enabled resilient control for model-based building automation systems," in *Proceedings of the 12th Conference of International Building Performance Simulation Association*, 2011, pp. 286–293.

[13] J. W. Hines, D. Garvey, J. Garvey, and R. Seibert, "Nuclear application of on-line sensor calibration monitoring for saftey critical sensors," in *Proceedings of the First World Congress on Engineering Asset Management*, 2006.

[14] S. M. Meerkov, "Mathematical theory of behavior-individual and collective behavior of retardable elements," *Mathematical Biosciences*, vol. 43, no. 1-2, pp. 41–106, 1979.

[15] P. T. Kabamba, W.-C. Lin, and S. M. Meerkov, "Rational probabilistic deciders-Part I: Individual behavior," *Mathematical Problems in Engineering*, vol. 2007, Article ID 35897, 31 pages, 2007.

[16] ——, "Rational probabilistic deciders-Part II: Collective behavior," *Mathematical Problems in Engineering*, vol. 2007, Article ID 82184, 34 pages, 2007.

[17] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi, "Bayesian network reasoning with uncertain evidences," *Science*, vol. 220, pp. 671–680, 1983.

[18] Y. Peng, S. Zhang, and R. Pan, "Bayesian network reasoning with uncertain evidences," *International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems*, vol. 18, no. 5, pp. 539–564, 2010.