A Resilient Condition Assessment Monitoring (ReCAM) System

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

Presenter: Wen-Chiao Lin

5th International Symposium on Resilient Control Systems
August 15, 2012, Salt Lake City, UT

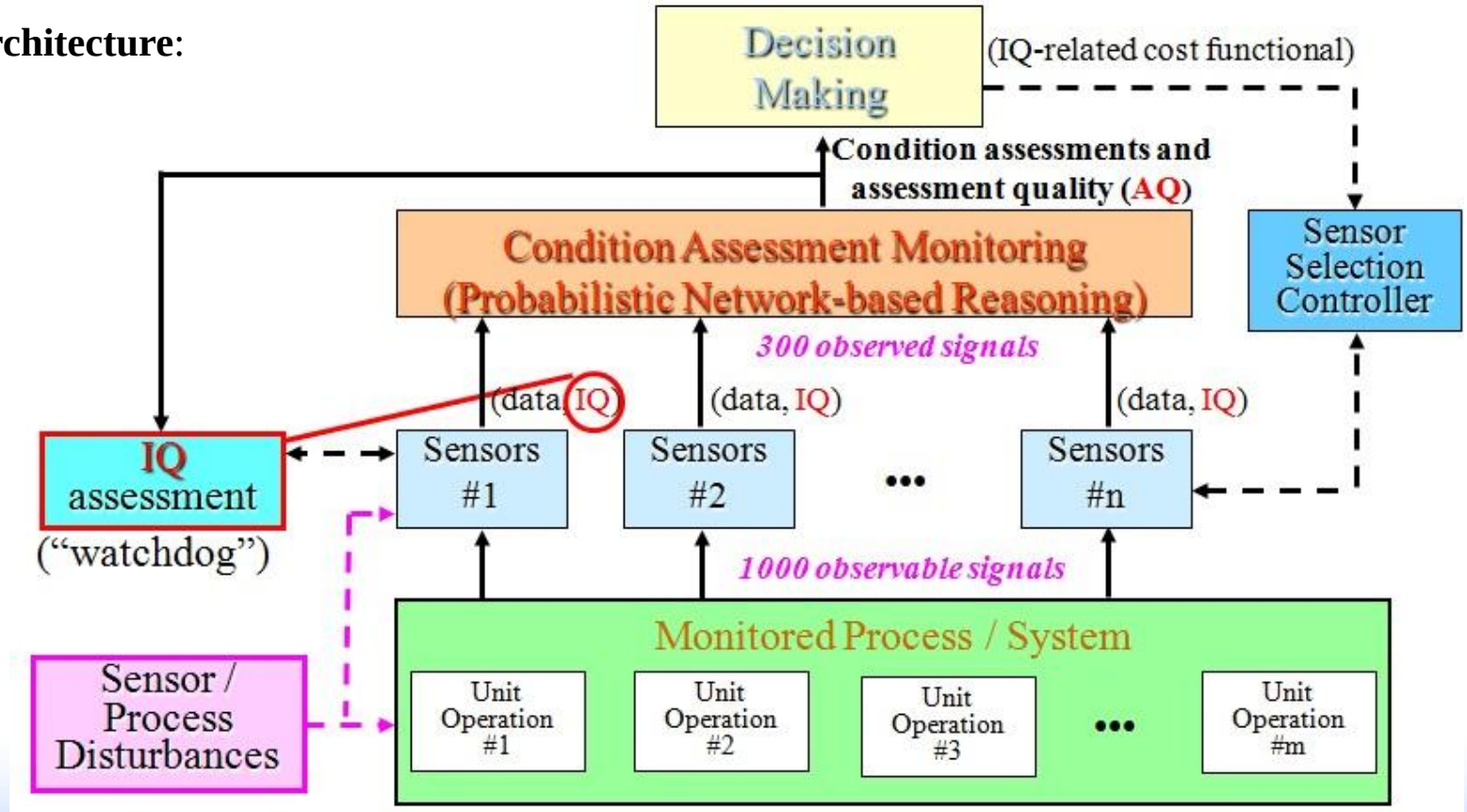
Idaho National Laboratory

Outline of Presentation

- Introduction
- Plant & sensor models
- Sensor information layer
- Plant health/condition assessment layer
- Sensor selection layer
- Application to simplified power plant model
- Conclusions

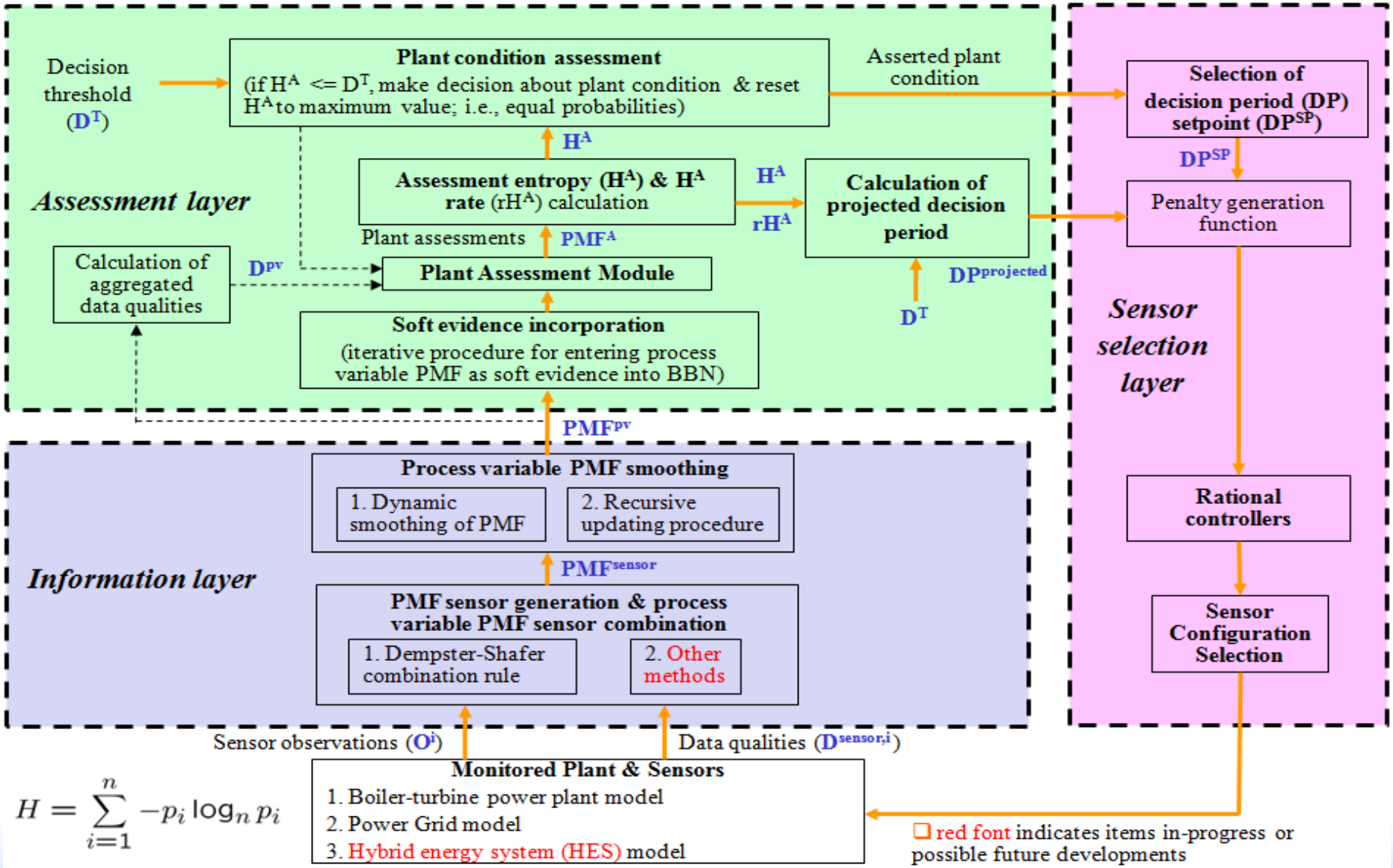
Introduction

- Complex engineering systems need to be reliably monitored to ensure safety and proper operations.
- Monitoring challenges include efficient processing of information and correct assessment of facility health (physical & cyber) despite possible natural or malicious disturbances.
- **Goal**: Design and evaluate the performance of a monitoring system that *degrades gracefully* under natural or malicious sensor malfunctioning. We refer to such a system as *resilient*.
- **Architecture**:



IQ: Information Quality (includes both Data Quality and Data Relevance)
AQ: Assessment Quality (includes confidence on assessment)

ReCAM Structure



$$H = \sum_{i=1}^{n} -p_i \log_n p_i$$

Idaho National Laboratory

- ReCAM here aims at selecting sensors to make plant health assessments within desired time periods, while previous work focuses on selecting sensors to maximize assessment confidence.

Monitored Plant and Sensors

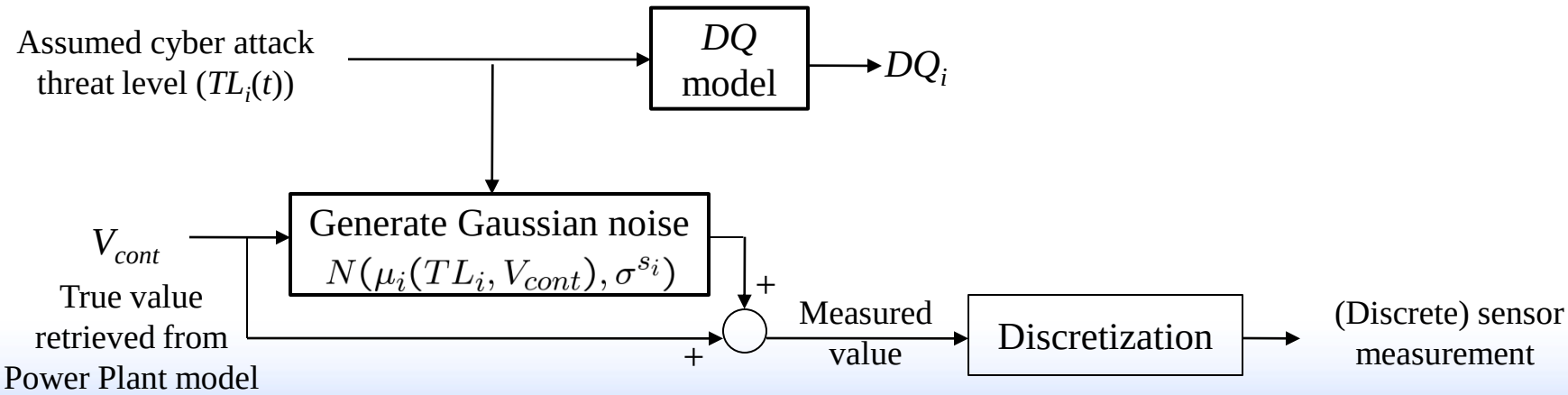
❑ Plant model

- V_i, i=1,2,…M, : random variables for process variables, taking discrete values (e.g., L, N, or H).
- G : random variable for plant status, taking discrete values (e.g., *Normal*, *Degrading*, or *Down*).
- Plant model: A set of conditional probabilities:

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

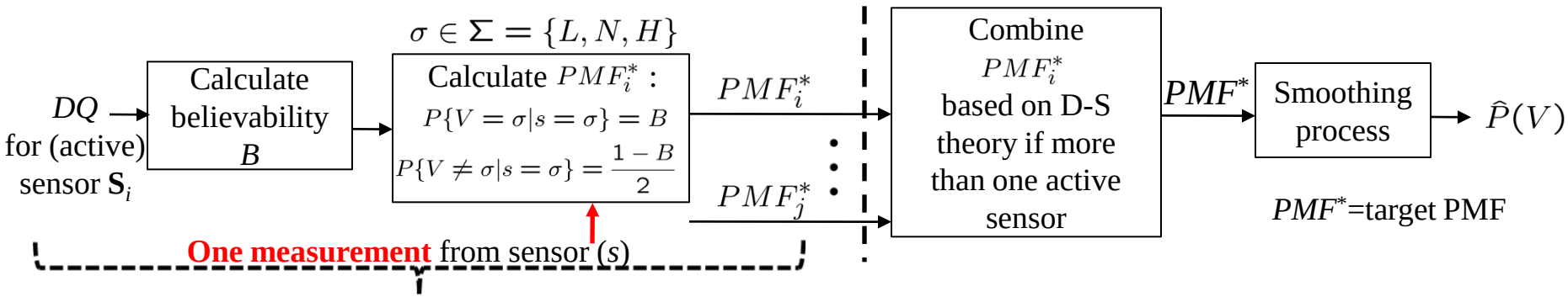
- Bayesian Belief Network (BBN) is used to organize this information.

❑ Sensor model / cyber attack model



Information Layer

- A given process variable, V, observed by (active) sensors $\mathbf{S}_1$, $\mathbf{S}_2$,…



This portion is conducted for each (active) sensor $\mathbf{S}_i$ associated with V

- Believability:

$$B = \frac{1}{|\Sigma|}[(|\Sigma|-1)DQ+1] \xrightarrow{\text{(if \textbf{three} possible values for } V)} B = \frac{2}{3}DQ + \frac{1}{3}$$

- PMF_i^* calculation: If measurement s from $\mathbf{S}_i$ is Normal (N):

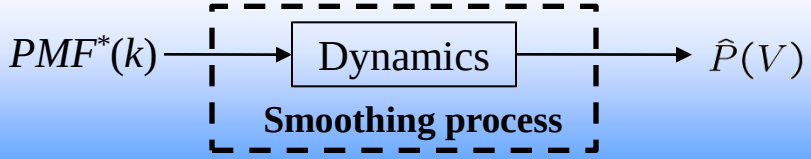
$$PMF_i^* = [P_L \quad P_N \quad P_H] = [\frac{1-B}{2} \quad B \quad \frac{1-B}{2}]$$

- Combination rule based on Demspter-Shafer theory (2 sensors):

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

can be extended to more than two sensors

- Combined PMF^* used as a target for a smoothing process to prevent abrupt changes in $\hat{P}(V)$



Assessment Layer

$\hat{P}(V_i), i = 1, 2, \ldots, M$ at time k → Assessment algorithm → $\hat{P}(G)$

- Consider one process variable with $\hat{P}(V)$ at time k.

From plant model and prior belief of *G*

- Jeffrey's rule:

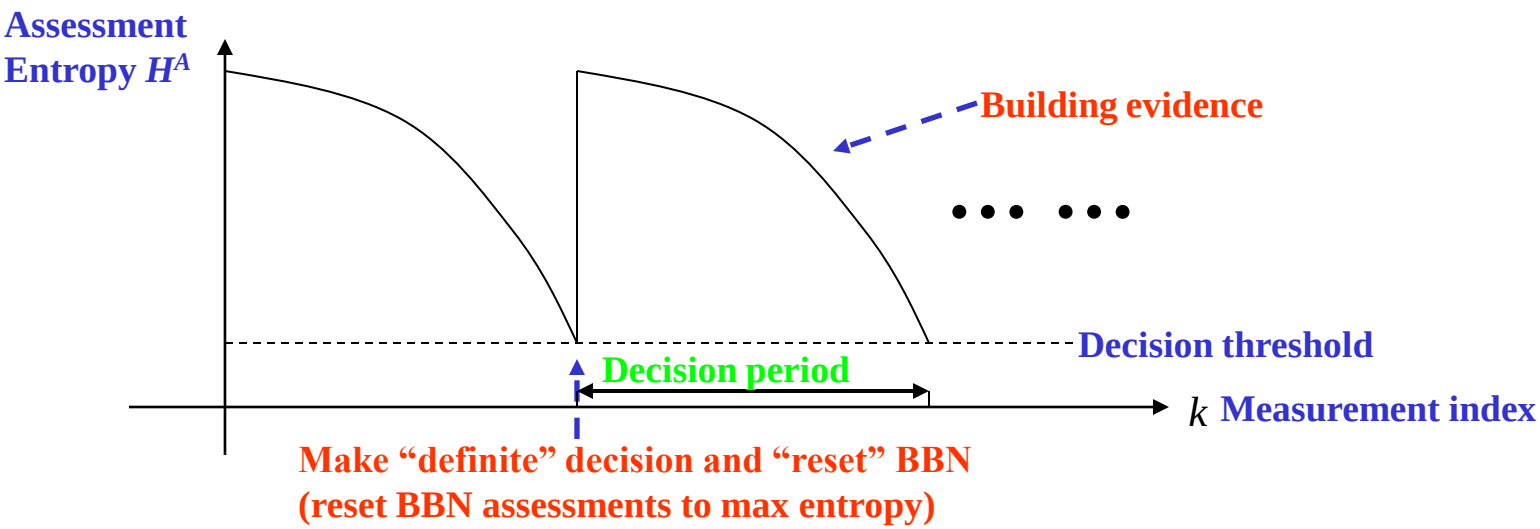
$$Q(G,V) = \begin{cases} P(G,V)\dfrac{\hat{P}(V)}{P(V)} & \text{if } P(V) \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

- Updated distribution of G, $\hat{P}(G)$ is then the marginal probability $Q(G)$

- Let $S(\hat{P}(V))$ be the set of all joint probability distributions of G and V such that the marginal probability of V is $\hat{P}(V)$.
- $Q(G,V)$ obtained by Jeffrey's rule above is the ***I*-projection** of $P(G,V)$ onto $S(\hat{P}(V))$, i.e., the distance from $P(G,V)$ to $Q(G,V)$ is minimum (w.r.t. Kullbeck-Leibler measure or relative entropy) among all distributions in $S(\hat{P}(V))$.
- **Question**: What if $\hat{P}(V_1)$ and $\hat{P}(V_2)$ are estimated at time k?
- **Solution**: Project $P(G,V_1,V_2)$ onto $S(\hat{P}(V_1)) \cap S(\hat{P}(V_2))$.
- **IPFP Idea**: Apply Jeffrey's rule *repeatedly*: Project $P(G,V_1,V_2)$ onto, $S(\hat{P}(V_1))$ and then project the result onto $S(\hat{P}(V_2))$, and then project the result onto $S(\hat{P}(V_1))$, and so on until convergence.
  - Implemented for BBN model using **virtual nodes**.

Assessment Entropy & Decisions

- Assessment algorithm is applied as $\hat{P}(V_i), i = 1, 2, \ldots, M$ are being calculated times k=1,2,…
- If current time is k, prior 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 plant decreases from its previous value calculated at k-1.



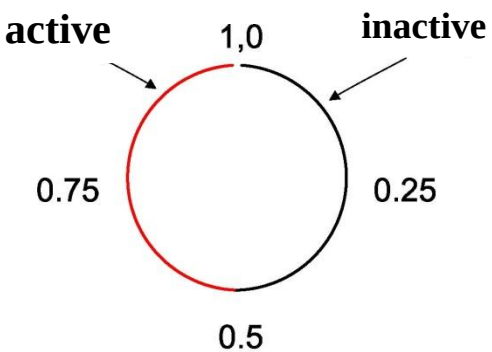
- Once the assessment entropy of plant decreases below a (user-defined) decision threshold, **a definite decision is made about the plant state** (e.g., whether the plant **is** normal, degrading, or down) and **the belief** of plant state is **reset to complete ignorance** (e.g., $P(G)$=[1/3 1/3 1/3]) for the subsequent assessment, and the assessment procedure repeats.

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

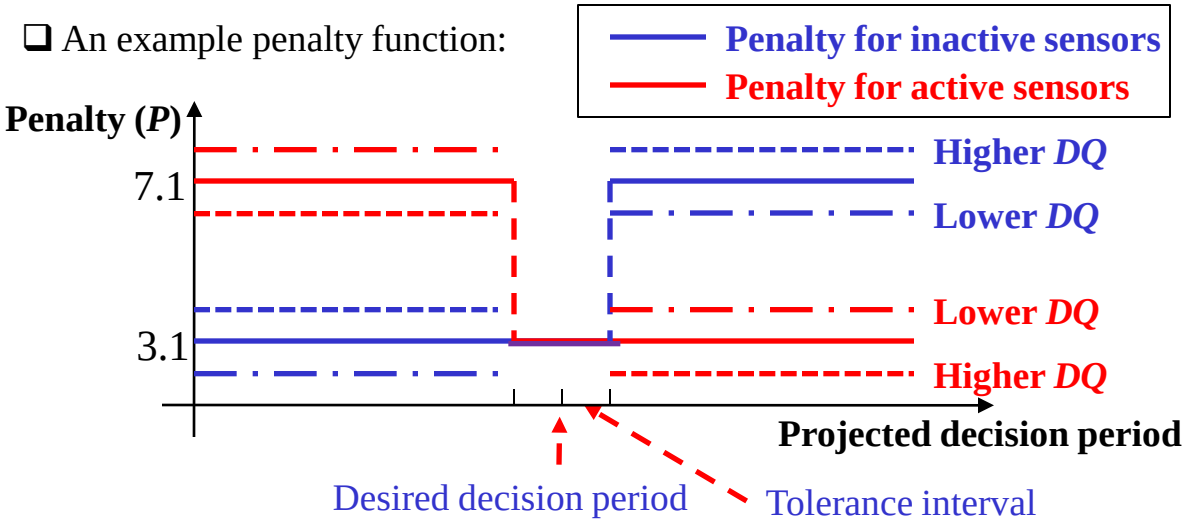
Sensor Selection Layer

- **Goal**: Select sensor configurations to meet (user-defined) decision period.
- Each sensor is equipped with a rational controller formulated as a ring element.
  - ❑ $\dot{x} = \varphi^N(\{x\})$
  - ❑ Ring elements are penalized so that decision period is achieved within some tolerance.

Ring element



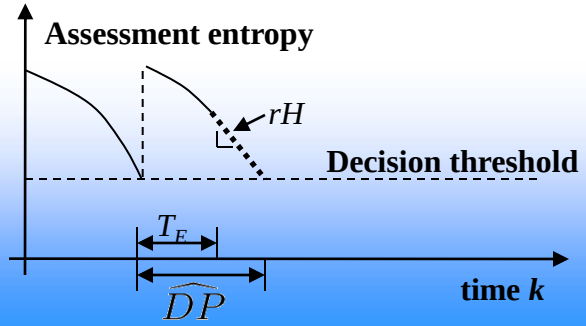
❑ An example penalty function:



Basic Idea:

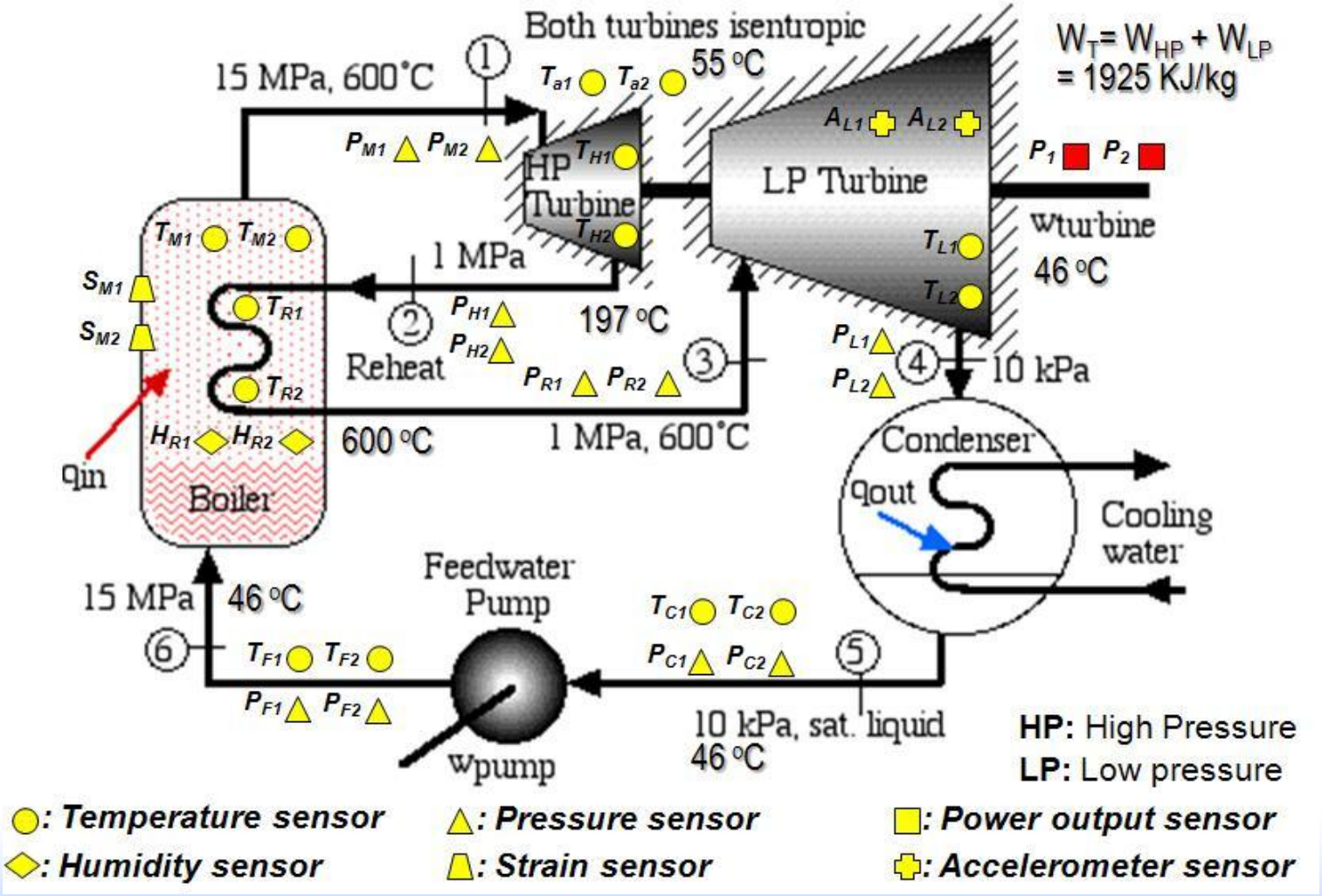
- If projected decision period $\widehat{DP}$ longer than desired, penalize **inactive** sensors;
- If $\widehat{DP}$ shorter than desired, penalize **active** sensors.
- Sensors with **high** DQ incur **less** penalty when active and **more** when inactive;
- Sensors with **low** DQ incur **more** penalty when active and **less** when inactive.

❑ **Projected decision period** ($\widehat{DP}$): calculated based on time elapsed (T_E) from last decision on plant state, assessment entropy decrease rate (rH), and decision threshold.

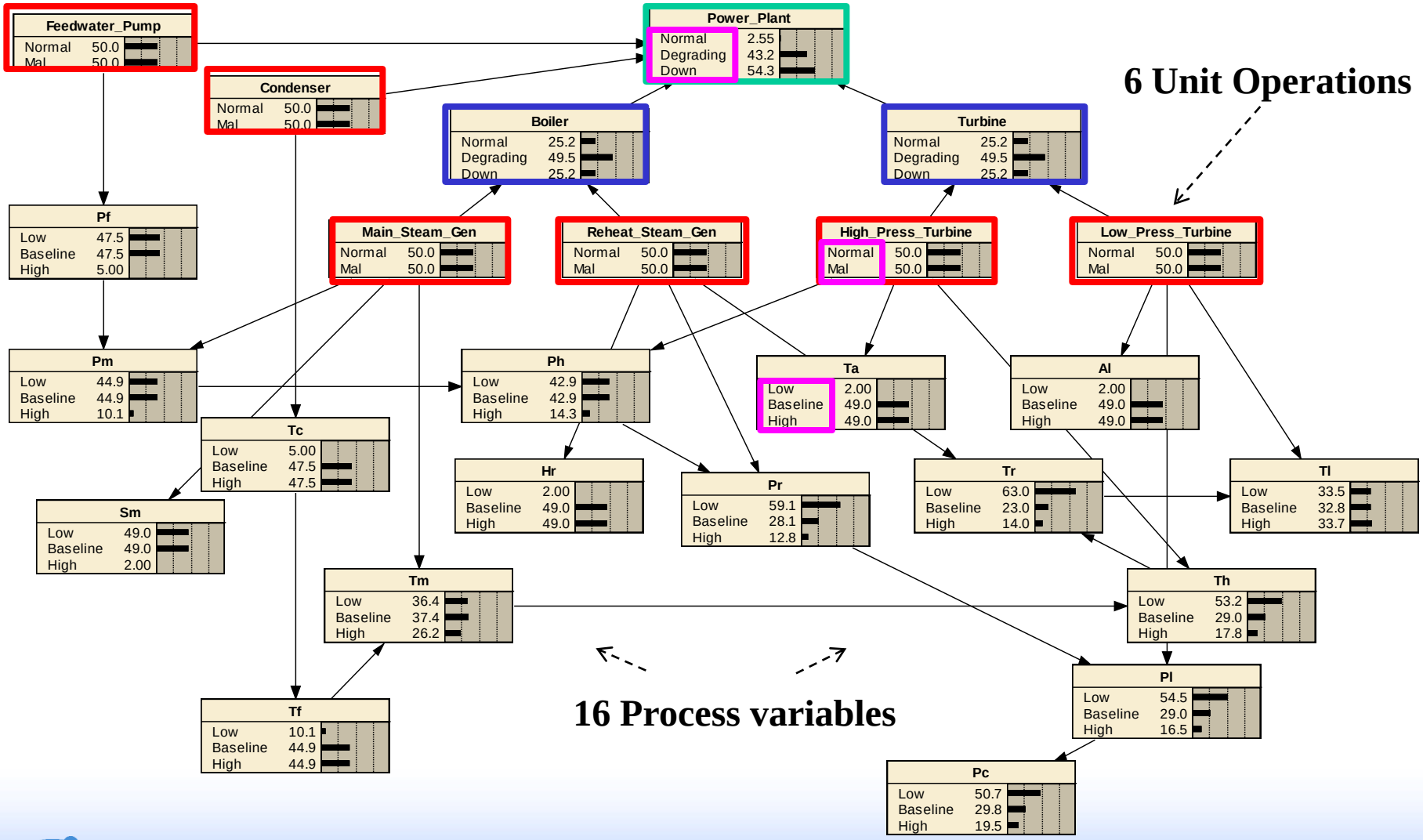


Simplified Power Plant Model

- Consider a power plant consisting of 6 unit operations and 16 process variables



BBN for Boiler-Turbine Power Plant

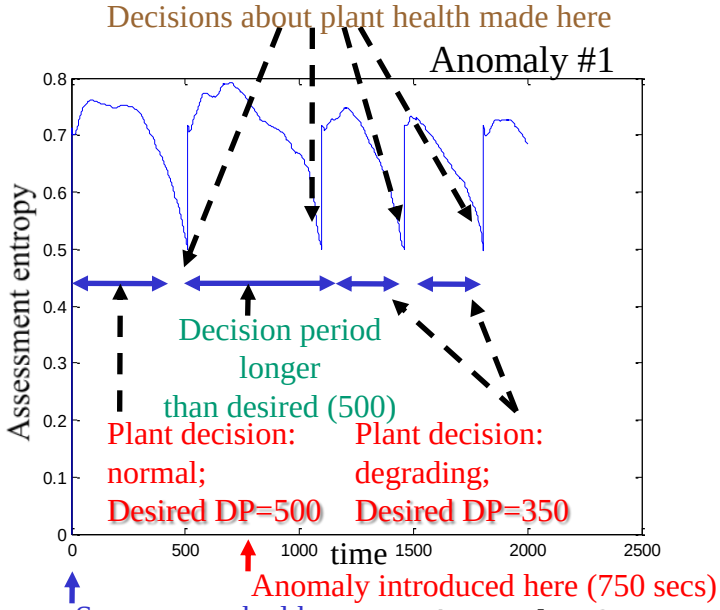


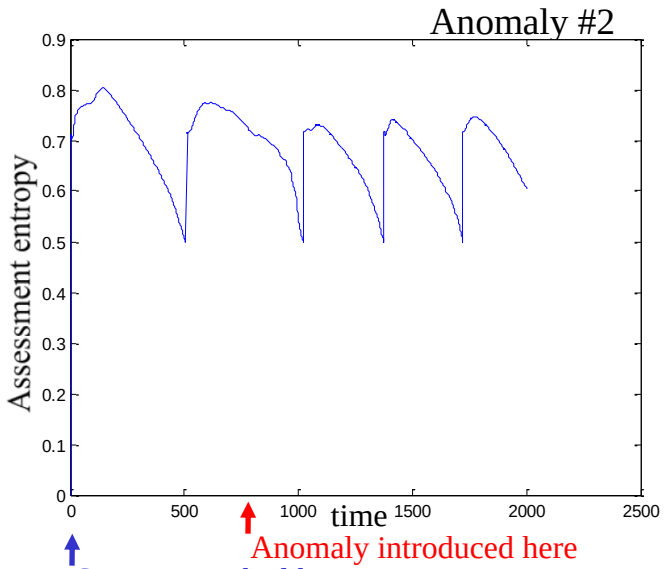
Idaho National Laboratory

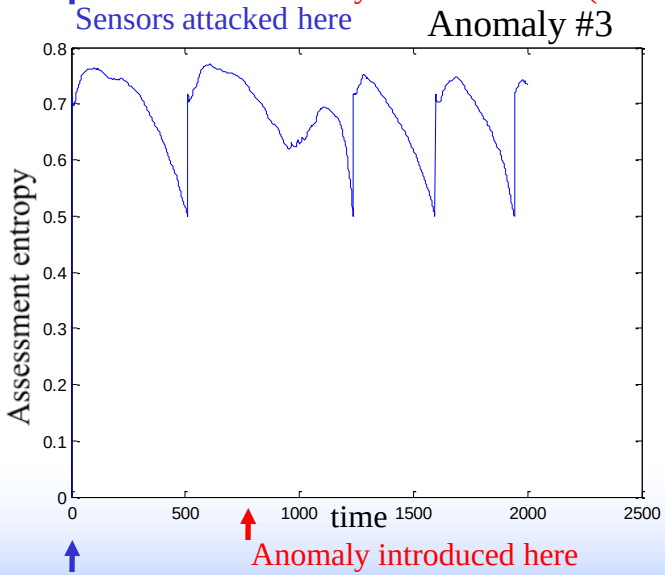
Anomalies / Cyber Attacks Considered

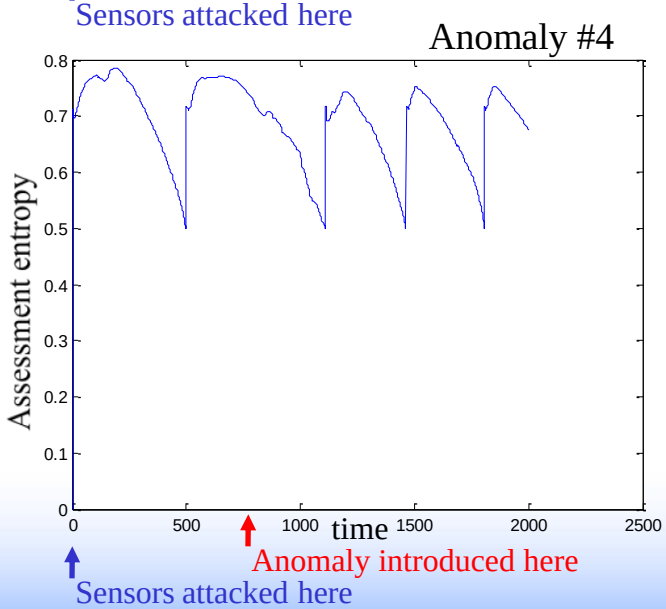
- **4 types of plant anomalies**:
  - ❑ **Anomaly #1**, in MSG: Low Heat Transfer (T_M < 600 °C, S_M < 4.56e-3)
  - ❑ **Anomaly #2**, in RSG: Pipeline rupture (P_R < 1 MPa, T_R < 600 °C, H_R > 4.6%)
  - ❑ **Anomaly #3**, in HPT: Improper Heat Insulation (T_H < 197 °C, T_a > 63.25 °C)
  - ❑ **Anomaly #4**, in LPT: Decreased Efficiency (T_L > 46 °C, A_L > 1.15)
- **Two sets of redundant sensors**, *A* & *B*, *e*ach set associated with given process variables
  - ❑ Sensors assumed to have additive Gaussian white noise with zero mean and accordingly computed variance.
- **Plant anomaly**:
  - ❑ Power plant operating normal from 0 to 749 seconds;
  - ❑ From 750 to 4000 seconds, reheat steam generator (RSG) is malfunctioning (pipeline rupture, Anomaly #2);
- **Sensor attacks** (i.e., sensor readings are added / subtracted a bias):
  - ❑ All sensors are normal from 0 to 1499 seconds;
  - ❑ Attack #1: From 1500 to 2499 seconds, 12 sensors attacked:
    - ➢ In set A, (3) sensors measuring pressure (P_R) and temperature (T_R) in RSG and humidity (H_R) in air around RSG are attacked (DQ = 0.3);
    - ➢ Three additional sensors in set A are randomly chosen to be attacked (DQ = 0.3);
    - ➢ Six sensors from set B are randomly chosen to be attacked (DQ = 0.3).
  - ❑ Attack #2: From 2500 to 4000 seconds, 12 sensors attacked:
    - ➢ Previously attacked sensors are restored;
    - ➢ Similar procedure is followed to choose the sensors to be attacked.

Half Sensors Are Attacked (DQ=0.1)





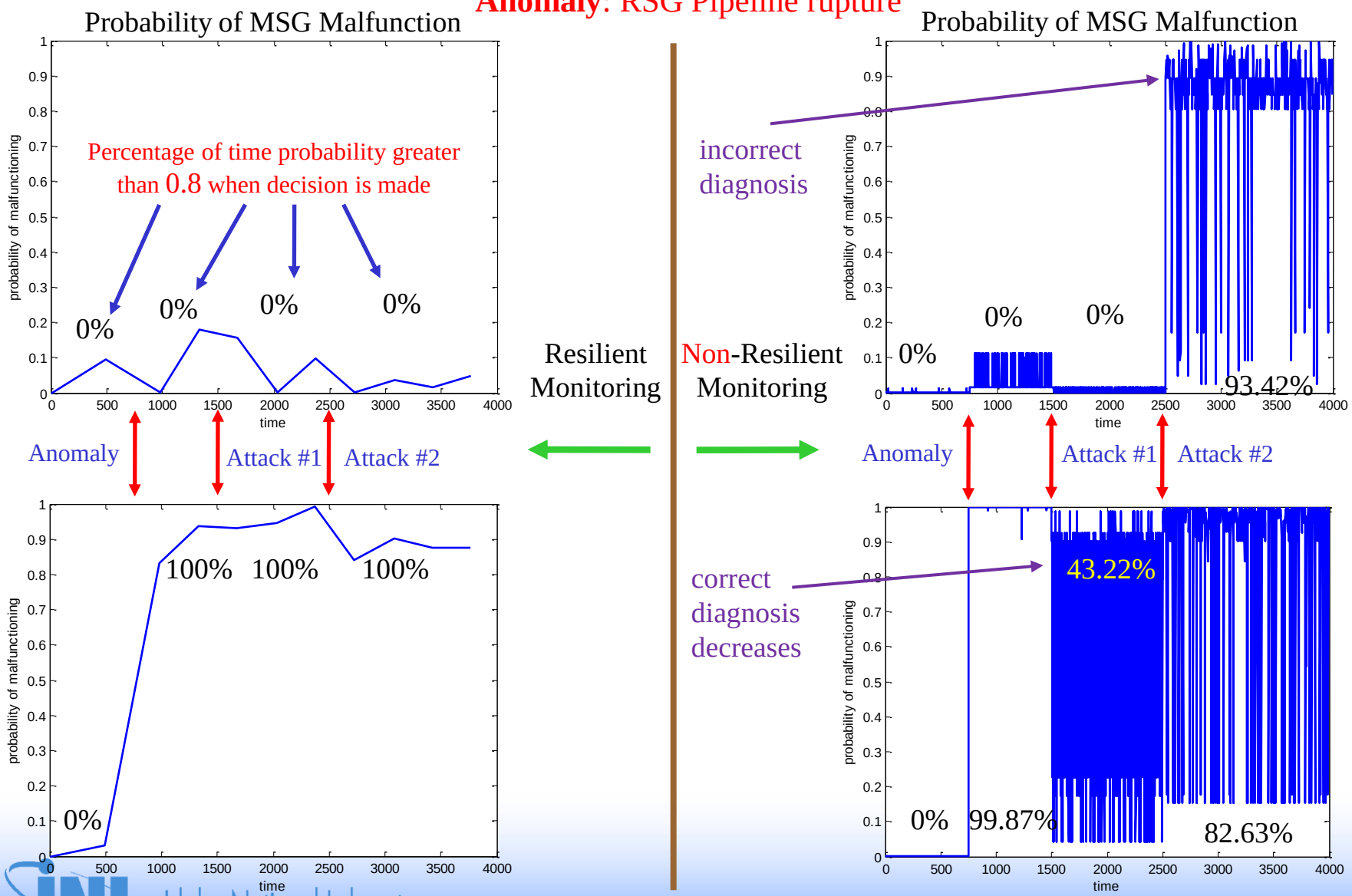




Idaho National Laboratory

Resilient vs Non-resilient: MSG and RSG

Anomaly: RSG Pipeline rupture

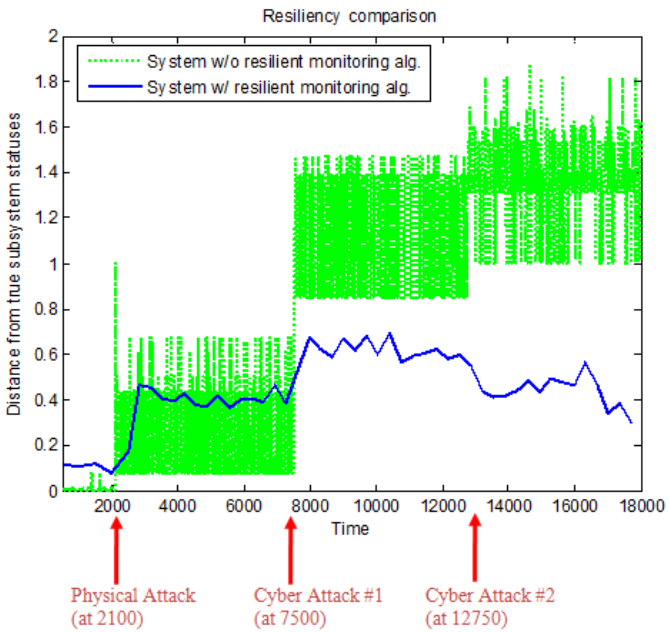


Resilient vs Non-resilient

# 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%

"Significant confusion in making a conclusive assessment under non-resilient monitoring case"

R: Resilient system **NR:** Non-resilient system



- **Measure of resiliency:** $\|T - \hat{T}\|_2$ with

$$T = [p_{MSG}\ p_{RSG}\ p_{HPT}\ p_{LPT}\ p_{FWP}\ p_{Condenser}]$$
$$\hat{T} = [\hat{p}_{MSG}\ \hat{p}_{RSG}\ \hat{p}_{HPT}\ \hat{p}_{LPT}\ \hat{p}_{FWP}\ \hat{p}_{Condenser}]$$

- *p_i=0 for $i \neq RSG$; p_{RSG}=0 for time < 2100; p_{RSG}=1 otherwise.*

where p_i and $\hat{p}_i$ are, the **true** and **estimated** probabilities that unit operation *i* is malfunctioning.

Idaho National Laboratory

Conclusions

- A resilient condition assessment monitoring (ReCAM) system is developed.

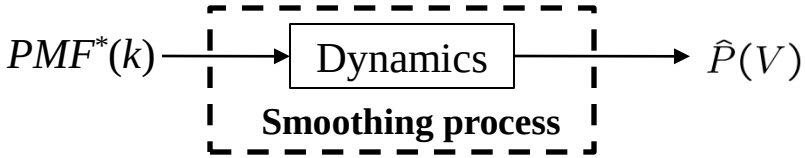
- Developed system is applied to a simplified power plant model and resiliency of the system is demonstrated.

- Results show that improved monitoring performance and resiliency can be achieved.

- Future work includes extending ReCAM to monitoring and protection of power grids and to control, resulting in a resilient monitoring, adaptation and control (ReMAC) system.

Backup Slide

Smoothing Process



- At each time instant k, $PMF^*(k)$ is calculated and the smoothing process is simulated.
- Dynamics for smoothing process is given by: $\tau \frac{d}{dt} PMF(t) = PMF^*(k) - PMF(t)$
  - ❑ At time t=0, $PMF(0)$ is uniformly distributed. 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 input $PMF^*(k)$ 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.