

Fault-Tolerant Operation and Control of Dynamical Systems

11/08/02

Christoforos Hadjicostis
Coordinated Science Lab. and Dept. of Electrical and Computer Engineering
University of Illinois, Urbana-Champaign

RESEARCH PROFILE

- **Monitoring and control of complex networked systems**
 - Infrastructure constraints (e.g. communication delays, packet drops)
 - Hardware, communication and/or algorithmic overhead
- **Fault-tolerant dynamic systems**
 - System dynamics and structure, coding for protection
 - Special-purpose architectures (e.g. communication, signal processing)
 - Implications to digital design (fast/inexpensive microprocessors)
- **Other interests**
 - Soft-decision decoding
 - Path/time diversity techniques in communication networks
 - Architectures for communication and signal processing systems

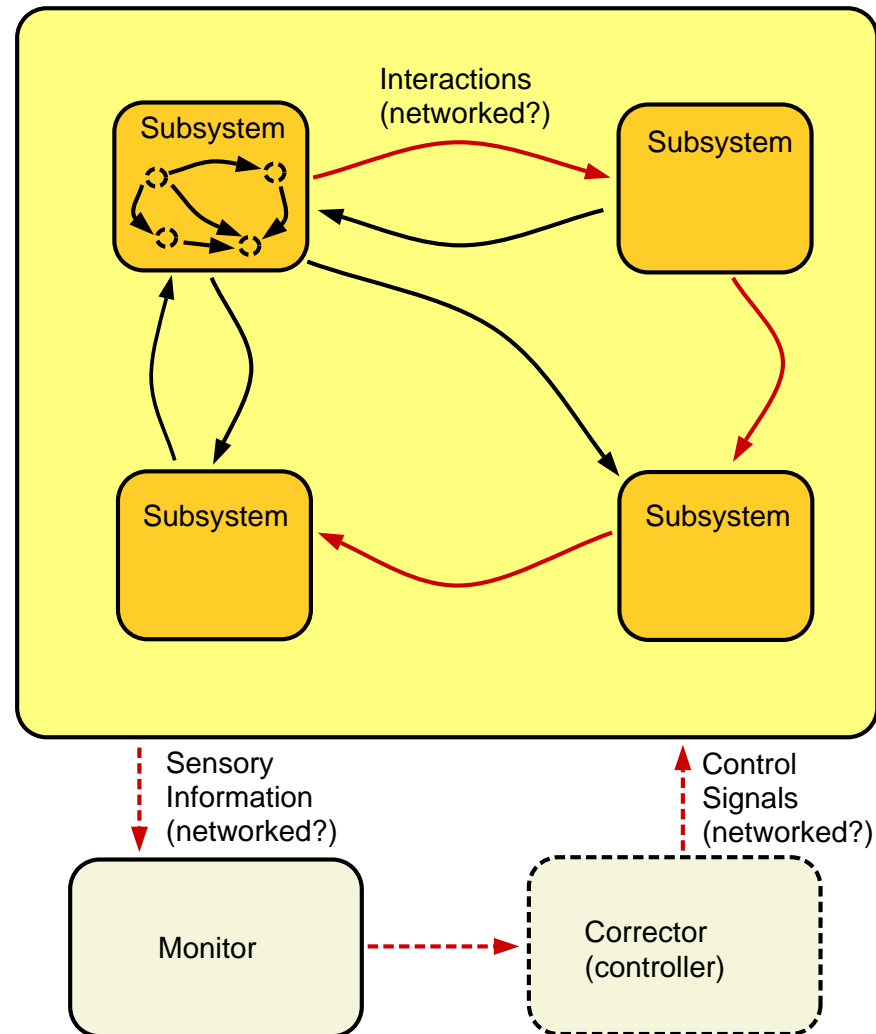
FAULT MONITORING AND TOLERANCE IN DISTRIBUTED SYSTEMS

Structural issues:

- Local vs global information
- Sensitivity to faults and delays
- Observability/controllability

Monitoring architecture:

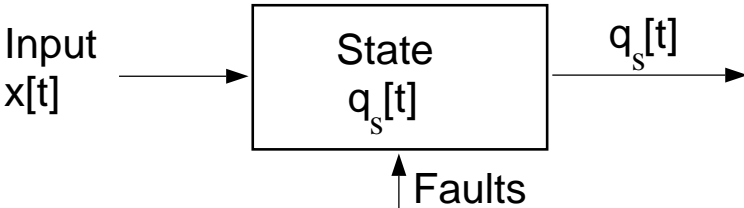
- Hierarchical vs distributed
- Sensor/actuator allocation
- Communication overhead
- Robustness to incomplete and/or incorrect data



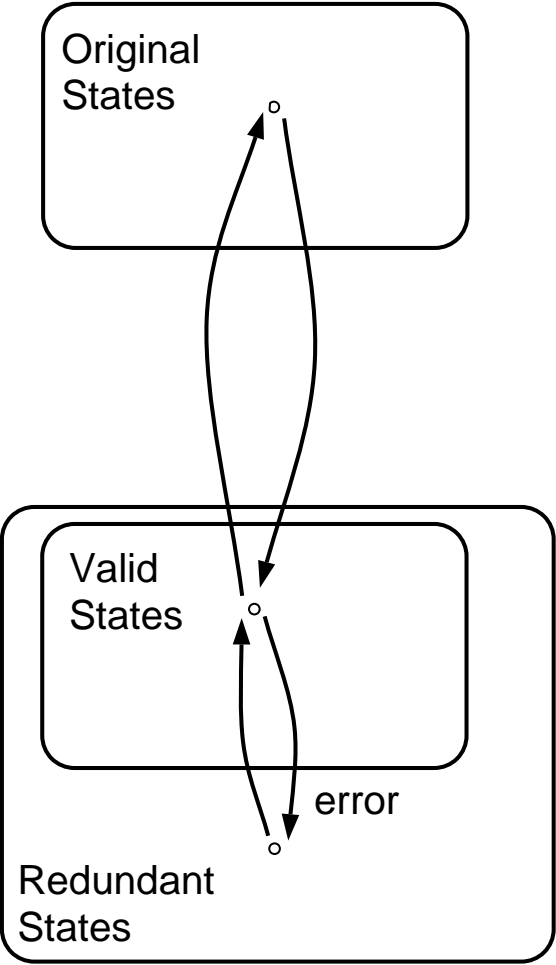
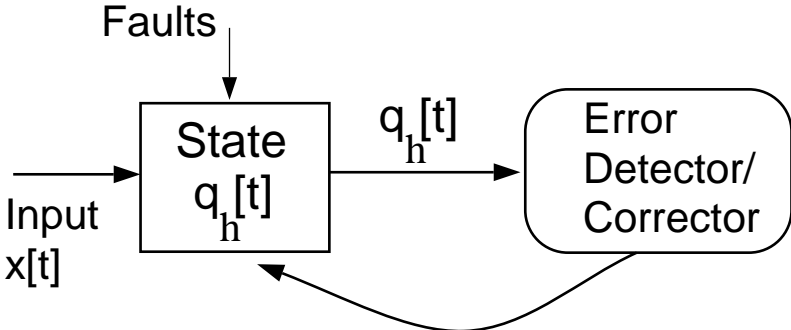
FAULT MONITORING AND TOLERANCE IN ENERGY PROCESSING SYSTEMS

- **Fault monitoring (ability to detect and identify faults)**
 - Tradeoffs between detection delay, complexity and redundancy
 - Role of system dynamics
- **Fault accommodation in energy processing systems**
 - Connections with fault tolerance schemes in digital systems
 - Reliability and availability considerations
 - Real-time constraints, performance guarantees, resource efficiency
 - Links between power systems and power electronics
- **ONR Control Challenge**

REDUNDANT IMPLEMENTATIONS (“CODED” SYSTEMS)

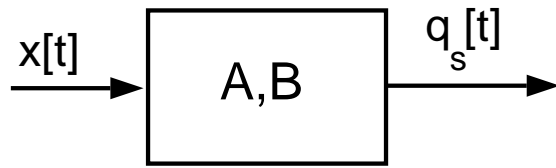


Replace with larger dynamic system:



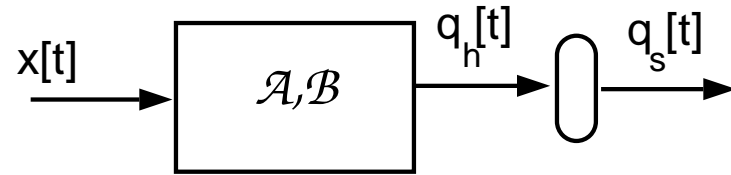
REDUNDANT IMPLEMENTATIONS OF DISCRETE-TIME LTI DYNAMIC SYSTEMS

Original System



$$\mathbf{q}_s[t + 1] = \mathbf{A}\mathbf{q}_s[t] + \mathbf{B}\mathbf{x}[t]$$

Redundant Implementation



$$\mathbf{q}_h[t + 1] = \mathcal{A}\mathbf{q}_h[t] + \mathcal{B}\mathbf{x}[t]$$

- **Concurrent simulation:** $\mathbf{q}_s[t] = \mathbf{L}\mathbf{q}_h[t]$
 - **Encoding constraints:** $\mathbf{q}_h[t] = \mathbf{G}\mathbf{q}_s[t]$
- } **Linear (not necessary)**

- **Fault detection:** If $\mathbf{q}_h[t]$ is *not* in the column space of \mathbf{G} , or

$$\mathbf{P}\mathbf{q}_h[t] \neq \mathbf{0}, \quad \mathbf{P}\mathbf{G} = \mathbf{0}$$

CHARACTERIZATION OF REDUNDANT IMPLEMENTATIONS

$$\left. \begin{array}{l}
 \underline{\text{Original System}} \\
 \mathbf{q}_s[t+1] = \mathbf{A}\mathbf{q}_s[t] + \mathbf{B}\mathbf{x}[t] \\
 \mathbf{q}_s \text{ is } d\text{-dimensional}
 \end{array} \right\}
 \begin{array}{l}
 \mathbf{q}_h[t] \xrightarrow{=\mathbf{G}} \mathbf{q}_s[t] \\
 \mathbf{q}_s[t] \xleftarrow{=\mathbf{L}} \mathbf{q}_h[t]
 \end{array}
 \left\{ \begin{array}{l}
 \underline{\text{Redundant Implementation}} \\
 \mathbf{q}_h[t+1] = \mathcal{A}\mathbf{q}_h[t] + \mathcal{B}\mathbf{x}[t] \\
 \mathbf{q}_h \text{ is } (d+s)\text{-dimensional}
 \end{array} \right.$$

Standard redundant implementations (Hadjicostis & Verghese 1999):

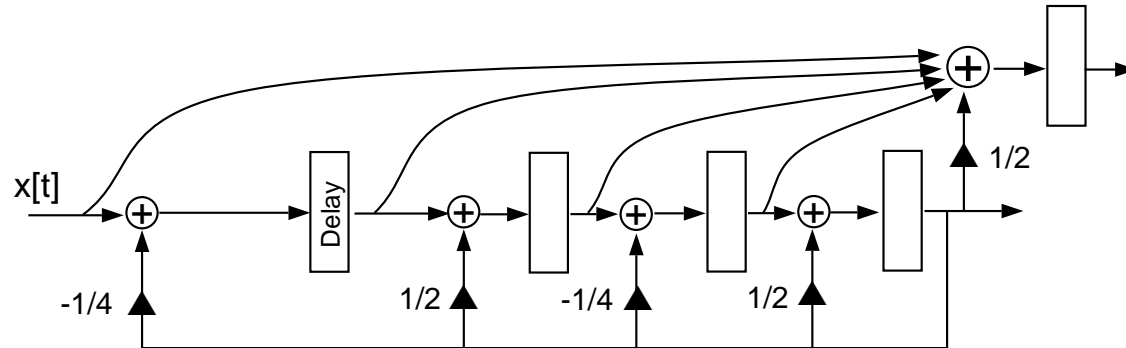
$(\mathcal{A}, \mathcal{B})$ is a redundant implementation for (\mathbf{A}, \mathbf{B}) iff $(\mathcal{A}, \mathcal{B})$ is similar to the following standard form:

$$\mathbf{q}_\sigma[t+1] = \underbrace{\begin{bmatrix} \mathbf{A} & \mathbf{A}_{12} \\ \mathbf{0} & \mathbf{A}_{22} \end{bmatrix}}_{\mathcal{A}_\sigma} \mathbf{q}_\sigma[t] + \underbrace{\begin{bmatrix} \mathbf{B} \\ \mathbf{0} \end{bmatrix}}_{\mathcal{B}_\sigma} \mathbf{x}[t]$$

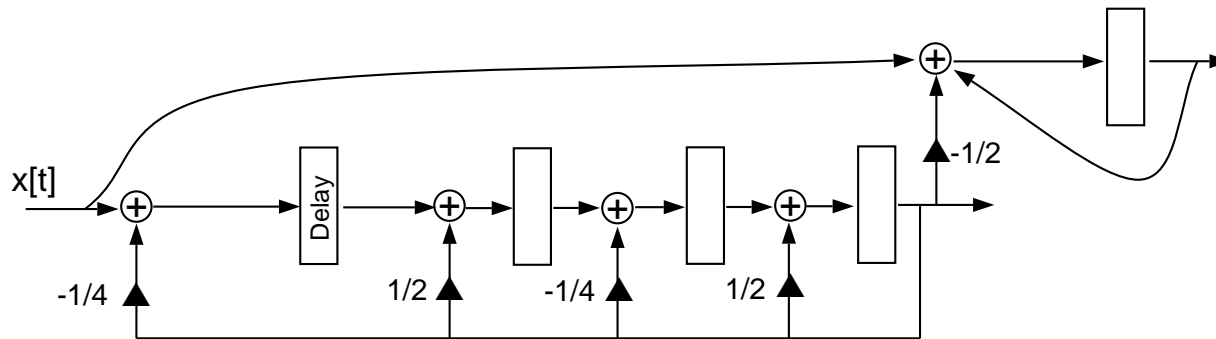
for some matrices $\mathbf{A}_{12}, \mathbf{A}_{22}$

EXAMPLE: REDUNDANT IMPLEMENTATIONS FOR CHECKSUM SCHEME

Traditionally:



Using previous theorem:



CONCURRENT CHECKING

Fault model: A single fault corrupts a single state variable

$$\mathbf{q}_f[t] = \underbrace{\mathbf{q}_h[t]}_{\text{fault-free}} + v \mathbf{e}_i$$

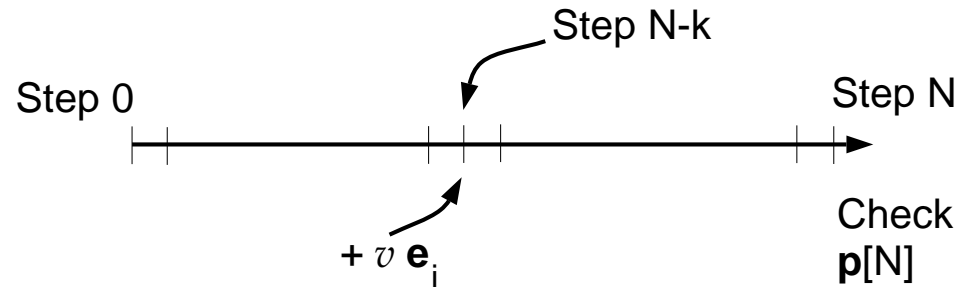
Justification: Constrained interconnections of adders, multipliers and delays
 \Rightarrow a single fault corrupts a single state variable

Concurrent error detection: At end of *each* time step, perform the *parity check*

$$\mathbf{p}[t] \equiv \mathbf{P} \mathbf{q}_f[t] = \mathbf{P} v \mathbf{e}_i \stackrel{?}{=} \mathbf{0}$$

Error detection/correction capabilities: Constraints on matrix \mathbf{P} (coding theory)

NON-CONCURRENT CHECKING



Goal: Design redundant implementation so that knowledge of $p[N]$ allows detection and identification of error(s) in the interval $[0, N]$

Motivation: Relax checking requirements (e.g., periodic checking)

Need: For each fault (f_j), identify

- Value (v_j)
- State variable (e_{i_j})
- Step ($N - k_j$)

NON-CONCURRENT CHECKING (2)

Error model: At step $N - k_j$, fault f_j causes

$$\mathbf{q}_f[N - k_j] = \mathbf{q}_h[N - k_j] + v_j \mathbf{e}_{i_j}$$

Error propagation: At step N ,

$$\mathbf{q}_f[N] = \mathbf{q}_h[N] + \mathcal{A}^{k_j} v_j \mathbf{e}_{i_j}$$

Parity check: At step N ,

$$\mathbf{p}[N] = \mathbf{P} \mathbf{q}_f[N] = v_j \mathbf{P} \mathcal{A}^{k_j} \mathbf{e}_{i_j}$$

Multiple errors result in:

$$\mathbf{p}[N] = \sum_{j=1}^D v_j \mathbf{P} \mathcal{A}^{k_j} \mathbf{e}_{i_j}$$

Task: Construct the redundant implementation so that D errors can be identified

SYNDROME GENERATION

Observation: Syndrome $\mathbf{p}[N]$ is a linear combination of columns of

$$\mathbf{S} = [\mathbf{P} \quad \mathbf{PA} \quad \mathbf{PA}^2 \quad \cdots \quad \mathbf{PA}^N]$$

Lemma 1: Detection of D errors *if and only if*
all sets of D columns of \mathbf{S} are linearly independent
 \Rightarrow Need at least D additional variables ($s \geq D$)

Lemma 2: Identification of D errors *if and only if*
all sets of $2D$ columns of \mathbf{S} are linearly independent
 \Rightarrow Need at least $2D$ additional variables ($s \geq 2D$)

Theorem (Hadjicostis 2001): The syndrome matrix \mathbf{S} can be expressed as

$$\mathbf{S} = [\mathbf{P} \quad \mathbf{A}_{22}\mathbf{P} \quad \mathbf{A}_{22}^2\mathbf{P} \quad \cdots \quad \mathbf{A}_{22}^N\mathbf{P}]$$

CONSTRUCTION FOR NON-CONCURRENT IDENTIFICATION OF D ERRORS

Fact: Any $2D$ columns of \mathbf{V} are linearly independent if $x_i \neq x_j$

$$\mathbf{V}(x_1, x_2, \dots, x_r) = \begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_r \\ x_1^2 & x_2^2 & \dots & x_r^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{2D-1} & x_2^{2D-1} & \dots & x_r^{2D-1} \end{bmatrix}$$

Construction of redundant implementation:

- $2D$ additional state variables ($s = 2D$)
- $\Lambda = \text{diag}(1, x, x^2, x^3, \dots, x^{2D-1})$, $\mathbf{M} = \mathbf{V}(x_{d+1}, x_{d+2}, \dots, x_\eta)$

- **Step 1:** In standard coordinates, set

$$\mathbf{A}_{22} = \mathbf{M}^{-1} \Lambda \mathbf{M} \text{ and } \mathbf{C} = -\mathbf{M}^{-1} \mathbf{V}(x_1, x_2, \dots, x_d)$$

- **Step 2:** Perform similarity transformation with $\mathcal{T} = \begin{bmatrix} \mathbf{I}_d & \mathbf{0} \\ \mathbf{C} & \mathbf{I}_{2D} \end{bmatrix}$

THEOREM AND PROOF

Theorem (Hadjicostis 2001):

Resulting redundant implementation allows non-concurrent

- (i) identification of D errors, or
- (ii) detection of $2D$ errors

Why? Syndrome matrix \mathbf{S} can be written as

$$\mathbf{S} = \mathbf{M}^{-1} \underbrace{\mathbf{V}(x_1, \dots, x_\eta, x_1x, \dots, x_\eta x, x_1x^2, \dots, x_\eta x^2, \dots, x_1x^N, \dots, x_\eta x^N)}_{\mathbf{Q}}$$

\mathbf{Q} is a *large* Vandermonde matrix ($2D \times (\eta(N + 1))$ -dimensional)

Requirement: Choose $x, x_1, x_2, \dots, x_\eta$ so that $x_i x^k$ are *unique*

\Rightarrow any $2D$ columns of \mathbf{Q} are linearly independent

FURTHER DISCUSSION

- Perform one non-concurrent parity check at time step N :

$$\mathbf{p}[N] = \mathbf{P} \mathbf{q}_f[N]$$

- (i) Detect $2D$ faults
 - (ii) Identify D faults
- } On any variable, at any step in $[0, N]$

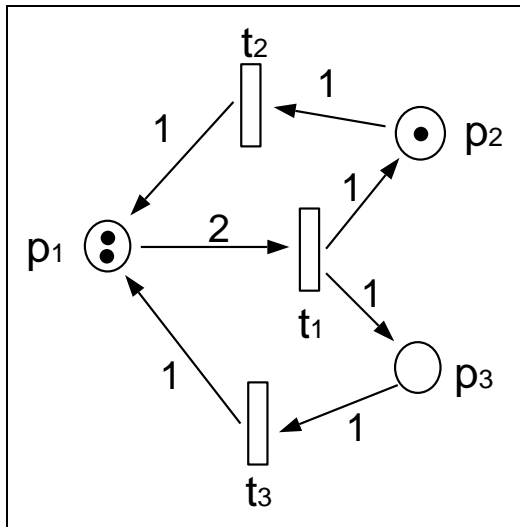
- When allowed to implement systems, we need to choose:

- (i) Encoding constraints (\mathbf{P} or \mathbf{G})
- (ii) Redundant dynamics (\mathbf{A}_{22})
- (iii) Efficient, robust, fast identification schemes

- When given a fixed system (e.g. a power system/network), we need to:

- Analyze parity schemes based on available sensory information
- Consider optimal allocation of any additional sensors, use of redundancy

FAULT DIAGNOSIS IN DES: PETRI NET MODELS



If transition t_1 “fires”:

$$\mathbf{q}[t + 1] = \underbrace{\begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}}_{\text{“state } \mathbf{q}[t]\text{”}} + \underbrace{\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}}_{\text{“postconditions”}} - \underbrace{\begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}}_{\text{“preconditions”}}$$

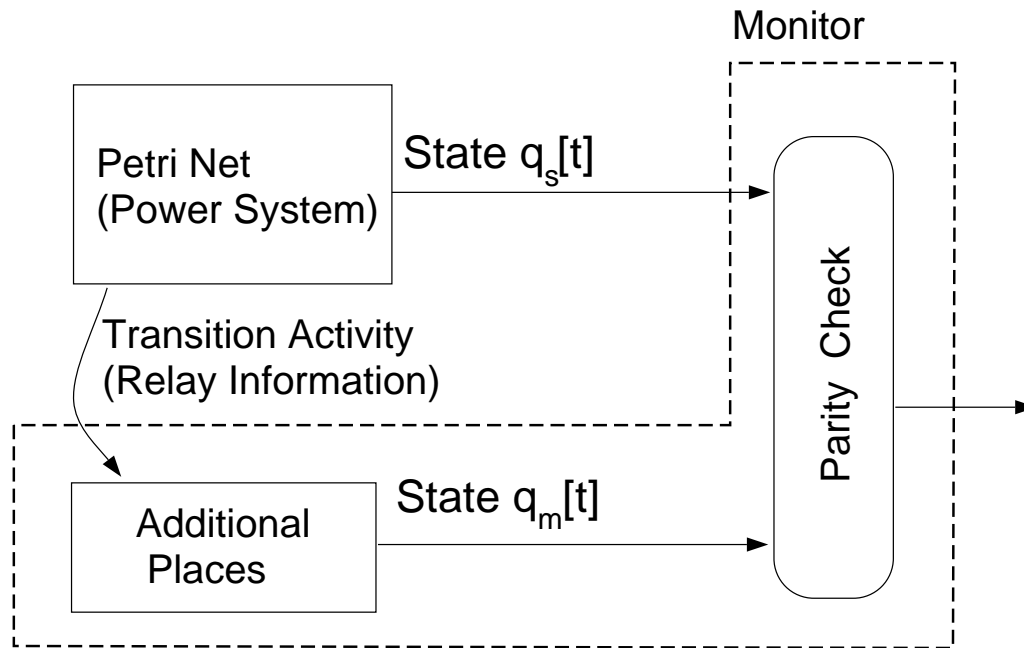
$$\mathbf{B}^+ = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \mathbf{B}^- = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \mathbf{x}[t] = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

“State Evolution”:
$$\mathbf{q}[t + 1] = \mathbf{q}[t] + \underbrace{(\mathbf{B}^+ - \mathbf{B}^-)}_{\mathbf{B}} \mathbf{x}[t]$$

Interpretation depends on underlying DES; most commonly:

- **Tokens:** System resources, acknowledgments, packets
- **Places:** Buffers, storage locations, preconditions, postconditions
- **Transitions:** Events, actions, processors, servers, machinery

CONCURRENT MONITORING USING LINEAR CHECKS



Invariant condition:

$$\mathbf{q}_m[t] = \mathbf{C}\mathbf{q}_s[t]$$

$\mathbf{q}_s[\cdot]$ is n -dimensional

$\mathbf{q}_m[\cdot]$ is d -dimensional

- State evolution of embedding: $\mathbf{q}_h[t + 1] = \mathbf{q}_h[t] + \begin{bmatrix} \mathbf{B} \\ \mathbf{CB} \end{bmatrix} \mathbf{x}[t]$

where $\mathbf{q}_h[t] = \begin{bmatrix} \mathbf{q}_s[t] \\ \mathbf{q}_m[t] \end{bmatrix}$

- Parity check: $\underbrace{\begin{bmatrix} -\mathbf{C} & \mathbf{I}_d \end{bmatrix}}_{\mathbf{P}} \mathbf{q}_h[t] \stackrel{?}{=} \mathbf{0}$

SYNDROME-BASED DETECTION AND IDENTIFICATION OF FAILURES

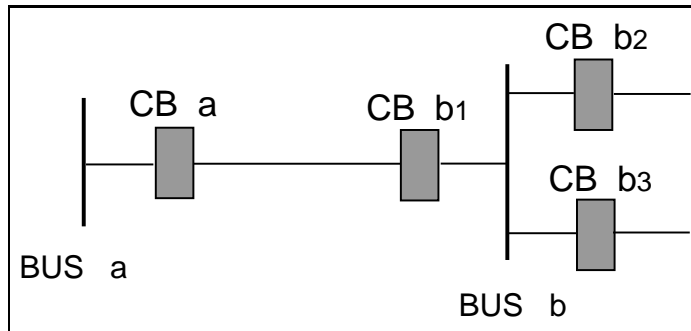
- **Additive error model:** $\mathbf{q}_f[t] = \underbrace{\mathbf{q}_h[t]}_{\text{fault free}} + \mathbf{e}_f$

- **Parity check / Syndrome generation:**

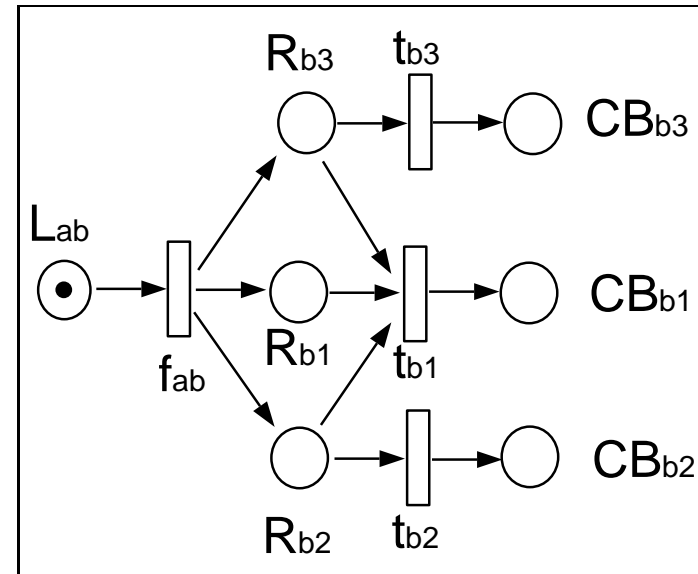
$$\mathbf{s}[t] = \underbrace{\begin{bmatrix} -\mathbf{C} & \mathbf{I}_d \end{bmatrix}}_{\mathbf{P}} \mathbf{q}_f[t] = \mathbf{P}\mathbf{e}_f$$

- **Single Error Detection:** Choose \mathbf{C} so that syndromes are non-zero
- **Single Error Identification:** Choose \mathbf{C} so that syndromes are unique
- **Multiple Errors:** Applications of linear algebra and coding theory

PETRI NET MODELING OF LINE FAILURES

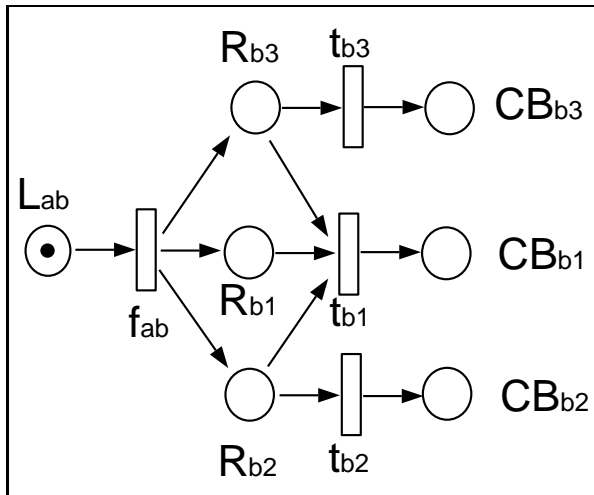


Discrete Event Model



- Transition f_{ab} models failure in line $a-b$
- Primary protection: Relay R_{b1} and circuit breaker CB_{b1}
- Secondary protection: Relays R_{b2} , R_{b3} and circuit breakers CB_{b2} , CB_{b3}
- See Hadjicostis & Verghese, "Power System Monitoring using Petri Net Embeddings," IEE Proceedings C, vol. 147, no. 5, pp. 299-303, September 2000

PETRI NET MODELING OF LINE FAILURES (2)



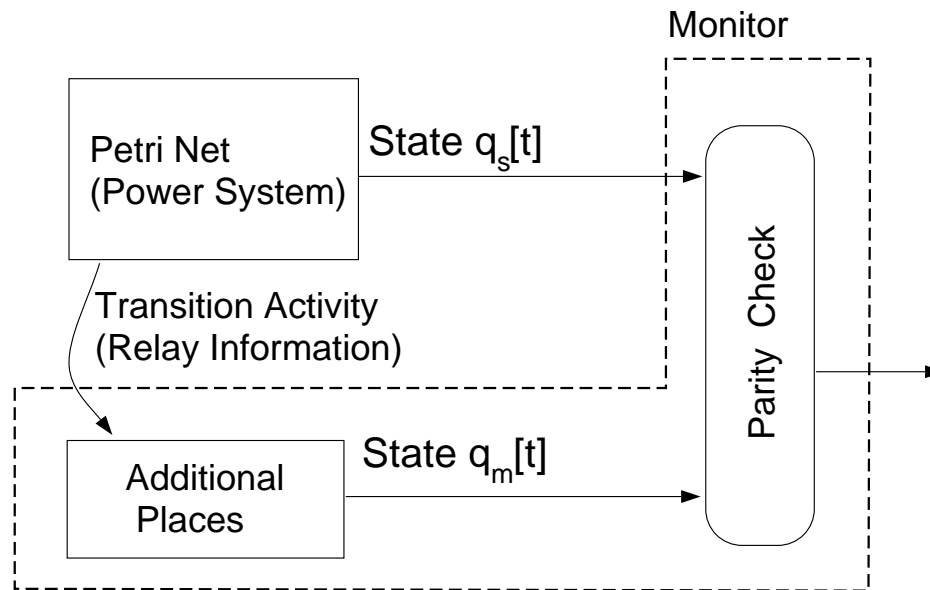
$$\mathbf{q}_s[t+1] \equiv \begin{bmatrix} L_{ab}[t+1] \\ R_{b1}[t+1] \\ R_{b2}[t+1] \\ R_{b3}[t+1] \\ CB_{b1}[t+1] \\ CB_{b2}[t+1] \\ CB_{b3}[t+1] \end{bmatrix} = \mathbf{q}_s[t] + \underbrace{\begin{bmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 0 \\ 1 & -1 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}}_{\mathbf{B}} \mathbf{x}[t]$$

Monitor does NOT have access to:

- Transition f_{ab}
- Places L_{ab} and R_{b1}, R_{b2}, R_{b3}

⇒ Need to deal with unobservable/unavailable information

IMPLICATIONS TO MONITOR DESIGN



Enforce Invariant condition:

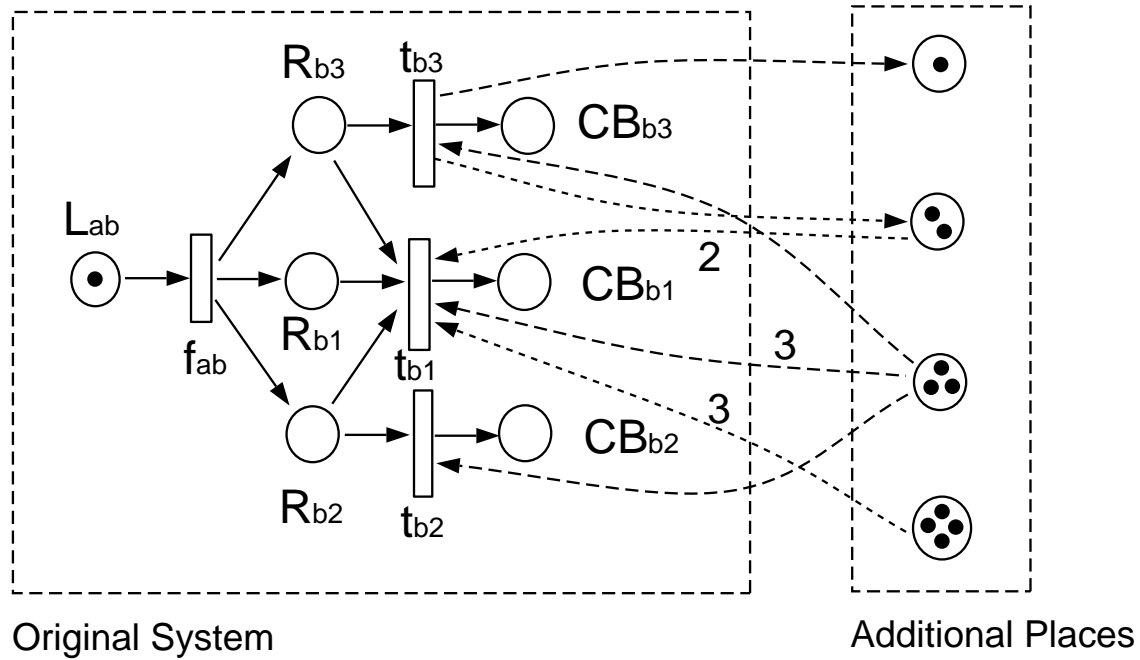
$$\mathbf{q}_m[t] = \mathbf{C}\mathbf{q}_s[t]$$

$\mathbf{q}_s[\cdot]$ has dimension 7

$\mathbf{q}_m[\cdot]$ has dimension 4

- No transition information from f_{ab} implies $\mathbf{CB}(:, 1) = \mathbf{0}$
- Unique syndrome $\mathbf{s}[t] = \begin{bmatrix} -\mathbf{C} & \mathbf{I}_4 \end{bmatrix} \mathbf{e}_f$ for each combination of failures
- \mathbf{e}_f needs to be specified for different failures f

MONITOR DESIGN



$$C = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 & 0 & 1 & 1 \\ 3 & 1 & 1 & 1 & 0 & 0 & 0 \\ 4 & 2 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$CB = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & -2 & 0 & 1 \\ 0 & -3 & -1 & -1 \\ 0 & -3 & 0 & 0 \end{bmatrix}$$

CODING-BASED DIAGNOSIS: SYNDROMES FOR DIFFERENT FAILURES

1. Line Failure f_{ab} :

$$\text{Faulty State: } \mathbf{q}_{f_{ab}}[t] = \mathbf{q}_h[t] + \mathbf{e}_1$$

$$\text{Syndrome: } \mathbf{s}_{f_{ab}}[t] = \mathbf{P}\mathbf{q}_{f_{ab}}[t] = -\mathbf{C}(:, 1)$$

2. Misfiring of Circuit Breakers f_{b_j} :

$$\text{Faulty State: } \mathbf{q}_{f_{b_j}}[t] = \mathbf{q}_h[t] + \begin{bmatrix} \mathbf{0} \\ \mathbf{CB} \end{bmatrix} \mathbf{x}_{tb_j} - \mathbf{e}_{R_{b_j}}$$

$$\text{Syndrome: } \mathbf{s}_{f_{b_j}}[t] = \mathbf{P}\mathbf{q}_{f_{b_j}}[t] = (\mathbf{CB})(:, j + 1) + \mathbf{C}(:, j + 1)$$

3. Erroneous/Missing Reports from Circuit Breakers $f_{CB_{b_i}}$:

$$\text{Faulty State: } \mathbf{q}_{f_{CB_{b_i}}}[t] = \mathbf{q}_h[t] \pm \mathbf{e}_{CB_{b_i}}$$

$$\text{Syndrome: } \mathbf{s}_{CB_{b_i}}[t] = \mathbf{P}\mathbf{q}_f[t] = \mp \mathbf{C}(:, i + 4)$$

IMMEDIATE RESEARCH PLANS

- **Fault tolerance in continuous-time systems**
 1. Fault detection, parity methods, sensor allocation, thresholding
 2. Computer-based diagnosers, links with discrete-event systems
 3. Checking/protection of the correcting mechanism (resources permitting)
- **Role of redundancy, reconfiguration**
 1. Fault modeling, upset modeling
 2. Rollback, reset, restart
 3. Fault detection delay vs complexity/accuracy considerations
 4. Control of electrical machines
- **Application: ONR Control Challenge (resources permitting)**