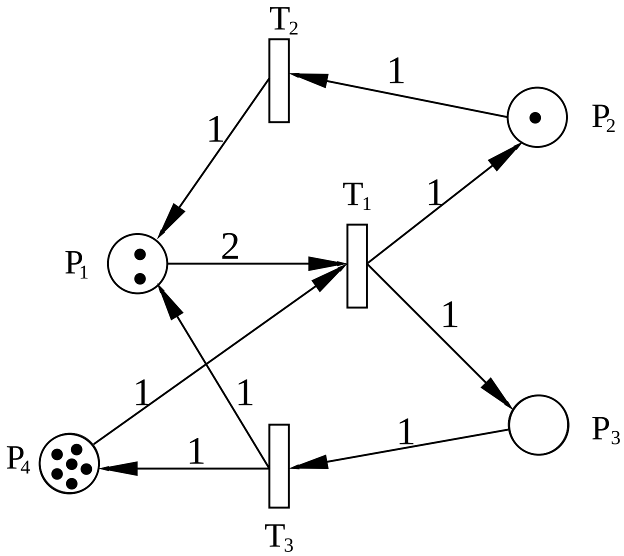
Centralized and Distributed Fault Identification in Discrete Event Systems

Yingquan Wu and Christoforos N. Hadjicostis

Coordinated Science Laboratory and
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

July 2003

PETRI NET NOTATION



Places: $\{P_1,\ \ P_2,\ \ \ldots,\ \ P_n\}$

Transitions: $\{T_1,\ \ T_2,\ \ \ldots,\ \ T_m\}$

Marking: Tokens at each place
E.g., $\mathbf{q}_s[t] = [2\ \ 1\ \ 0\ \ 6]^T$

- Matrix notation for arc weights:

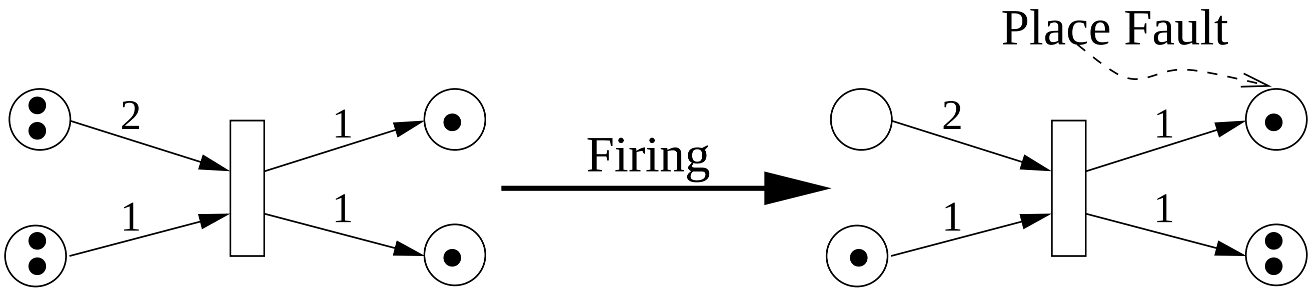
$$\mathbf{B}^- : P_i \xrightarrow{b_{ij}^-} T_j\ , \qquad \mathbf{B}^+ : T_j \xrightarrow{b_{ij}^+} P_i\ , \qquad \mathbf{B} \triangleq \mathbf{B}^+ - \mathbf{B}^-$$

- State (marking) evolution:

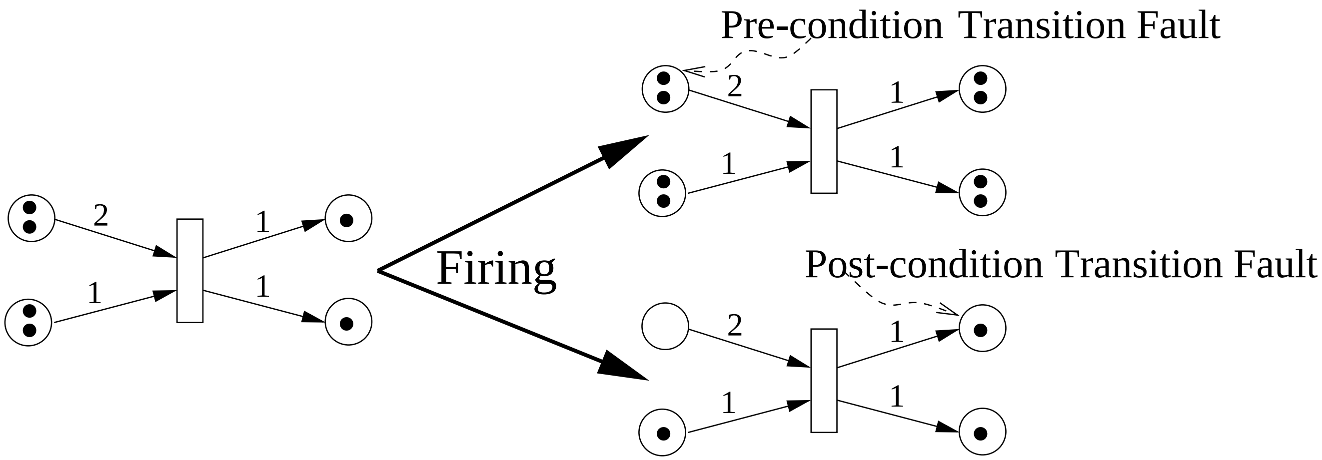
$$\mathbf{q}_s[t+1] = \mathbf{q}_s[t] + \mathbf{B}\mathbf{x}[t], \quad \mathbf{q} \geq \mathbf{0}, \ \ \mathbf{x} > \mathbf{0}$$

FAULT TYPES AND MODELS

- Place fault: $\mathbf{q}_f[t] = \mathbf{q}_s[t] + \mathbf{e}_P$



- Transition fault: $\mathbf{q}_f[t] = \mathbf{q}_s[t] + \mathbf{B}^- \mathbf{e}_T^-$ or $\mathbf{q}_f[t] = \mathbf{q}_s[t] - \mathbf{B}^+ \mathbf{e}_T^+$



PROBLEM FORMULATION

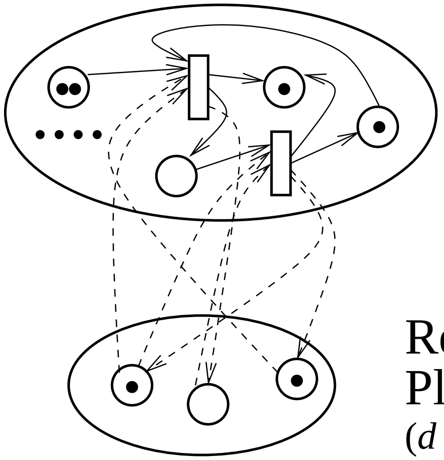
- Assumptions:
  - Underlying DES modeled as Petri net
  - Unobservable transitions
  - Periodically observable place marking
- Objective: Based on the (periodically observable) place marking

Non-concurrently identify transition and place faults

REDUNDANT PETRI NET EMBEDDING

- *Encoded* Petri net marking:

$$\mathbf{q}_h[t] = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{C} \end{bmatrix} \mathbf{q}_s[t]$$



Underlying DES
(n places, m transitions)

Redundant
Places
(d places)

- Arc weights given by (**C** and **D** are matrices to be designed):

$$\mathcal{B}^+ = \left[\frac{\mathbf{B}^+}{\mathbf{C}\mathbf{B}^+ - \mathbf{D}} \right], \qquad \mathcal{B}^- = \left[\frac{\mathbf{B}^-}{\mathbf{C}\mathbf{B}^- - \mathbf{D}} \right]$$

- Periodic observability:

$$\mathbf{q}_f[N] = \mathbf{q}_h[N] - \mathcal{B}^+\mathbf{e}_T^+ + \mathcal{B}^-\mathbf{e}_T^- + \mathbf{e}_P$$

FRAMEWORK

- Parity check: $\mathbf{s}[N] \overset{\triangle}{=} \mathbf{P}\mathbf{q}_f[N] = \underbrace{\begin{bmatrix} -\mathbf{C} & \mathbf{I}_d \end{bmatrix}}_{\mathbf{P}} \mathbf{q}_f[N]$
- $\mathbf{s}[N] = \mathbf{0}$ under no (transition or place) faults
- Design criteria for identification scheme:
  - Low complexity
  - Small number of redundant places and redundant arc weights
- Main result: Given a Petri net with m transitions and n places and using $2k$ redundant places,
  - any k place and any $2k-1$ transition faults can be identified
  - complexity is $O(k^2 m + kn)$

TRANSITION FAULT IDENTIFICATION

- Accumulation of transition faults: $\mathbf{q}_f[N] = \mathbf{q}_h[N] - \mathcal{B}^+\mathbf{e}_T^+ + \mathcal{B}^-\mathbf{e}_T^-$
- Transition fault syndrome:

$$\begin{aligned}\mathbf{s}[N] &\triangleq \mathbf{P}\mathbf{q}_f[N] \\ &= [-\mathbf{C} \;\; \mathbf{I}_d]\left(\mathbf{q}_h[N] - \begin{bmatrix}\mathbf{B}^+ \\ \mathbf{C}\mathbf{B}^+ - \mathbf{D}\end{bmatrix}\mathbf{e}_T^+ + \begin{bmatrix}\mathbf{B}^- \\ \mathbf{C}\mathbf{B}^- - \mathbf{D}\end{bmatrix}\mathbf{e}_T^-\right) \\ &= \mathbf{D}(\underbrace{\mathbf{e}_T^+ - \mathbf{e}_T^-}_{\mathbf{e}_T}) = \mathbf{D}\mathbf{e}_T, \qquad \text{where} \quad \mathbf{e}_T \in \mathbb{Z}^m\end{aligned}$$

- Assumptions about transition faults:

— No cancellations ⟷ $\min\{\mathbf{e}_T^+,\ \mathbf{e}_T^-\} = \mathbf{0}$

— Up to k faults ⟷ $\sum_{i=1}^m |e_T^i| \leq k$

TRANSITION FAULT IDENTIFICATION (2)

- Design of matrix $\mathbf{D}$ with k redundant places:

$$\mathbf{D}_k \triangleq \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 3 & \dots & m \\ 1 & 2^2 \bmod p & 3^2 \bmod p & \dots & m^2 \bmod p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2^k \bmod p & 3^k \bmod p & \dots & m^k \bmod p \end{pmatrix}$$

- Up to $k-1$ transition faults can be identified

- Complexity is $O(k^2 m)$

- Methodology described in Y. Wu and C. N. Hadjicostis, “On solving composite power polynomial equations.” Submitted to *Mathematics of Computation*

PLACE FAULT IDENTIFICATION

- Accumulation of place faults: $\mathbf{q}_f[N] = \mathbf{q}_h[N] + \mathbf{e}_P$
- Place fault syndrome: $\mathbf{s}_P[N] \triangleq \mathbf{P}\mathbf{q}_f[N] = \begin{bmatrix} -\mathbf{C} & \mathbf{I}_d \end{bmatrix} \mathbf{e}_P$,
  where $\mathbf{e}_P \in \mathbb{Z}^{n+d}$
- Assumptions about place faults:
  - — Up to k faults $\longleftrightarrow$ Maximum of k nonzero entries in $\mathbf{e}_P$
  - — Erroneous number of tokens in a place bounded in $[-\frac{p-1}{2}, \ \frac{p-1}{2}]$
- Connections to decoding of Reed-Solomon codes in GF(p):
  - – Natural mapping: $e \to e \pmod p$
  - – Transformation to systematic form: $\mathbf{H} = \mathbf{\Phi} \underbrace{\begin{bmatrix} -\mathbf{C} & \mathbf{I}_d \end{bmatrix}}_{\mathbf{P}}$

PLACE FAULT IDENTIFICATION (2)

- Design of matrix **P** with $2k$ redundant places ($\eta = n + 2k$):

$$\mathbf{P}_{2k} = \underbrace{\begin{pmatrix} \alpha^{\eta-2k} & \alpha^{\eta-2k+1} & \dots & \alpha^{\eta-1} \\ \alpha^{2(\eta-2k)} & \alpha^{2(\eta-2k+1)} & \dots & \alpha^{2(\eta-1)} \\ \alpha^{3(\eta-2k)} & \alpha^{3(\eta-2k+1)} & \dots & \alpha^{3(\eta-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2k(\eta-2k)} & \alpha^{2k(\eta-2k+1)} & \dots & \alpha^{2k(\eta-1)} \end{pmatrix}^{-1}}_{\mathbf{\Phi}^{-1}} \underbrace{\begin{pmatrix} 1 & \alpha^{1} & \alpha^{2} & \alpha^{3} & \dots & \alpha^{\eta-1} \\ 1 & \alpha^{2} & \alpha^{4} & \alpha^{6} & \dots & \alpha^{2(\eta-1)} \\ 1 & \alpha^{3} & \alpha^{6} & \alpha^{9} & \dots & \alpha^{3(\eta-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2k} & \alpha^{4k} & \alpha^{6k} & \dots & \alpha^{2k(\eta-1)} \end{pmatrix}}_{\tilde{\mathbf{H}}_{2k}}$$

- Up to k place faults can be identified:
  (i) Set $\mathbf{s}'_P[N] = \mathbf{\Phi}\mathbf{s}_P[N] \pmod{p}$
  (ii) Apply the Berlekamp-Massey algorithm

- Complexity is $O(k\eta) = O(k^2 + kn)$

SYNTHESIS FOR MIXED FAULTS

- Fault syndrome:

$$\mathbf{s}[N] \overset{\triangle}{=} \mathbf{P}\mathbf{q}_f[N] = \mathbf{P}(\mathbf{q}_h[N] - \mathcal{B}^+\mathbf{e}_T^+ + \mathcal{B}^-\mathbf{e}_T^- + \mathbf{e}_P)$$

$$= \mathbf{D}\mathbf{e}_T + \mathbf{P}\mathbf{e}_P$$

- Matrix design:

$$\mathbf{D}^* \overset{\triangle}{=} -p \cdot \mathbf{D}$$

$$\mathbf{C}^* \overset{\triangle}{=} p \cdot \mathbf{1} - \mathbf{C}, \quad \mathbf{P}^* \overset{\triangle}{=} [-\mathbf{C}^* \quad \mathbf{I}] = [\mathbf{C} - p \cdot \mathbf{1} \quad \mathbf{I}]$$

- Place fault syndrome:

$$\mathbf{s}_P \equiv \mathbf{s}[N] \equiv [\mathbf{C}^* \quad \mathbf{I}]\mathbf{e}_P \pmod{p}$$

$$\mathbf{s}'_P \overset{\triangle}{=} \mathbf{\Phi}\mathbf{s}_P \equiv \mathbf{\Phi}[\mathbf{C}^* \quad \mathbf{I}]\mathbf{e}_P \equiv \mathbf{H}\mathbf{e}_P \pmod{p}$$

SYNTHESIS FOR MIXED FAULTS (2)

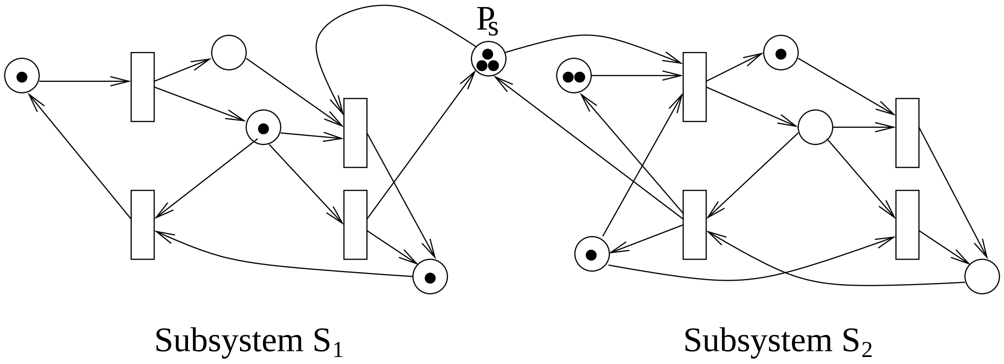
- Transition fault syndrome:

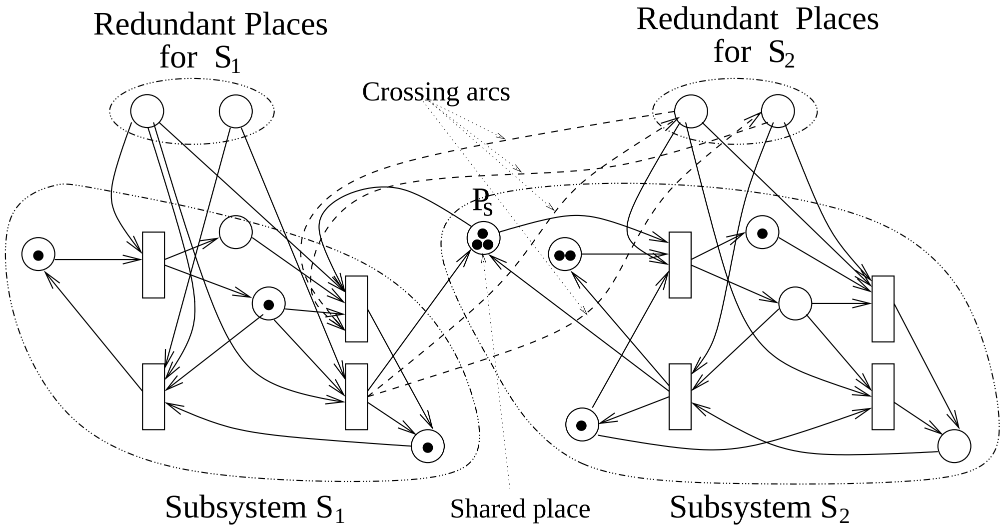
$$\mathbf{s}_T \overset{\triangle}{=} (\mathbf{s}[N] - \mathbf{P}^*\mathbf{e}_P)/p = (\mathbf{D}^*/p)\mathbf{e}_T = -\mathbf{D}\mathbf{e}_T$$

- With $2k$ redundant places, can simultaneously identify:
  - Up to $2k-1$ transition faults $(\min\{\mathbf{e}_T^-,\ \mathbf{e}_T^+\} = \mathbf{0})$
  - Up to k place faults $(|e_P^i| \leq \frac{p-1}{2})$

- Complexity is $O(k^2m + k\eta) = O(k^2m + kn)$

SIMPLE DISTRIBUTED SYSTEM





COMPENSATION RULE IN DISTRIBUTED SYSTEMS

- When the firing of a transition in $\mathcal{S}_1$ *generates* tokens in places of $\mathcal{S}_2$:

Choose arc weights: $\mathbf{w}^{(2)+} = \mathbf{C}^{(2)*}\mathbf{e}_P^{(2)} \qquad (\mathbf{e}_P^{(2)} \geq \mathbf{0})$

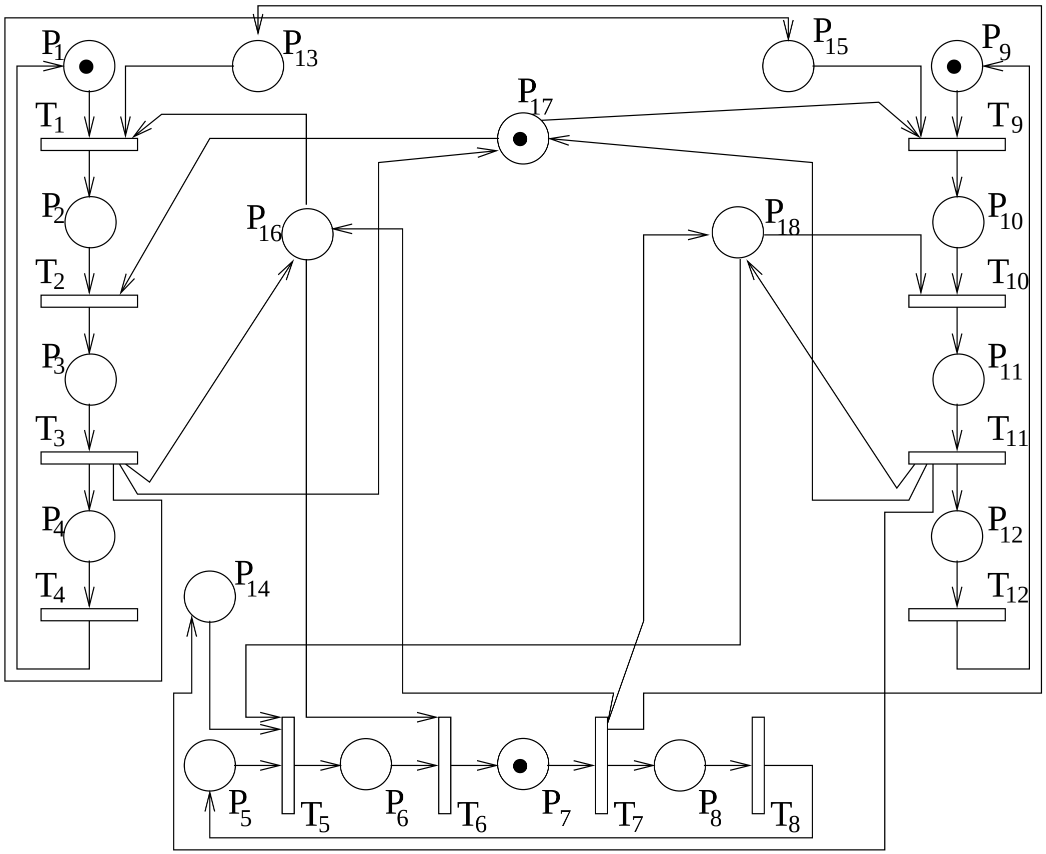
Parity check:
$$\mathbf{P}\mathbf{q}_f^{(2)}[t] = [-\mathbf{C}^{(2)*} \;\; \mathbf{I}_d](\mathbf{q}_h^{(2)}[t] + \begin{bmatrix} \mathbf{e}_P^{(2)} \\ \mathbf{w}^{(2)+} \end{bmatrix}) = -\mathbf{C}^{(2)*}\mathbf{e}_P^{(2)} + \mathbf{w}^{(2)+} = \mathbf{0}$$

- When the firing of a transition in $\mathcal{S}_1$ *consumes* tokens from places of $\mathcal{S}_2$:

Choose arc weights: $\mathbf{w}^{(2)-} = -\mathbf{C}^{(2)*}\mathbf{e}_P^{(2)} \qquad (\mathbf{e}_P^{(2)} \leq \mathbf{0})$

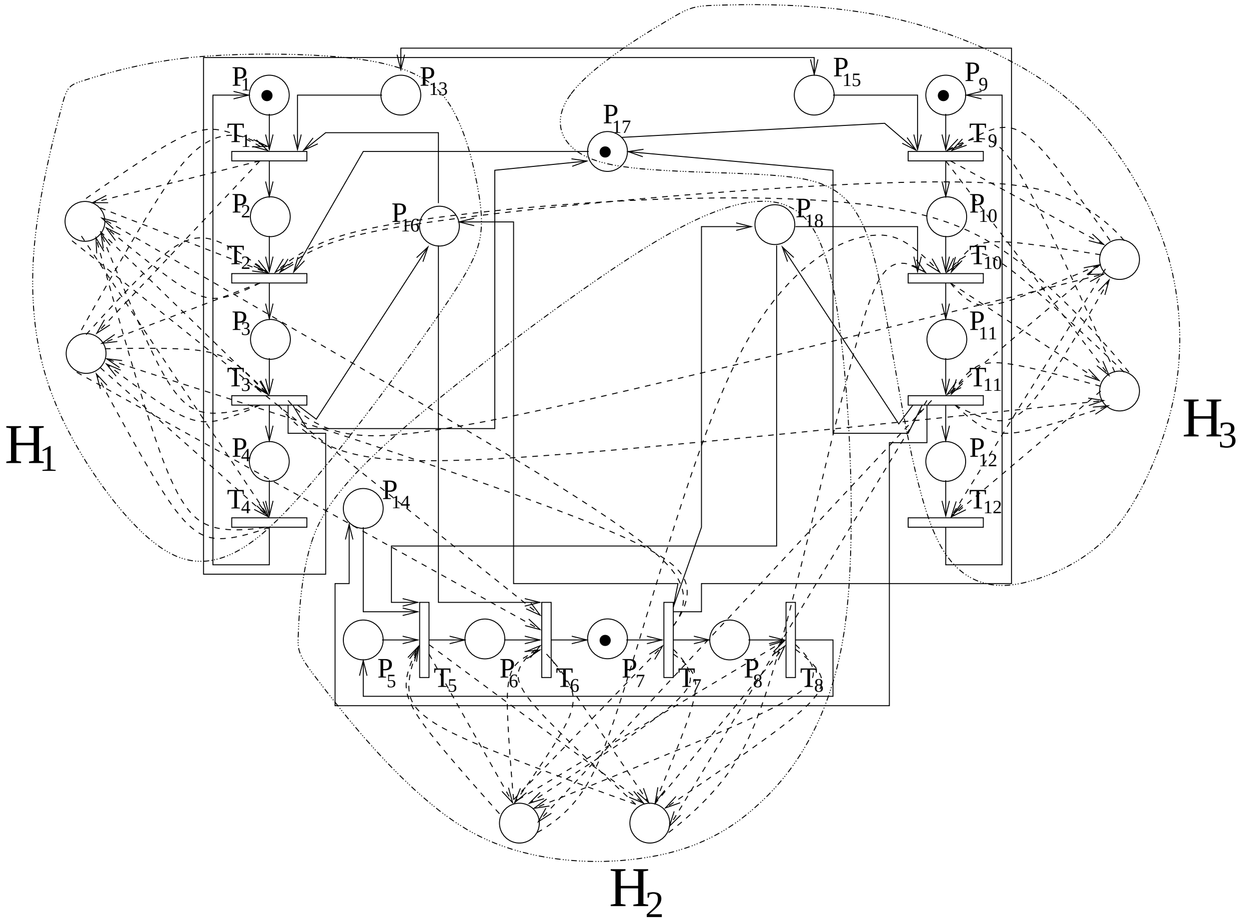
Parity check:
$$\mathbf{P}\mathbf{q}_f^{(2)}[t] = [-\mathbf{C}^{(2)*} \;\; \mathbf{I}_d](\mathbf{q}_h^{(2)}[t] + \begin{bmatrix} \mathbf{e}_P^{(2)} \\ -\mathbf{w}^{(2)-} \end{bmatrix}) = -\mathbf{C}^{(2)*}\mathbf{e}_P^{(2)} - \mathbf{w}^{(2)-} = \mathbf{0}$$

EXAMPLE: THREE MACHINES AND THREE ROBOTS



Example taken from Al-Jaar and Desrochers, “Petri nets in automation and manufacturing.” In *Advances in Automation and Robotics*, 1990

EXAMPLE: SYSTEM DECOMPOSITION



Identify two transition faults and/or one place fault

($|e_P^i| \leq 5$ in each subsystem)

REDUNDANT EMBEDDING FOR SUBSYSTEM S_1

- Choose prime $p = 11$, primitive element $\alpha = 2$
- Parity check matrix decomposition:

$$\tilde{\mathbf{H}} = \begin{pmatrix} 1 & 2 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 \\ 1 & 2^2 & 2^4 & 2^6 & 2^8 & 2^{10} & 2^{12} & 2^{14} \end{pmatrix} \equiv \underbrace{\begin{pmatrix} 9 & 7 \\ 4 & 5 \end{pmatrix}}_{\boldsymbol{\Phi}} \underbrace{\left(\begin{array}{cccccc|cc} 7 & 8 & 3 & 9 & 8 & 9 & 1 & 0 \\ 10 & 1 & 3 & 10 & 3 & 4 & 0 & 1 \end{array} \right)}_{\mathbf{P}^{(1)}=[\mathbf{C}^{(1)}\ \ \mathbf{I}_2]} \pmod{11}$$

- Matrix design:

$$\mathbf{D}^{(1)*} = -11 \cdot \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1^2 & 2^2 & 3^2 & 4^2 \end{pmatrix} \pmod{11} \right\} = \begin{pmatrix} -11 & -22 & -33 & -44 \\ -11 & -44 & -99 & -55 \end{pmatrix}$$

$$\mathbf{C}^{(1)*} = 11 - \begin{pmatrix} 7 & 8 & 3 & 9 & 8 & 9 \\ 10 & 1 & 3 & 10 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 8 & 2 & 3 & 2 \\ 1 & 10 & 8 & 1 & 8 & 7 \end{pmatrix}$$

DISTRIBUTED REDUNDANT EMBEDDING

- Redundant arc weights:

$$\mathbf{C}^{(1)*}\mathbf{B}^{(1)-} - \mathbf{D}^{(1)*} = \begin{pmatrix} 20 & 25 & 41 & 46 \\ 27 & 54 & 107 & 56 \end{pmatrix}$$

$$\mathbf{C}^{(1)*}\mathbf{B}^{(1)+} - \mathbf{D}^{(1)*} = \begin{pmatrix} 14 & 30 & 37 & 48 \\ 21 & 52 & 107 & 56 \end{pmatrix}$$

- Crossing arc weights:

$$T_7 : \quad \mathbf{w}_7^{(1)+} = \mathbf{C}^{(1)*} \cdot (0\ 0\ 0\ 0\ 1\ 1)^T = \begin{pmatrix} 5 \\ 15 \end{pmatrix}$$

$$T_6 : \quad \mathbf{w}_6^{(1)-} = -\mathbf{C}^{(1)*} \cdot (0\ 0\ 0\ 0\ 0\ \ -1)^T = \begin{pmatrix} 2 \\ 7 \end{pmatrix}$$

Sequence of Events and Faults

$$
\begin{array}{rlllrrl}
 & \mathbf{q}_f^{(0)}[1] & = (1\ 0\ 0\ 0\ 0\ 0 & 4 & 1) & \text{Fault-free} \\
T_7: & \mathbf{q}_f^{(1)}[1] & = (1\ 0\ 0\ 0\ 1\ 1 & 9 & 16) & \text{Fault-free} \\
T_1: & \mathbf{q}_f^{(1)}[2] & = (0\ 1\ 0\ 0\ 0\ 0 & 3 & 10) & \text{Fault-free} \\
T_2: & \mathbf{q}_f^{(1)}[3] & = (0\ 1\ 1\ 0\ 0\ 0 & 33 & 62) & \text{Pre-condition at } T_2 \\
T_3: & \mathbf{q}_f^{(1)}[4] & = (0\ 1\ 0\ 3\ 0\ 1 & 29 & 62) & P_4 \text{ corrupted by } +2 \\
T_4: & \mathbf{q}_f^{(1)}[5] & = (0\ 1\ 0\ 2\ 0\ 1 & -17 & 6) & \text{Post-condition at } T_4 \\
T_9: & \mathbf{q}_f^{(1)}[6] & = (0\ 1\ 0\ 2\ 0\ 1 & -17 & 6) & \text{Fault-free} \\
T_{10}: & \mathbf{q}_f^{(1)}[7] & = (0\ 1\ 0\ 2\ 0\ 1 & -17 & 6) & \text{Pre-condition at } T_{10} \\
T_{11}: & \mathbf{q}_f^{(1)}[8] & = (0\ 1\ 0\ 2\ 0\ 1 & -17 & 6) & \text{Fault-free} \\
T_8: & \mathbf{q}_f^{(1)}[9] & = (0\ 1\ 0\ 2\ 0\ 1 & -17 & 6) & \text{Fault-free} \\
T_5: & \mathbf{q}_f^{(1)}[10] & = (0\ 1\ 0\ 2\ 0\ 1 & -17 & 6) & \text{Fault-free} \\
T_6: & \mathbf{q}_f^{(1)}[11] & = (0\ 1\ 0\ 2\ 0\ 0 & -19 & -1) & \text{Fault-free} \\
T_7: & \mathbf{q}_f^{(1)}[12] & = (0\ 1\ 0\ 2\ 0\ 0 & -19 & -1) & \text{Post-condition at } T_7
\end{array}
$$

Distributed Fault Identification

- Place fault syndrome:

$$\mathbf{s}^{(1)}[12] = [-\mathbf{C}^{(1)*} \;\; \mathbf{I}_2]\, \mathbf{q}_f^{(1)}[12] = \begin{pmatrix} -26 \\ -13 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 9 \end{pmatrix}$$

- Parity check calculation:

$$\underbrace{\begin{pmatrix} 9 & 7 \\ 4 & 5 \end{pmatrix}}_{\boldsymbol{\Phi}} \begin{pmatrix} 7 \\ 9 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 7 \end{pmatrix} \equiv \underbrace{\begin{pmatrix} 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 \\ 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 \end{pmatrix}}_{\tilde{\mathbf{H}}} \mathbf{e}_P^{(1)}$$

- Place fault indicator vector: $\mathbf{e}_P^{(1)} = [0 \; 0 \; 0 \; 2 \; 0 \; 0]^T$

- Transition fault syndrome:

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 9 & 5 \end{pmatrix}}_{\mathbf{D}} \mathbf{e}_T^{(1)} = -(\mathbf{s}^{(1)}[12] - \mathbf{P}^{(1)*}\mathbf{e}_P^{(1)})/11 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

- Transition fault indicator vector: $\mathbf{e}_T^{(1)} = [0 \;\; -1 \; 0 \; 1]^T$

CONCLUSIONS

- With $2k$ redundant places, we achieve *simultaneous* identification

  (i) Up to $2k-1$ transition faults *and*

  (ii) Up to k place faults

- Easy implementation and low computational complexity

- Extension to distributed settings with enhanced capability

SEQUENCE OF EVENTS AND FAULTS

$$
\begin{array}{llllll}
 & \mathbf{q}_f^{(0)}[1] & = (1\ 0\ 0\ 0\ 0\ 0 & 200+4 & 200+1) & \text{Fault-free} \\
T_7: & \mathbf{q}_f^{(1)}[1] & = (1\ 0\ 0\ 0\ 1\ 1 & 200+9 & 200+16) & \text{Fault-free} \\
T_1: & \mathbf{q}_f^{(1)}[2] & = (0\ 1\ 0\ 0\ 0\ 0 & 200+3 & 200+10) & \text{Fault-free} \\
T_2: & \mathbf{q}_f^{(1)}[3] & = (0\ 1\ 1\ 0\ 0\ 0 & 200+33 & 200+62) & \text{Pre-condition at } T_2 \\
T_3: & \mathbf{q}_f^{(1)}[4] & = (0\ 1\ 0\ 3\ 0\ 1 & 200+29 & 200+62) & P_4 \text{ corrupted by } +2 \\
T_4: & \mathbf{q}_f^{(1)}[5] & = (0\ 1\ 0\ 2\ 0\ 1 & 200-17 & 200+6) & \text{Post-condition at } T_4 \\
T_9: & \mathbf{q}_f^{(1)}[6] & = (0\ 1\ 0\ 2\ 0\ 1 & 200-17 & 200+6) & \text{Fault-free} \\
T_{10}: & \mathbf{q}_f^{(1)}[7] & = (0\ 1\ 0\ 2\ 0\ 1 & 200-17 & 200+6) & \text{Pre-condition at } T_{10} \\
T_{11}: & \mathbf{q}_f^{(1)}[8] & = (0\ 1\ 0\ 2\ 0\ 1 & 200-17 & 200+6) & \text{Fault-free} \\
T_8: & \mathbf{q}_f^{(1)}[9] & = (0\ 1\ 0\ 2\ 0\ 1 & 200-17 & 200+6) & \text{Fault-free} \\
T_5: & \mathbf{q}_f^{(1)}[10] & = (0\ 1\ 0\ 2\ 0\ 1 & 200-17 & 200+6) & \text{Fault-free} \\
T_6: & \mathbf{q}_f^{(1)}[11] & = (0\ 1\ 0\ 2\ 0\ 0 & 200-19 & 200-1) & \text{Fault-free} \\
T_7: & \mathbf{q}_f^{(1)}[12] & = (0\ 1\ 0\ 2\ 0\ 0 & 200-19 & 200-1) & \text{Post-condition at } T_7
\end{array}
$$