Non-Concurrent Error Detection and Correction in Switched Linear Controllers

Shreyas Sundaram and Christoforos N. Hadjicostis

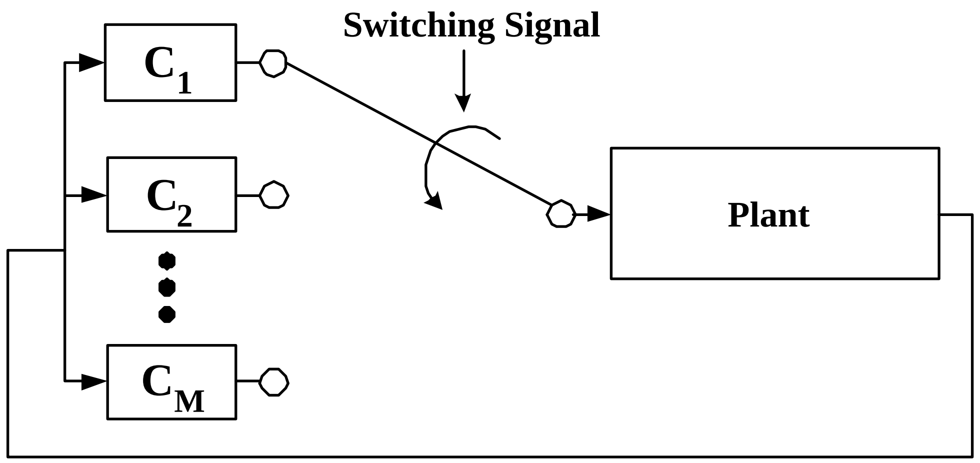
Coordinated Science Laboratory

and

Department of Electrical and Computer Engineering

University of Illinois at Urbana-Champaign

Switched Control



- Better handling of modelling uncertainty
- Stabilizes systems that cannot be stabilized otherwise

Fault Tolerance

Fault tolerance describes ability to:

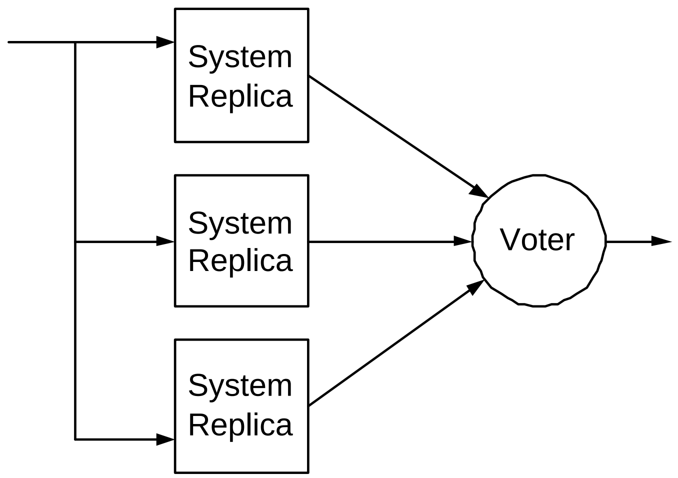
- Withstand internal faults
- Produce overall desirable “behavior”

Necessary or desirable in:

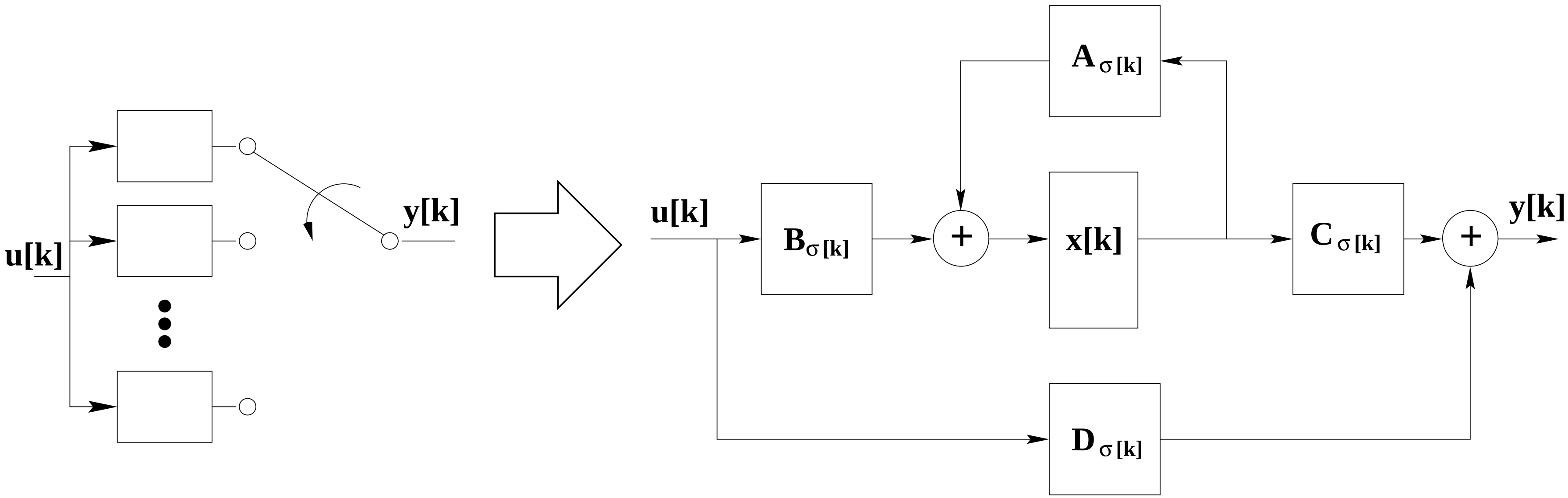
- Life-threatening circumstances (military, transportation, medical)
- Systems in inaccessible environments (space missions)
- Reliable systems from unreliable components (faster, less expensive, less power)

Universal approach: Modular Redundancy

- Problems:
  - Replication
  - Voter reliability



Fault Detection and Correction in Switched Controllers (1)



- Switched linear controller given by:

$$\mathcal{S}: \quad x[k+1] = \mathbf{A}_{\sigma[k]} x[k] + \mathbf{B}_{\sigma[k]} u[k] \ , \quad x[k] \in \mathbb{R}^n$$

- Goal: Detect and correct transient state-transition faults

Fault Detection and Correction in Switched Controllers (2)

- Embed $\mathcal{S}$ in a redundant system of dimension $\eta = n + d$:

$$\mathcal{H}: \quad x_h[k+1] = \mathcal{A}_{\sigma[k]} x_h[k] + \mathcal{B}_{\sigma[k]} u[k] \ , \quad x_h[k] \in \mathbb{R}^\eta$$

- Enforce linear encoding and decoding:

$$x[k] = \mathbf{L} x_h[k]$$
$$x_h[k] = \mathbf{G} x[k]$$

- Fault detection: Choose parity check matrix $\mathbf{P}$ such that:
  - If there is no error, $\mathbf{P} x_h[k] = 0$
  - If $x_h[k]$ is not in the column space of $\mathbf{G}$, $\mathbf{P} x_h[k] \neq 0$

Characterization of Redundant Controller Implementations

$$\mathcal{S}: \quad x[k+1] = \mathbf{A}_{\sigma[k]} x[k] + \mathbf{B}_{\sigma[k]} u[k] \ , \quad x[k] \in \mathbb{R}^n$$

$$\mathcal{H}: \quad x_h[k+1] = \mathcal{A}_{\sigma[k]} x_h[k] + \mathcal{B}_{\sigma[k]} u[k] \ , \quad x_h[k] \in \mathbb{R}^\eta$$

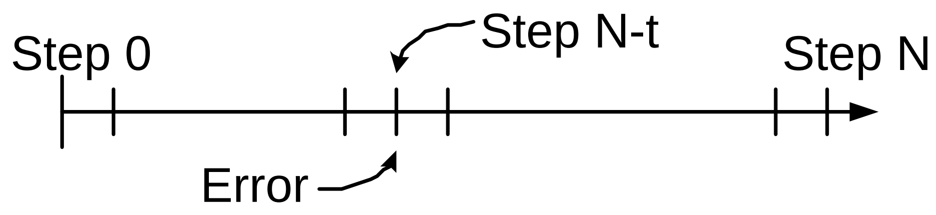
- $\mathcal{H}$ is a redundant implementation of $\mathcal{S}$ iff $\mathcal{H}$ is similar to the following standard form:

$$x_r[k+1] = \underbrace{\begin{bmatrix} \mathbf{A}_{\sigma[k]} & \mathbf{A}_{12_{\sigma[k]}} \\ \mathbf{0} & \mathbf{A}_{22_{\sigma[k]}} \end{bmatrix}}_{\mathcal{A}_{r_{\sigma[k]}} = \mathcal{T}^{-1} \mathcal{A}_{\sigma[k]} \mathcal{T}} x_r[k] + \underbrace{\begin{bmatrix} \mathbf{B}_{\sigma[k]} \\ \mathbf{0} \end{bmatrix}}_{\mathcal{B}_{r_{\sigma[k]}} = \mathcal{T}^{-1} \mathcal{B}_{\sigma[k]}} u[k]$$

$$\mathbf{P}\mathcal{T} = \begin{bmatrix} \mathbf{0} & \mathbf{I}_d \end{bmatrix} \equiv \mathbf{P}_r$$

for some sets of matrices $\mathbf{A}_{12_{\sigma[k]}}$ and $\mathbf{A}_{22_{\sigma[k]}}$, and some invertible $\mathcal{T}$.

Non-Concurrent Detection and Identification (1)



- Motivation: relax checking requirements (e.g., periodic checking)
- Design redundant implementation so that parity check at time N allows detection and identification of errors in $[0, N-1]$
- For each error (j), need to identify:
  - affected state variable (e_{i_j})
  - value of error (v_j)
  - time-step ($N - t_j$)

Non-Concurrent Detection and Identification (2)

- Additive error model: fault at time-step $N-t$ causes

$$x_f[N-t] = \underbrace{x_h[N-t]}_{\text{fault-free}} + ve_i$$

- With D errors, faulty state at step N given by

$$x_f[N] = x_h[N] + \sum_{j=1}^{D} \left\{ v_j \left(\prod_{i=N-t_j}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_{i_j} \right\}$$

- Parity check at step N yields

$$\mathbf{s}[N] \equiv \mathbf{P} x_f[N] = \sum_{j=1}^{D} \left\{ v_j \mathbf{P} \left(\prod_{i=N-t_j}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_{i_j} \right\}$$

Non-Concurrent Detection and Identification (3)

Theorem

- If $\mathcal{H}$ is a redundant implementation of $\mathcal{S}$, syndrome $\mathbf{s}[N]$ can be expressed as

$$\mathbf{s}[N] = \sum_{j=1}^{D} \left\{ v_j \left(\prod_{i=N-t_j}^{N-1} \mathbf{A}_{22_{\sigma[i]}} \right) \mathbf{P} e_{i_j} \right\}$$

- If all $\mathbf{A}_{22_{\sigma[k]}} = \mathbf{A}_{22}$, syndrome is independent of switching sequence

$$\mathbf{s}[N] = \sum_{j=1}^{D} \left\{ v_j \mathbf{A}_{22}^{t_j} \mathbf{P} e_{i_j} \right\}$$

Syndrome Generation

Syndrome $\mathbf{s}[N]$ is a linear combination of D columns of

$$\mathbf{S} = \begin{bmatrix} \mathbf{P} & \mathbf{A}_{22}\mathbf{P} & \mathbf{A}_{22}^{2}\mathbf{P} & \cdots & \mathbf{A}_{22}^{N-1}\mathbf{P} \end{bmatrix}$$

- To detect D errors, need all sets of D columns of $\mathbf{S}$ to be linearly independent
  - Require at least D extra state variables
- To identify D errors, need all sets of $2D$ columns of $\mathbf{S}$ to be linearly independent
  - Require at least $2D$ extra state variables

Construction of a Redundant Implementation (1)

- Fact: Any $2D$ columns of $\mathbf{V}$ are linearly independent iff w_i's are distinct.

$$\mathbf{V}(w_1, w_2, \ldots, w_\rho) = \begin{bmatrix} w_1 & w_2 & \ldots & w_\rho \\ w_1^2 & w_2^2 & \ldots & w_\rho^2 \\ \vdots & \vdots & \ddots & \vdots \\ w_1^{2D} & w_2^{2D} & \ldots & w_\rho^{2D} \end{bmatrix}$$

- Basic idea: Make **S** look like a Vandermonde matrix

$$\mathbf{S} = \begin{bmatrix} \mathbf{P} & \mathbf{A}_{22}\mathbf{P} & \mathbf{A}_{22}^2\mathbf{P} & \cdots & \mathbf{A}_{22}^{N-1}\mathbf{P} \end{bmatrix}$$

- Define $\Lambda = \mathrm{diag}(w, w^2, w^3, \ldots, w^{2D-1}, w^{2D})$
  - $\Lambda^k \mathbf{V}(w_1, w_2, \ldots, w_\rho)$ is also a Vandermonde matrix

Construction of a Redundant Implementation (2)

- Construction:
  - $2D$ additional state variables ($d = 2D$)
  - Select appropriate parameters $w, w_1, w_2, \ldots, w_{n+d}$
  - $\Lambda = \mathrm{diag}(w, w^2, w^3, \ldots, w^{2D-1}, w^{2D})$, $\mathbf{M} = \mathbf{V}(w_{n+1}, w_{n+2}, \ldots, w_{n+d})$
  - In standard implementation, set $\mathbf{A}_{22} = \mathbf{M}^{-1}\Lambda\mathbf{M}$, $\mathbf{A}_{12_{\sigma[k]}} = 0$
  - For similarity transformation, use $\mathcal{T} = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{C} & \mathbf{I}_{2D} \end{bmatrix}$ where

$$\mathbf{C} = -\mathbf{M}^{-1}\mathbf{V}(w_1, w_2, \ldots, w_n)$$

- Theorem: Resulting implementation allows non-concurrent identification of D errors (detection of $2D$ errors)
- Efficient decoding of errors
  - Modified Peterson-Gorenstein-Zierler (PGZ) algorithm

Example (1)

- Switched system: $x[k+1] = \mathbf{A}_{\sigma[k]}x[k] + \mathbf{B}_{\sigma[k]}u[k], \ \ \sigma[k] \in \{1, 2\}$

$$\mathbf{A}_1 = \begin{bmatrix} -1/2 & 1 & 0 \\ 1/4 & 0 & 1 \\ 1/5 & 0 & 0 \end{bmatrix}, \quad \mathbf{B}_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix};$$

$$\mathbf{A}_2 = \begin{bmatrix} -1/5 & 1 & 0 \\ 1/3 & 0 & 1 \\ 1/9 & 0 & 0 \end{bmatrix}, \quad \mathbf{B}_2 = \begin{bmatrix} 1.5 \\ 1 \\ 0 \end{bmatrix}.$$

- Goal: Protect against two errors in $[0, 4] \Rightarrow$ use 4 additional state variables
- Choose $\{w_1, w_2, w_3, w_4, w_5, w_6, w_7, w\} = \{-1, 1, -3, 3, -5, 5, 7, \frac{1}{2}\}$

Example (2)

- Construct required matrices

$$\mathbf{M} = \mathbf{V}(w_4, w_5, w_6, w_7)$$

$$\begin{bmatrix} 3 & -5 & 5 & -7 \\ 9 & 25 & 25 & 49 \\ 27 & -125 & 125 & -343 \\ 81 & 625 & 625 & 2401 \end{bmatrix}$$

$$\Lambda = \mathrm{diag}(w, w^2, w^3, w^4)$$

$$\begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 1/4 & 0 & 0 \\ 0 & 0 & 1/8 & 0 \\ 0 & 0 & 0 & 1/16 \end{bmatrix}$$

$$\mathbf{C} = -\mathbf{M}^{-1}\mathbf{V}(w_1, w_2, w_3)$$

$$\begin{bmatrix} 0.300 & -0.400 & 0.400 \\ -0.180 & 0.080 & -0.720 \\ -0.080 & 0.080 & -0.120 \\ 0.057 & -0.029 & 0.171 \end{bmatrix}$$

$$\mathbf{A}_{22} = \mathbf{M}^{-1}\Lambda\mathbf{M}$$

$$\begin{bmatrix} 0.604 & -0.440 & 0.928 & -0.325 \\ -0.084 & 0.580 & -0.037 & 0.846 \\ -0.104 & 0.129 & -0.074 & 0.100 \\ 0.030 & -0.154 & 0.014 & -0.173 \end{bmatrix}$$

Example (3)

- Resulting fault-tolerant implementation:

$$x_h[k+1] = \left[\begin{array}{c|c} \mathbf{A}_{\sigma[k]} & \mathbf{0} \\ \hline \mathbf{C}\mathbf{A}_{\sigma[k]} - \mathbf{A}_{22}\mathbf{C} & \mathbf{A}_{22} \end{array}\right] x_h[k] + \left[\begin{array}{c} \mathbf{B}_{\sigma[k]} \\ \hline \mathbf{C}\mathbf{B}_{\sigma[k]} \end{array}\right] u[k]$$

$$\mathbf{P} = \left[\begin{array}{c|c} -\mathbf{C} & \mathbf{I}_{2D} \end{array}\right]$$

- Errors affect variable 2 at time step 2, and variable 6 at time step 4:

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 1.50 \\ 1.00 \\ 0 \\ 0.05 \\ -0.19 \\ -0.04 \\ 0.06 \end{bmatrix} \Rightarrow \begin{bmatrix} 1.25 \\ \circled{0.88} \\ 1.30 \\ 0.74 \\ -1.13 \\ -0.23 \\ 0.28 \end{bmatrix} \Rightarrow \begin{bmatrix} 2.12 \\ 2.72 \\ 0.14 \\ -0.30 \\ -0.29 \\ 0.01 \\ 0.08 \end{bmatrix} \Rightarrow \begin{bmatrix} 2.65 \\ 0.67 \\ 1.42 \\ 1.15 \\ -1.46 \\ \circled{0.56} \\ 0.38 \end{bmatrix}$$

Example (4)

- Compute syndrome

$$\mathbf{s}[4] = \mathbf{P}x_f[4] = \begin{bmatrix} 0.047 \\ -0.015 \\ 0.889 \\ 0.005 \end{bmatrix}$$

- Use PGZ to find the corresponding linear combination of 2 columns of

$$\mathbf{S} = \begin{bmatrix} \mathbf{P} & \mathbf{A}_{22}\mathbf{P} & \mathbf{A}_{22}^2\mathbf{P} & \mathbf{A}_{22}^3\mathbf{P} & \mathbf{A}_{22}^4\mathbf{P} \end{bmatrix}$$

  - $\mathbf{s}[4] = 0.9\mathbf{P}(:,6) + 0.5(\mathbf{A}_{22}^2\mathbf{P})(:,2)$

$\Rightarrow$ Error at time step 4 affected variable 6 by value 0.9, and error at time step 2 affected variable 2 by value 0.5

Summary

- Reflection of hardware faults through appropriate error models
- Systematic embedding of switched controllers into redundant systems
  - Completely characterizes non-concurrent fault identification
  - Construction of fault-tolerant system through use of Vandermonde matrices
- Future work:
  - Robustness to finite precision effects
  - Utilize flexibility in choice of $\mathbf{A}_{12_{\sigma[k]}}$
  - Investigate designs that minimize redundant arithmetic operations