BINGHAMTON UNIVERSITY
State University of New York

Supervisory Control of Safety Critical Systems

N. Eva Wu
ECE Dept., Binghamton University
Binghamton, NY 13902-6000
607-777-4375, evawu@binghamton.edu

BINGHAMTON UNIVERSITY
State University of New York

Outline and Objective

- **Outline**
  - **Objective**
  - **Definitions**
  - **Reliability analysis**
  - **Supervisory control**
  - **Example**
- **Objective**
  - **Investigate the impact of control on fault-tolerance**
    - **An alternative view of fault tolerant control: supervisory control of failure processes**

BINGHAMTON UNIVERSITY
State University of New York

Definitions

- A fault is an unpermitted deviation of at least one characteristic property or variable of the system
- A failure is a permanent interruption of a (sub)system's ability to perform a required function under specified conditions
- Reliability is the probability that a (sub)system will perform a required function for a given period of time when operated under stated operating conditions
- Reliability modeling for an *N* component system amounts to the determination of a structure mapping $\{0,1\}^N \rightarrow \{0,1\}$ where '1' means intact, and '0' means failed

BINGHAMTON UNIVERSITY
State University of New York

Definitions

- A Markov process is a stochastic process for which the probability that a system will undergo a transition from one state to another depends only on the current state
- A holding time of a Markov process is a r.v. that represents the time the process stays at a particular state
- A Markov reliability model is specified by the three tuple

$$(\mathcal{X}, p_x(0), \lambda_{x,x'})$$

- Supervisory control refers to the control of Markov process via transition rates, in particular,

$$c_{x',u}(t)\lambda_{x,x'}$$

- Coverage is the conditional probability that a system remains in operation given that a subsystem failure has occurred

BINGHAMTON UNIVERSITY
State University of New York

Definitions

- A fault parameter space is a Euclidean space of real parameters that change their values as the result of some fault or subsystem failure occurrence
- Closed-loop control performance under control law u

$$J_u(\theta) = \frac{1}{sup_{\|w\|_{in} \le 1} \left\| T_{wz}^{u}(\theta) w \right\|_{out}}$$

- A control performance threshold $J_{th}(\theta)$ that distinguishes a normal from s failed operation of a controlled system
- Diagnostic resolution

$$R_\kappa = \frac{1}{det(\kappa P)}, \varepsilon = \left\{ \theta \mid (\theta - \bar{\theta})' P^{-1} (\theta - \bar{\theta}) \le \kappa \right\}$$

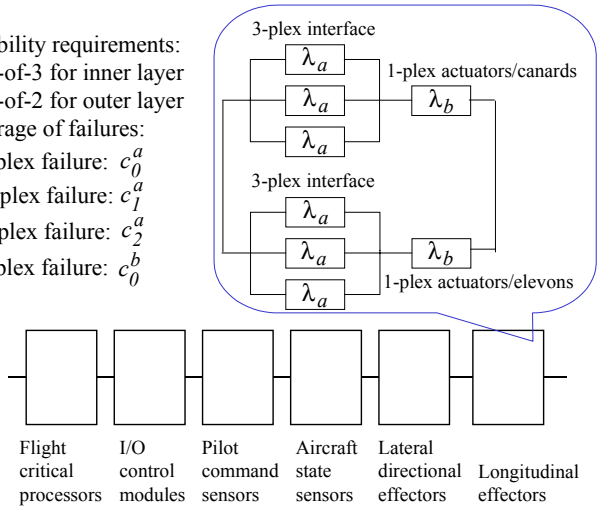
- A critical clearance time is the maximum period allowed between the occurrence of a fault or a subsystem failure and the establishment of a post-fault equilibrium which includes the departing trajectory from a pre-fault equilibrium in its ROA

BINGHAMTON UNIVERSITY
State University of New York

Reliability Analysis

- A reliability model for a flight control system

Reliability requirements:
1-out-of-3 for inner layer
1-out-of-2 for outer layer
Coverage of failures:
1st 3-plex failure: c_0^a
2nd 3-plex failure: c_1^a
3rd 3-plex failure: c_2^a
1st 1-plex failure: c_0^b



BINGHAMTON UNIVERSITY
State University of New York

Reliability Analysis

States and transition rates for a degradable 2-layer 3-

normal state	trans. rate	state w. 1 failure	trans. rate	state w. 2 failures	trans. rate	state w. 3 failures	trans. rate	state w. 4 failures
30103010	$3\lambda_a c_0^a$	21103010	$2\lambda_a c_1^a$	12103010	$\lambda_a c_2^a$	03103010	$3\lambda_a c_0^a$	03102110
							$3\lambda_a \bar{c}_0^a$	$03102110d$
							λ_b	$03103001d$
					$\lambda_a \bar{c}_2^a$	$03103010d$		
					$\lambda_b c_0^b$	12013010	$3\lambda_a c_0^a$	12012110
							$3\lambda_a \bar{c}_0^a$	$12012110d$
							λ_b	$12013001d$
					$\lambda_b \bar{c}_0^b$	$12013010d$		
			$2\lambda_a \bar{c}_1^a$	$12103010d$				
			$\lambda_b \bar{c}_0^b$	$21013010d$				
			$\lambda_b c_0^b$	21013010	$3\lambda_a c_0^a$	21012110	$2\lambda_a c_1^a$	21011210
							$2\lambda_a \bar{c}_1^a$	$21011210d$

BINGHAMTON UNIVERSITY
State University of New York

Reliability Analysis

- **Kolmogorov equation**

$$\dot{P} = PQ, P(0) = I$$

$$Q = \begin{bmatrix} q_{00} & q_{01} & 0 & 0 & 0 & 0 & q_{06} \\ 0 & q_{11} & q_{12} & 0 & 0 & 0 & q_{16} \\ 0 & 0 & q_{22} & q_{23} & 0 & 0 & q_{26} \\ 0 & 0 & 0 & q_{33} & q_{34} & 0 & q_{36} \\ 0 & 0 & 0 & 0 & q_{44} & q_{45} & q_{46} \\ 0 & 0 & 0 & 0 & 0 & q_{55} & q_{56} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

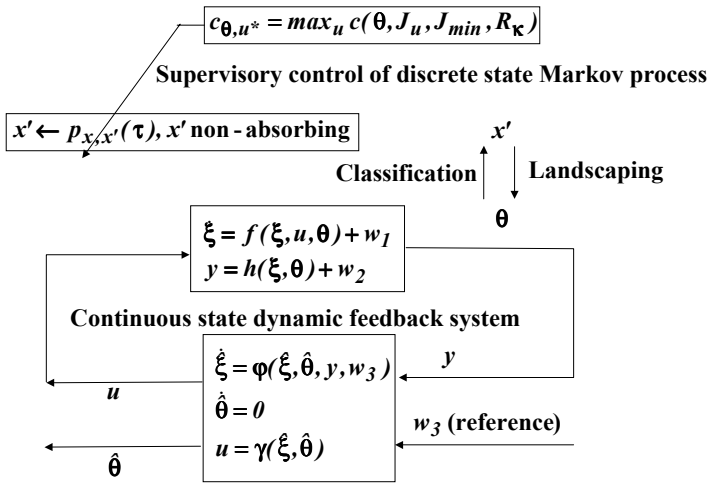
  - **Resort to numerical tools and approximations**
  - **An approximation and implication**

$$P_D(t) = 6\lambda_a(1 - c_0^a)t + 2\lambda_b(1 - c_0^b)t$$

BINGHAMTON UNIVERSITY
State University of New York

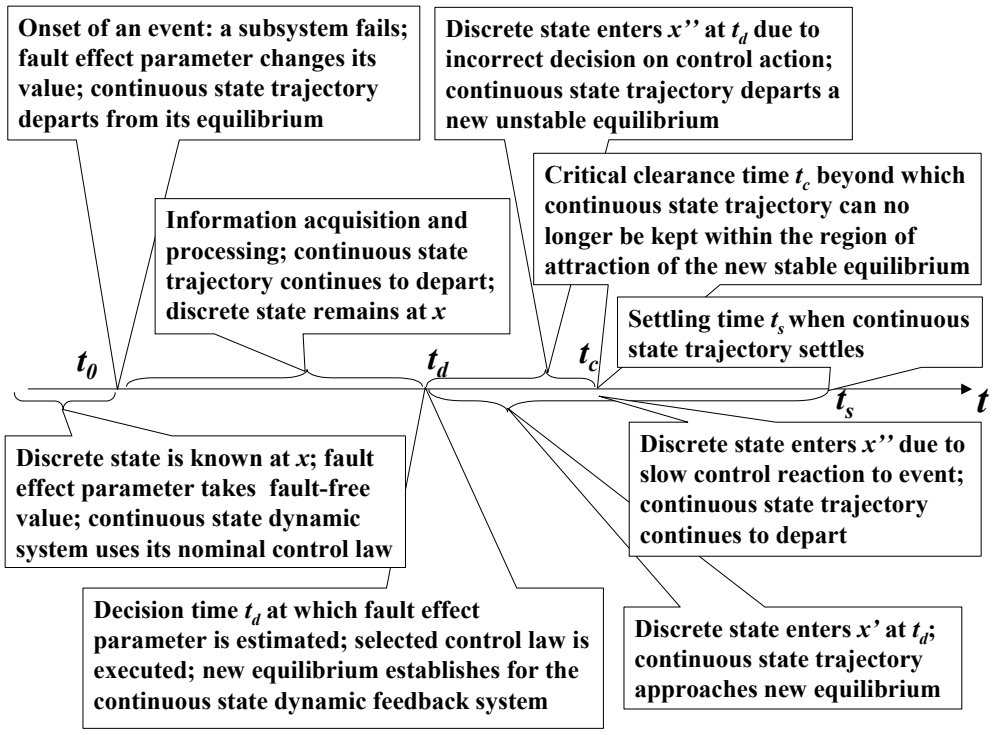
Supervisory Control

- **A two-level two-timescale model**



BINGHAMTON UNIVERSITY
State University of New York

Supervisory Control



BINGHAMTON UNIVERSITY
State University of New York

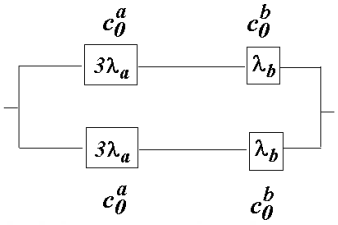
Supervisory Control

- **An optimal greedy policy**

$$max_u\, c_{\theta,u}(t_d), c_{\theta,u}(t_d) = \int_{\hat{\theta}\in\{\theta\in\Omega | J_u(\theta)\geq J_{th}(\theta)\}} f(\hat{\theta}, t_d \mid \theta) d\hat{\theta}$$

  - More robust control law leads to higher coverage
  - More stringent control requirement leads to lower coverage
  - Higher diagnostic resolution leads to higher coverage
- **The above policy minimizes system level failure probability**

An Example



- **HIMAT aircraft**
  - Focusing on controllable transitions
  - Landscaping and classification
  - Control performance
  - Diagnosis resolution
  - Coverage