The Markov/CCMT Methodology and Its Application to the Reliability Modeling of Digital Control Systems

Diego Mandelli, Jason Kirshenbaum, Paolo Bucci, Tunc Aldemir

The Ohio State University
Nuclear Engineering Program

Dynamic PRA/PSA Workshop – Annapolis 2007

Outline

1. Introduction
2. The Markov/CCMT methodology
   - Modeling of Type I interactions
   - Modeling of Type II interactions
   - Markov/CCMT analysis
3. Markov/CCMT methodology and the reliability modeling of digital I&C systems
4. Conclusion

The Markov/CCMT methodology

Methodology for the reliability modeling of systems which, due to their intrinsic nature, require dynamic tools.

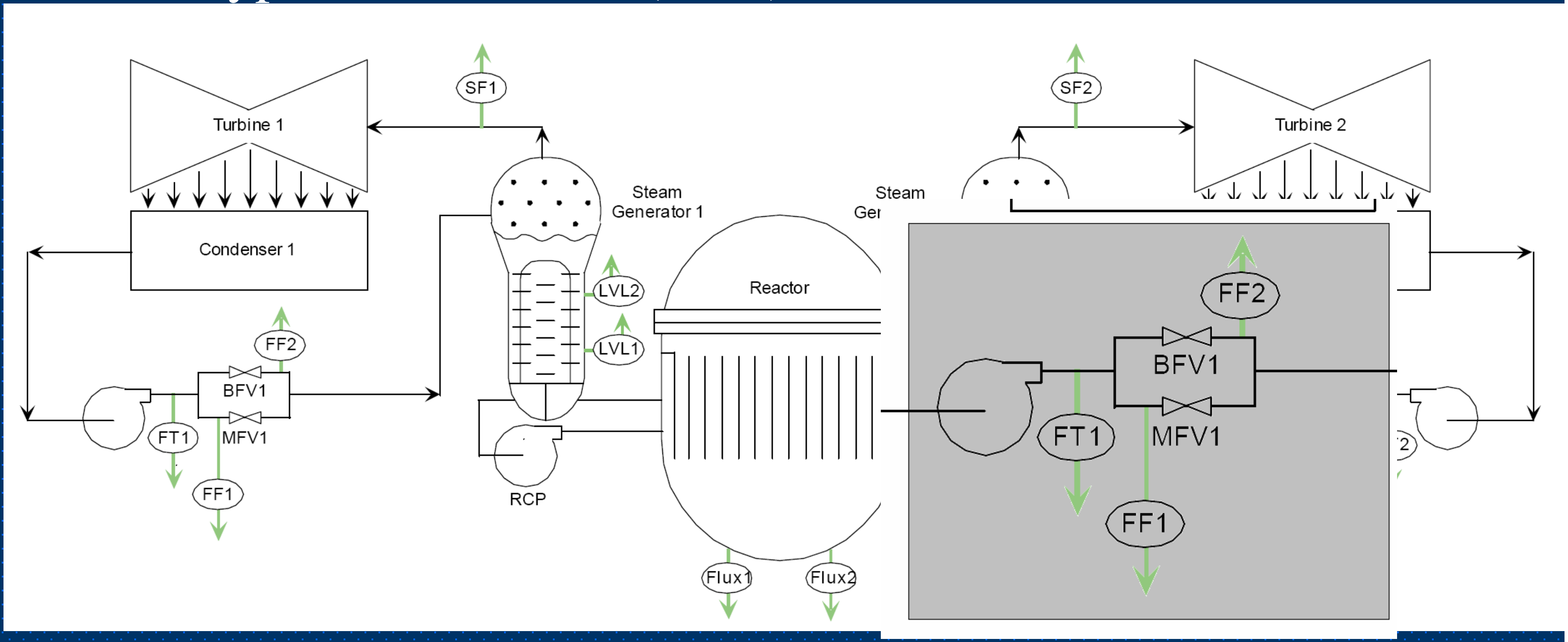
Stochastic description of the system evolution:

- Type I Interactions - Dynamic interactions between physical process variables (e.g., temperature, pressure, etc.) and the I&C systems that monitor and manage the process
- Type II Interactions - Dynamic interactions within the I&C system itself due to the presence of software/firmware (e.g., multi-tasking and multiplexing)

A reference case: PWR Feedwater System

Digital Feedwater Control System (DFWCS) Components:

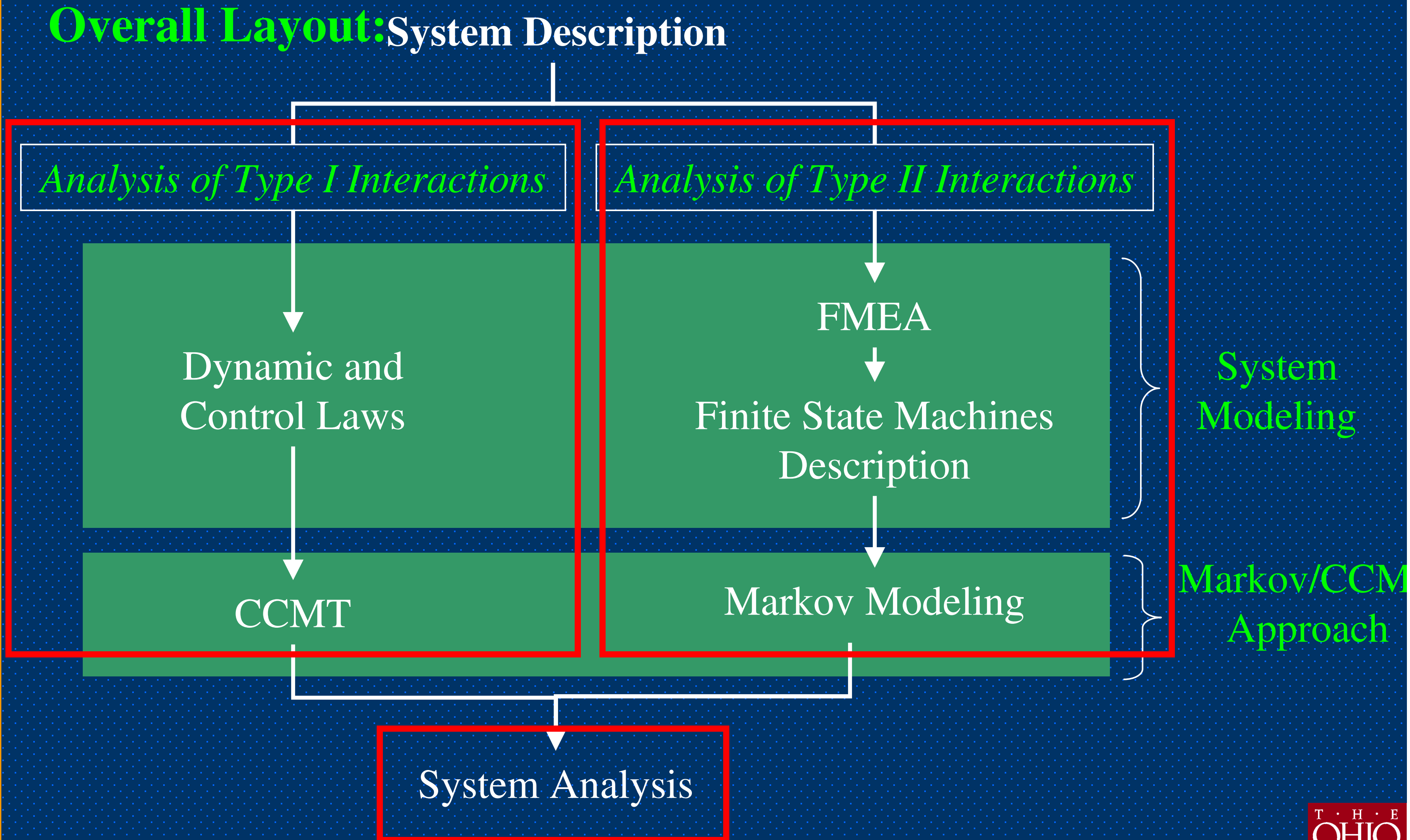
- ✓ Main Feedwater Valve (MFV)
- ✓ Bypass Flow Valve (BFV)



THE OHIO STATE UNIVERSITY

The Markov/CCMT methodology

Overall Layout:



THE OHIO STATE UNIVERSITY

The Markov/CCMT methodology

Two steps:
- System Modeling
- Markov/CCMT approach

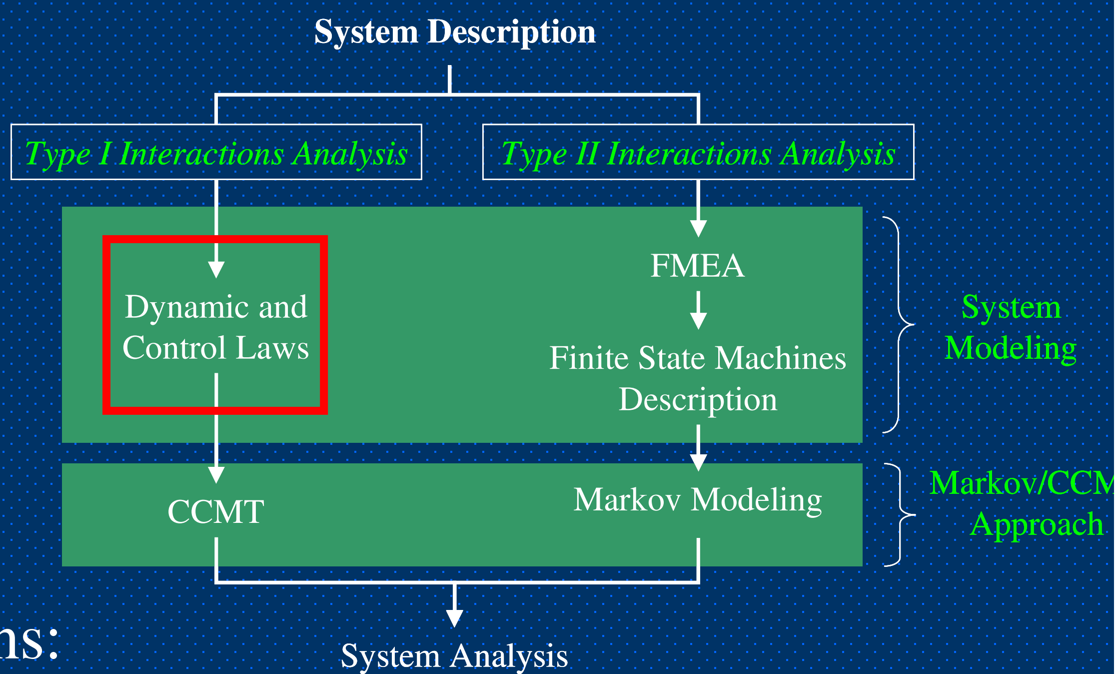
For each of these steps, the following are analyzed separately:

- Type I Interactions
- Type II Interactions

The system analysis merges the information for both Type I and II Interactions.

Modeling of Type I interactions

Dynamic and control laws

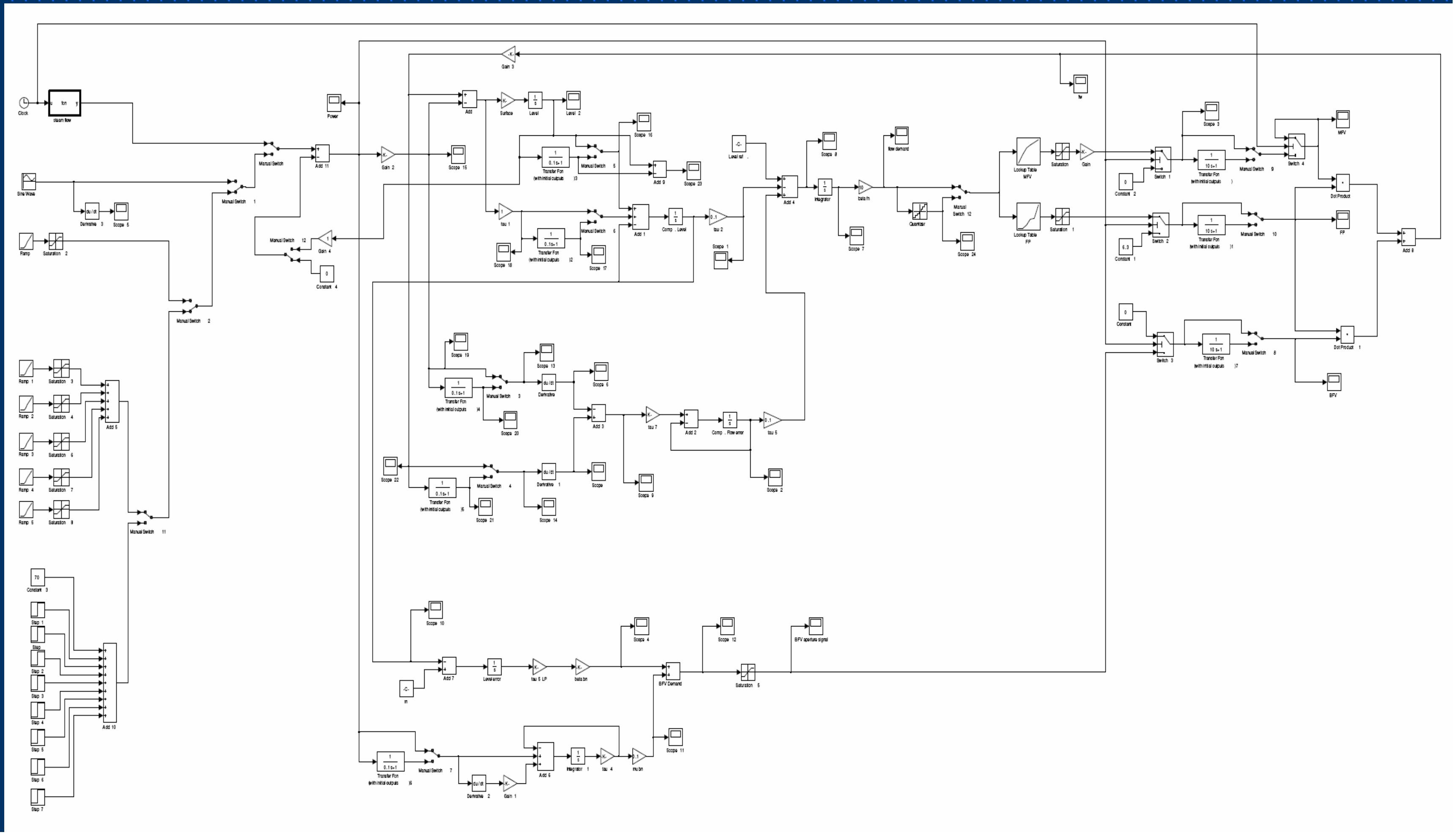


Possible implementations:

- Java/C/C++ (simple systems)
- Simulink models (more elaborate systems)

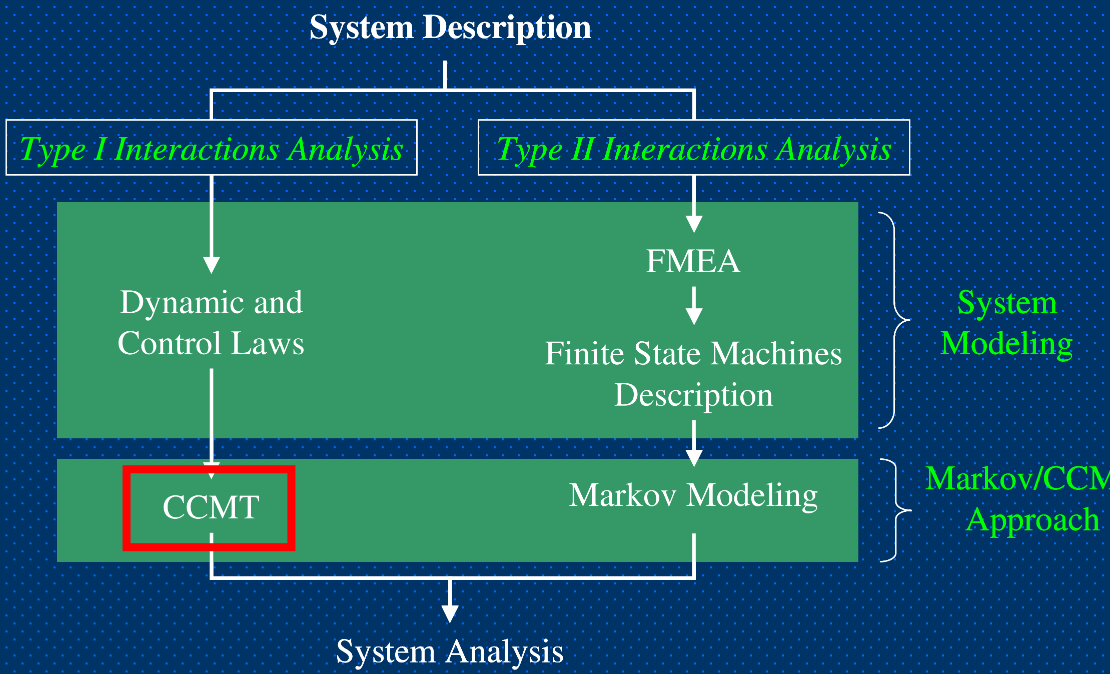
Type I interactions modeling

Simulink model of a Digital Feedwater Control System



Modeling of Type I Interactions

Cell-to-Cell Mapping Technique



Dynamics of the system described in terms of probability of transitions between process variable magnitude intervals (cells) that partition the state space (CVSS)

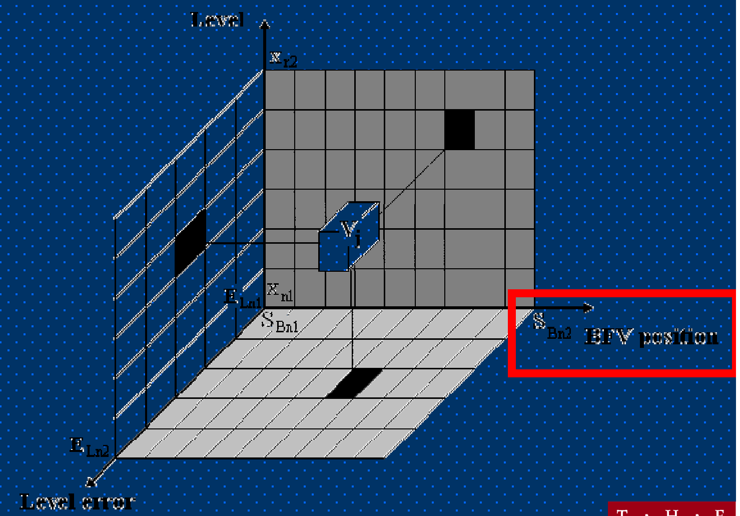
Modeling of Type I interactions

Cell-to-Cell Mapping Technique

- CVSS is divided into cells (Possibility to capture uncertainties and errors in the monitoring phase of the process)
- Through the set of dynamic and control laws it is possible to determine:

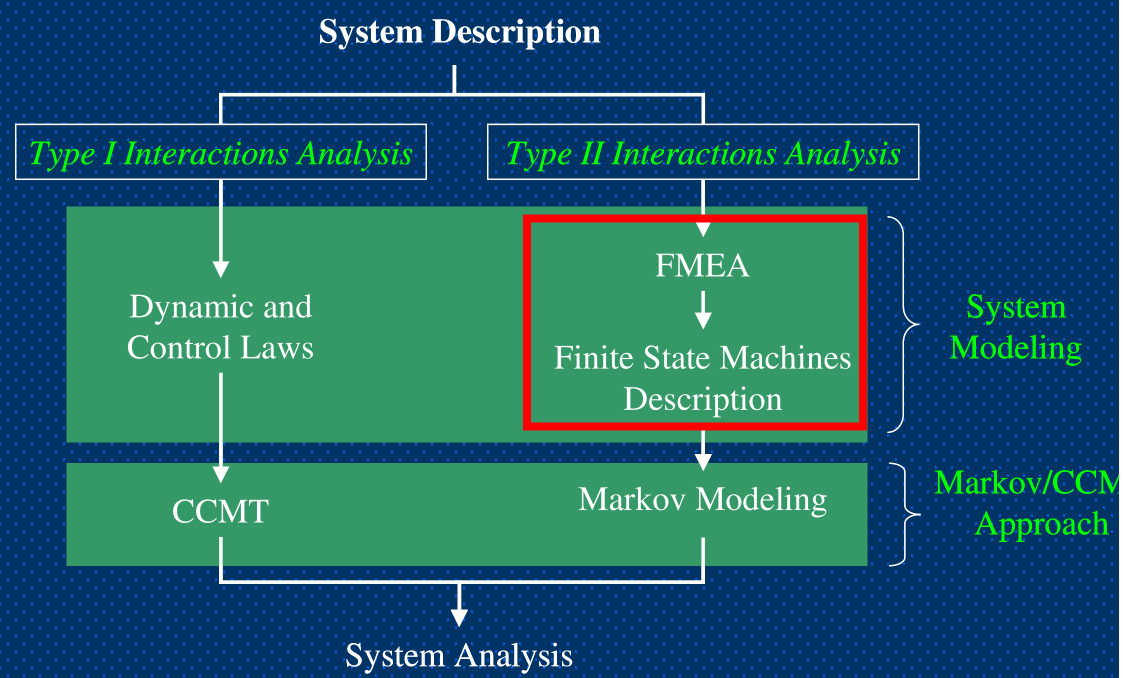
$$g(j|j',n',t)$$

Probability at time t to transit from cell j' to j given component state combination n'.



Modeling of Type II Interactions

Interaction among controllers components



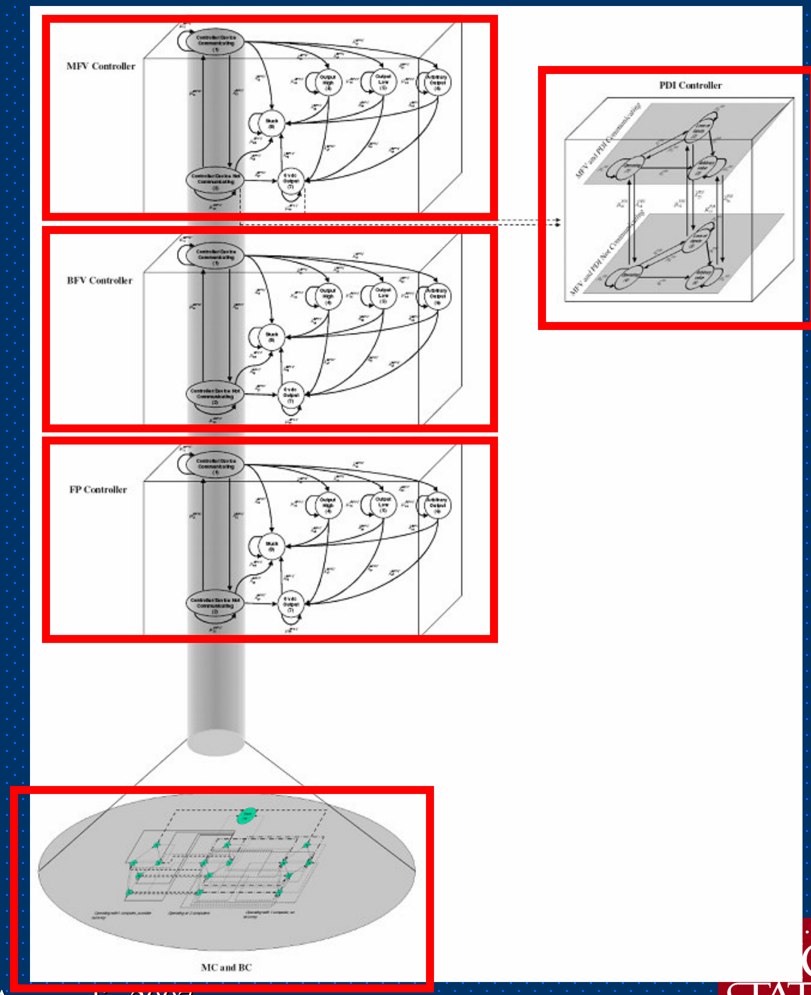
Two Steps:

- FMEA: Failure Modes and Effect Analysis
- Finite State Machine Description

Modeling of Type II Interactions

DFWCS Finite State Machine

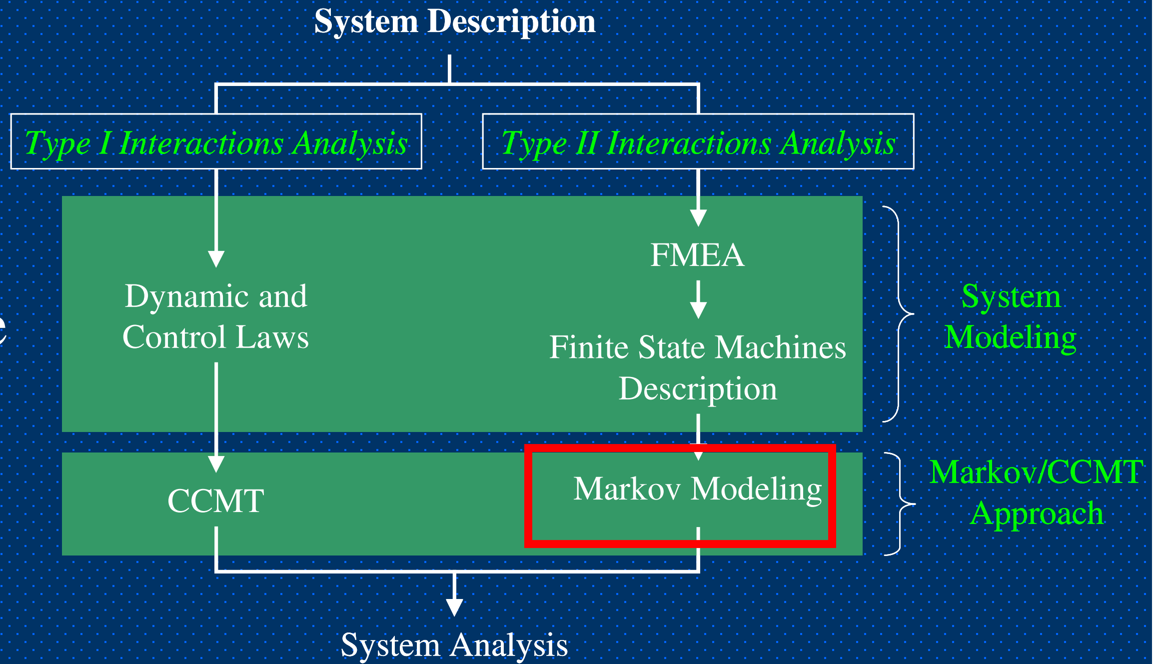
- MFV Controller
- BFV Controller
- FP Controller
- Main and Backup
- Computers
- PDI Controller



Modeling of Type II Interactions

Markov Modeling

- Markov Models deducted from the Finite State Machine description
- The goal is to determine:



$$h(n|n',j'\rightarrow j)$$

Probability that a component state combination change from n' to n during a transition from j to j'.

Modeling of Type II Interactions

Markov Modeling

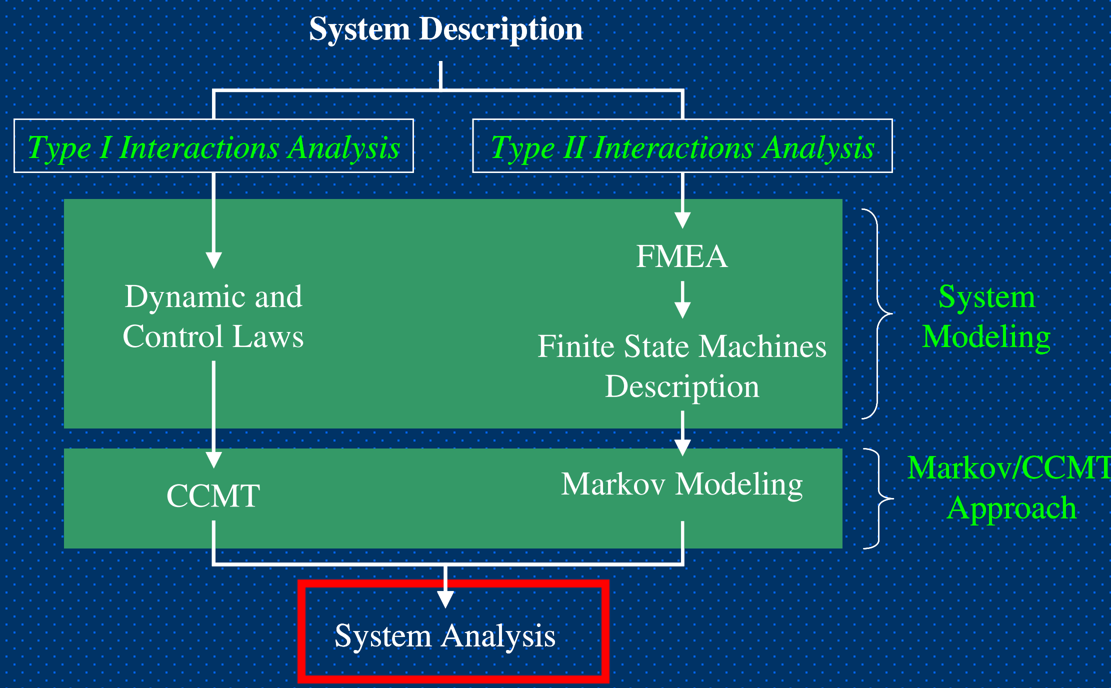
In general, $h(n|n',j'\rightarrow j)$ can depend on both:

- Time: failure rates may depend on time $\lambda = \lambda(t)$
- Process status: failure rates may depend on process variables like temperature, pressure….

System Analysis

System Analysis

- Markov: $h(n|n',j'\rightarrow j)$
- CCMT: $g(j|j',n',t)$



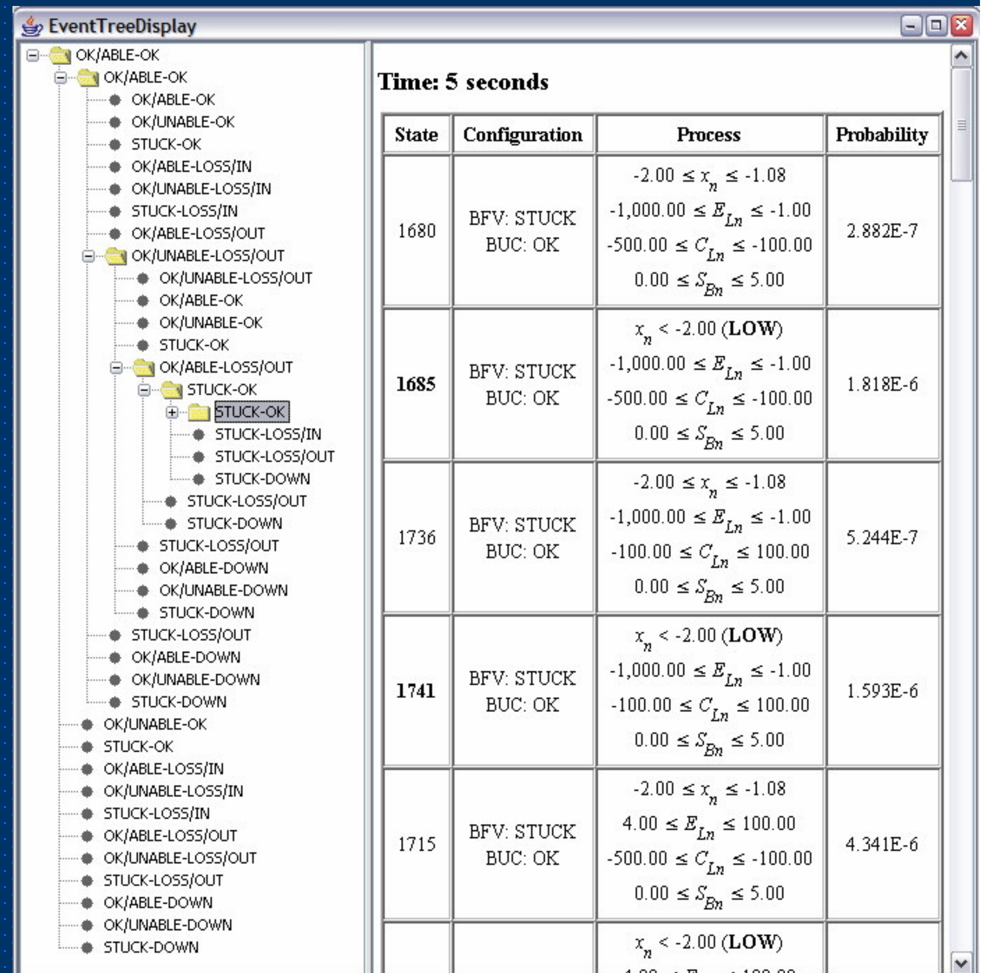
$$q(n, j|n', j',t) = h(n|n',j'\rightarrow j) \cdot g(j|j',n',t)$$

$$\boxed{p_{nj}(t+1)} = \boxed{\sum_{n'=1}^{N}\sum_{j'=1}^{J}}\boxed{q(n, j\,|\,n'\,j',t)}\boxed{p_{nj}(t)}$$

System Analysis

Local Analysis

- Event Trees are generated
- Trajectory of each point correspond to a single branch of the overall Event Tree (i.e. a possible scenario)
- Possibility to graphically visualize each scenario



System Analysis

Global Analysis

Time (in seconds) (Depth of DET)	Number of LOW failure scenarios	Number of HIGH failure scenarios	Number of scenarios without failure
1	0 (0.0%)	0 (0.0%)	243 (100.0%)
2	0 (0.0%)	0 (0.0%)	1,242 (100.0%)
3	530 (10.8%)	0 (0.0%)	4,384 (89.2%)
4	1,480 (9.3%)	0 (0.0%)	14,439 (90.7%)
5	4,999 (10.2%)	186 (0.4%)	43,727 (89.4%)
6	14,811 (10.2%)	2,518 (1.7%)	127,292 (88.0%)
7	47,881 (11.5%)	6,531 (1.6%)	362,153 (86.9%)
8	140,644 (11.9%)	18,559 (1.6%)	1,022,695 (86.5%)
9	411,240 (12.3%)	50,259 (1.5%)	2,871,468 (86.2%)
10	1,126,498 (12.0%)	143,922 (1.5%)	8,091,530 (86.4%)

Conclusion

- Markov/CCMT can be used to analyze elaborate communication systems
- Coupling between components can be take into account
- Possibility to couple Markov/CCMT with exiting PRAs
- Uncertainties in the monitoring and process modeling can be taken into account through cell definitions
- Uncertainty in the initial conditions can be accounted for