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 Markov/CCMT methodology

Overall Layout: System Description

Analysis of Type I Interactions
- Dynamic and Control Laws
  - CCMT

Analysis of Type II Interactions
- FMEA
  - Finite State Machines Description
  - Markov Modeling

System Analysis
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
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 \( n' \).
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
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 \( j' \).
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

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

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

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

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