DYNAMIC PRA/PSA - A HISTORICAL PERSPECTIVE

Tunc Aldemir
Nuclear Engineering Program
The Ohio State University
Presentation Organization

- Workshop motivation
- Objectives
- Previous workshops and some conclusions
- Available dynamic methodologies
- Recent application areas
- A benchmark system
Workshop Motivation

• Over the past few years, attention on dynamic probabilistic risk/safety assessment (PRA/PSA) methodologies has increased both in the U.S. and abroad.

• Recent applications have included assessments of digital instrumentation and control systems and Level 2 PRAs.

• As part of the Idaho National Laboratory National University Consortium an Academic Center of Excellence (ACE) has been established at The Ohio State University (OSU). The OSU ACE will be a focal point for research related to the development of safety-related instrumentation, advanced control systems, and PRA for advanced nuclear power plant systems.

• Dissemination of the information relevant to ACE activities and fostering collaboration among national laboratories, universities, U.S. government and international stakeholders on I&C&RS issues is part of the mission of the OSU ACE.
Workshop Objectives

• Foster common understanding of specific applications requiring dynamic PRA/PSA in nuclear and aerospace areas.

• Identify the issues and potential solutions for the practical implementation of dynamic PRA/PSA in these specific applications, including
  • modeling for dynamic reliability,
  • input data requirements for dynamic reliability models, and,
  • extraction, synthesis and interpretation of data and information resulting from dynamic reliability analyses.

• Identify areas of future cooperation.
Previous Workshops

• ESREL'97 Dynamic System Reliability Workshop, June 16, 1997, Lisbon, Portugal
• "Dynamic Reliability: Future Directions", University of Maryland International Workshop Series on Advanced Topics in Reliability and Risk Analysis, September 19-20, 1998, College Park, Maryland, and,
• ESREL 2001 Embedded Workshop on Dynamic PSA and Accident Management in Nuclear Power Plants, September 16-20, 2001, Turin, Italy
Some Conclusions of Previous Workshops

• Dynamic methodologies may be needed whenever there is hardware/software/firmware/process/human interaction

• Benchmark problems need to be specified to identify the system features and conditions that necessitate the use of dynamic methodologies, as well as to compare the capabilities of different dynamic methodologies

• User-friendly interfaces are needed to facilitate the use of dynamic methodologies
Available Dynamic Methodologies

- Continuous Time
  - CET (Continuous Event Tree)
  - CCCMT (Continuous Cell-to-Cell Mapping Technique)

- Discrete Time
  - MC (Monte Carlo)
  - DYLAM
  - DETAM
  - ADS
  - ISA
  - ADAPT
  - MCDET
  - CCMT (Cell-to-Cell Mapping Technique)
  - Dynamic Event Tree Generation

- Graphical
  - PETRI NETS
  - DYNAMIC FLOWGRAPHS
  - GO-FLOW
  - DYNAMIC FAULT TREES
  - EVENT SEQUENCE DIAGRAMS
Some Recent Need Areas

- Digital upgrade of nuclear plant instrumentation and control systems
- Constellation project
- Seamless Level 1-2-3 PRA for nuclear power plants
- Advanced reactor designs with passive safety features
Benchmark DFWCS for Digital I&C System Modeling
DFWCS: Operating Modes

1. Low power (< 15%)
   • BFV operating
   • MFV closed
   • FP at minimum speed
2. High power (15% -100%)
   • BFV closed
3. Automatic transfer from Low to High power mode
4. Automatic transfer from High to Low power mode
DFWCS SIMULINK Model

High Power Mode

Low Power Mode

Actuated Devices
SIMULINK Model Testing

Simulator Input

Power increasing (High Power Mode)
SIMULINK Model Testing

MFV Response

MFV aperture (Scale from 0 to 10)

Time [s]

8.84 8.88 8.92 8.96 9.00 9.04 9.08

0 50 100 150 200 250 300 350

30 32 34 36 38 40 42 44 46 48 50

Time [s]
SIMULINK Model Testing

FP Response
Hardware/Software/Firmware States: Computers

2: Operating with 1 computer, possible recovery
1: Operating with 2 computers
3: Operating with 1 computer, no recovery

Computer States
A: Operating
B: Loss of one input
C: Loss of both inputs
D: Computer down
E: Arbitrary output

Macro States
1: Controller is receiving data from both computers
2: Controller is receiving data from 1 computer while the other one can be recovered
3: Controller is receiving data from 1 computer while the other one can not be recovered
Freeze: Controller sends the same data to the valves from the previous time step

<table>
<thead>
<tr>
<th>Primary goes down (recoverable)</th>
<th>Primary Release control of the process</th>
<th>Secondary computer watchdog timer trips or loss of output to controller</th>
<th>Common cause sensor failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary recovers</td>
<td>Primary computer watchdog timer trips or loss of output to controller</td>
<td>Primary goes down. Secondary unavailable</td>
<td></td>
</tr>
</tbody>
</table>
Hardware/Software/Firmware States:

Controllers
Hardware/Software/Firmware States:

Summary

- 5 Pairs of sensors, 2 Computers (MC, BC), MFV Controller, BFV Controller, FP Controller, PDI Controller
- Total of 100,018,800 states
- Reduces to 46,080 states by conglomeration into super components
  - Sensors -> MC
  - Sensors -> BC
  - Actuated device (valve, pump) -> controller
  - MC+BC -> Computer
- Reduces to 2250 states by merging states with similar effects on the controlled process (e.g., system is operational whether there is 1 or 2 computers)
Conclusion

• The need for dynamic methodologies seem to be more widely accepted in the PRA/PSA community
• A number of methodologies are available targeting specific applications
• The system features that may necessitate their use need to be identified
• Computational resource requirements and skill levels needed for their implementation still pose challenges
• There is need for better collaboration among different institutions sponsoring work in dynamic methodology development