DEVELOPMENT OF INTEGRATED SITE RISK USING THE MULTI-UNIT DYNAMIC PROBABILISTIC RISK ASSESSMENT (MU-DPRA) METHODOLOGY

Matt Dennis
Mohammad Modarres
Ali Mosleh

PSA 2017
Pittsburgh, PA

September 24-28, 2017
Outline

• Motivation and objective
• Multi-Unit Dynamic PRA (MU-DPRA) methodology
• Hardware reliability analysis
• Simulation tool development
Motivations

• Technological gaps
  – Current PRAs rely on iterative processes between system engineers, thermal-hydraulic specialists, and PRA practitioners
  – Accident sequence progression modeling (human performance, thermal-hydraulics, core damage phenomena, hardware reliability, etc.) remain fragmented in PRAs

• Needed advances post-Fukushima
  – IAEA Action Plan on Nuclear Safety recommended to “improve analytical modelling capabilities and further develop tools for assessment of multi-unit sites. . . ” [IAEA, 2012]
  – The 2011 earthquake and tsunami at Fukushima underlined multi-unit nuclear power plant risk and the need for extrapolating the results from a single unit nuclear power plant safety assessment [IAEA, 2013]
Purpose

- Multi-unit (or multi-module) PRA not formally considered [Fleming, 2003; Fleming, 2005; Hakata, 2007]
- Risk metrics (CDF and LERF) don’t fully capture site risks
- Nuclear reactor regulation based on single-unit safety goals [U.S. NRC, 2013, 2011; Muramatsu, 2008]

Need to develop simulation technology and methods to analyze multi-unit nuclear reactor accidents factoring in human actions, system dependencies and feedback
Objective

- Develop multi-unit dynamic PRA (MU-DPRA) framework
- Enhance the current simulation tools for MU-DPRA
- Establish a framework for system dependency classification and assessment of relative site risk
- Apply the MU-DPRA framework and tools to a multi-module concept
Probabilistic Estimation of Dependencies

- Assume events $CD_1,\ldots,CD_n$ represent random variables describing the “events of a core damage” in units 1 to n.
- Site CDF as summation of individual unit $CD_i$’s: Expressed as either:
  - marginal CDF for all conditions in the other unit(s)
  - conditional CDF of a unit, given a condition in other unit(s)
Multi-Unit Analysis Methodology

1. Classify dependencies
   • initiating events, shared connections, identical components, proximity dependencies, human dependencies, and organizational dependencies [Schroer and Modarres, 2013]

2. Develop dependency matrix

3. Rank base static PRA accident sequences

4. Identify dependencies associated with risk significant systems

5. Develop T-H model of reactor system

6. Develop probabilistic physics-of-failure model for safety system components affected by environmental factors

7. Develop ADS-IDAC simulation input that includes multi-unit model

8. Develop algorithms to avoid computational explosion by pruning dynamic scenarios via probability truncation, event time, or end state condition

9. Assess relative risk of MU-DPRA accident sequences
Expansion of static PRA accident sequences

**STATIC**
- Decay heat removal system
- Emergency core cooling system

**DYNAMIC**
- Environment

**MULTI-UNIT**
- Other Units/Modules

Time: $t = 0$
### Base PRA Usage – System Identification

#### Dedicated and Shared Systems

<table>
<thead>
<tr>
<th>Dedicated Single-Unit Structure, Systems and Components</th>
<th>Shared Multi-Unit Structures, Systems and Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety DC Electrical and Essential AC Distribution System</td>
<td>Cooling towers, pond or other ultimate heat sink</td>
</tr>
<tr>
<td>Reactor Building or Bay</td>
<td>Turbine-Generator Building</td>
</tr>
<tr>
<td>Pressure/Containment Vessel</td>
<td>Reactor Building</td>
</tr>
<tr>
<td>Decay Heat Removal System</td>
<td>Control Room</td>
</tr>
<tr>
<td>Emergency Core Cooling System</td>
<td>Spent Fuel Pool</td>
</tr>
<tr>
<td>Non-safety Control and Instrumentation System</td>
<td>Site Cooling Water System</td>
</tr>
<tr>
<td>Chemical Volume and Control System</td>
<td></td>
</tr>
</tbody>
</table>

**Dedicated Single-Unit**
- Structure, Systems, and Components

**Shared Multi-Unit**
- Structures, Systems, and Components
## Dependency Classification Matrix

<table>
<thead>
<tr>
<th>Accident Sequence Classifications</th>
<th>Definition</th>
<th>Potential Systems Belonging to Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiating Events</strong></td>
<td>Single events that have the capacity to affect multiple units</td>
<td>Loss of Offsite Power, Loss of Ultimate Heat Sink, seismic event (including seismically-induced tsunami), external fire, external flood, hurricane, high wind, extreme temperature</td>
</tr>
<tr>
<td><strong>Shared Connections</strong></td>
<td>Links that physically connect SSCs of multiple units</td>
<td>Reactor pool, chilled water system, BOP water system, spent fuel pool cooling system, circulating water system, reactor component cooling water system, high, medium and low voltage AC distribution systems</td>
</tr>
<tr>
<td><strong>Identical Components</strong></td>
<td>Components with same design, operations or operating environment</td>
<td>Safety DC electrical and essential AC distribution system, reactor vault/bay, containment, decay heat removal system, emergency core cooling system, non-safety instrumentation and control, chemical volume and control system, power conversion system</td>
</tr>
<tr>
<td><strong>Proximity Dependencies</strong></td>
<td>A single environment has the potential to affect multiple units</td>
<td>Reactors, ultimate heat sink, containment, non-safety DC electrical and essential AC distribution system, control room HVAC</td>
</tr>
<tr>
<td><strong>Human Dependencies</strong></td>
<td>A person’s interaction with a machine affects multiple units</td>
<td>Shared control room, operator staffing more than one reactor</td>
</tr>
<tr>
<td><strong>Organizational Dependencies</strong></td>
<td>Connection through multiple units typically by a logic error that permeates the organization</td>
<td>Same vendor for safety and non-safety system valves, consolidated utility ownership of multiple nuclear power plant sites, decision-maker overseeing more than one reactor or more than one operator</td>
</tr>
</tbody>
</table>
Dynamic PRA Advantage

- Dynamic includes explicit modeling of deterministic dynamic processes that take place during plant system evolution along with stochastic modeling [Hakobyan, 2008]
  - Parameters are represented as time-dependent variables in event tree construction with branching times determined from the systems analysis code (MELCOR, RELAP, MAAP, etc.)
  - The discrete dynamic event tree (DDET) branches occur at user specified times or when an action is required by the system or operator
  - T-H model informs how the dynamic system variables evolve in time for each branch
  - Advantage of DDET vs. conventional event tree is simulation of probabilistic system evolution consistent with the deterministic model
Coupling Simulator Technology with ADS-IDAC

- Accident Dynamic Simulator – Information, Decision, and Action in a Crew context cognitive model (ADS-IDAC) [Coyne, 2009; Zhu, 2008; Hsueh, 1996]
  - T-H model (RELAP5) coupled with crew cognitive model
  - Generates DDET using simplified branching rules to model variations in crew responses
- Explicitly represent timing and sequencing of events
- Calculates impact of variations of hardware events and operator performance
- Captures complex unit-to-unit interdependencies
ADS-IDAC Process Overview

Upgraded thermal-hydraulic engine to simulator-based RELAP5-HD

Upgrading hardware reliability module to account for time-dependent environmental factors

1. Initialize RELAP Model and Read ADS-IDAC Input Data
2. Initialize ADS-IDAC for Initial Accident Sequence
3. Set $t_{counter} = 0$
4. Run one RELAP time step ($\Delta t_{RELAP}$)
5. $t_{counter} = t_{counter} + \Delta t_{RELAP}$
6. $t_{counter} > \Delta t_{ADS-IDAC}$?
7. Yes
8. Check and Actuate Initiating Events
9. Yes
10. Update Control Panel
11. Check and Actuate Component Failures
12. Execute Control Panel Actions
13. Process Information (Decision Maker)
15. Decision-Making (Decision Maker)
17. New Branches Generated?
18. Yes
19. Queue New Sequences for Later Simulation
20. No
21. Current Sequence Complete?
22. Yes
23. All Sequences Run?
24. No
25. Simulation Done

Coyne, 2008

Upgrading hardware reliability module to account for time-dependent environmental factors
Current Hardware Reliability Model

- **Time dependent failures** occur at a prescribed time during the simulation evolution—used to reflect hardware failures (e.g., pump or valve failure at time $t$) or an accident initiating event.
- **Conditional failures** occur when a component changes operating state to a pre-selected target value, thereby initiating the conditional failure of another system or component.
- **Recovery** an option.
- **Probability of hardware failure and recovery** modeled through beta distributions.
Accelerated Hardware Reliability Methodology

RELAP5-HD
System Variables
- Pressure (P)
- Temperature (T)
- Viscosity (v)
- Cycles (CS)
- Flowrate (W)

RELAP5-HD Reactor
System State (1 to n)

ADS-IDAC
HWReliabilityModule
- Time-dependent failure probability
- Conditional failure probability

GoldSim

Hardware Reliability Model
\[ p_{VA} = p_{VA,B} \left[ (0.051 \times C_{P,PO} \times C_{v,PO} \times C_{W,PO}) 
\quad + (0.087 \times C_{P,SE} \times C_{v,SE} \times C_{T,SE}) 
\quad + (0.862 \times C_{CS,SP}) \right] \]
Thermal-Hydraulic Model Improvement

*(GSE, 2013)*
ADS-IDAC Multi-Unit Data Flow

ADS-IDAC executable

Model execution thread
Loops over model advancements
• HD-Client
• Data collection and intervention logic

Client – Server Executive (SimExec)
• HD-Server
• HD-Client
• Additional Models

Server executive (for each reactor module)
• HD-Server (1...n+1)
  • RELAP-HD initialization
  • RELAP-HD advancement (Tran1)
  • [BOP models]
Event Tree Analysis

- Marginal event tree for one unit
- Conditional event tree for more than one unit
# Exploratory, stylized accident sequences

<table>
<thead>
<tr>
<th>Initiating Event</th>
<th>Top Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seismically-induced loss of offsite power with degraded ultimate heat sink</td>
<td>Safety DC Electrical, Reactor Protection System, Chemical Volume and Control System, Decay Heat Removal System, Emergency Core Cooling System</td>
</tr>
<tr>
<td>External flood with loss of offsite power</td>
<td>Safety DC Electrical, Reactor Protection System, Chemical Volume and Control System, Decay Heat Removal System, Emergency Core Cooling System</td>
</tr>
</tbody>
</table>
Research Summary

Simulation
- Dynamic PRA code enhancement
- RELAP5 update
- T-H plant model development

System Connections
- Initiating events
- Shared connections
- Identical components
- Proximity dependencies
- Human dependencies
- Organizational dependencies

Methodology Development
- Integrated site risk
- Dependency matrix
- Hardware reliability

Application
- Multi-unit example
- Reliability data
- Branch point criteria
Conclusions

• Simulation-based technique is needed to manage the proliferation of system information and feedback of multi-unit sites
• A new module allows the ADS-IDAC operator control panel to interface with simulator-derived information from either RELAP-HD or other balance-of-plant simulation modules
• This research is expected to develop and demonstrate a novel methodology that provides a framework for more realistic PRA analyses and assessment of the relative contribution of important core damage end states