A Dynamic Assessment of Auxiliary Building Contamination due to a Cyber-Induced Interfacing System Loss of Coolant Accident

Z. Jankovsky, M. Denman*, T. Aldemir

* Sandia National Laboratories
Acknowledgement

• This work was supported by funds provided to The Ohio State University by the Laboratory Directed Research and Development program at Sandia National Laboratories.

Background

- Digital Instrumentation & Control
  - Finer control, lower cost
  - New failure modes, particularly common cause
- Objectives of this case study
  - Examine an interfacing system loss of coolant accident (ISLOCA) caused by a control system failure.
  - Address uncertainties in component capacities and timing of mitigating actions.
- Key results
  - Relationships between uncertain parameters and consequence measures (i.e., hydrogen in aux. building)
Outline

• Hypothetical Plant System
• Nominal Accident Sequence
• Modeling of Plant & Accident
• Uncertainties
• Results
• Insights & Conclusions
Hypothetical Plant Design (1/5)

Hypothetical Plant Design (2/5)

- Three-loop pressurized water reactor (PWR)
  - Reactor coolant system (RCS) operates at 15.5MPa

- High pressure safety injection (HPSI)
  - Operates at 12MPa
  - Intake from refueling water storage tank (RWST)
  - Discharge to RCS cold legs

- Accumulators
  - Tanks of borated water behind check valves on RCS cold legs
  - Passive injection if RCS pressure falls below 4.6MPa
Hypothetical Plant Design (4/5)

• Combined low pressure safety injection (LPSI) and residual heat removal (RHR) system
  • Intake from (RWST) for LPSI, or RCS hot leg for RHR
  • Discharge to RCS cold leg
  • Pumps and heat exchangers (HXs) outside of containment
  • Operates at 2MPa
  • Protected from RCS pressure by check valves on discharge and motor-operated valves (MOVs) on RHR intake
  • RCS water in HX tube side, component cooling water (CCW) in shell
Hypothetical Plant Design (5/5)

- **Component Cooling Water (CCW)**
  - Provides necessary cooling for RHR HXs, RHR/LPSI pumps, and HPSI pumps
  - Operates at 0.7MPa
- **Pilot-operated relief valves (PORVs)**
  - Automatically above 16MPa, re-close below 15.5MPa
  - May be operated manually from control room
  - Vent RCS to containment
Accident Sequence (1/4)

1. RHR Isolation Valves Open at Power
   - Yes: ISLOCA, Begin Recovery
   - No: RHR Intake Pipe Break
     - Yes: LPSI Disabled, Begin Recovery
     - No: Aux. Building Flood

2. RHR HX Tube Break
   - Yes: Begin Recovery
   - No: RHR HX Shell Break
     - Yes: CCW Disabled, Begin Recovery
     - No: Aux. Building Flood
Accident Sequence (3/4)

- **RHR intake pipe** *(BRK-1)* or **HX shell failure** *(BRK-3)* leads to flooding
  - RCS and RWST inventory spills into aux. building
  - Delays operator attempts to repair components
  - Allows radionuclides and hydrogen to infiltrate aux. building

- **Mitigating Actions**
  - Isolate RWST from RHR/LPSI from control room
  - Isolate RCS from RHR at MOV controller
  - Isolate RHR pipe and/or HX leak from pump or HX room
  - Open PORVs to minimize loss of inventory from containment
Accident Sequence (4/4)

- **RHR HX tube** *(BRK-2)* or shell *(BRK-3)* failure disables CCW
  - Either over-pressurized (tube only), or leaks (tube and shell)
  - HPSI pumps, RHR/LPSI pumps unavailable until CCW recovered

- **Mitigating Actions**
  - Isolate CCW from RHR from CCW room
Modeling of Plant & Accident

- MELCOR model of plant systems
  - USNRC severe accident analysis code
  - Thermal-hydraulics, core degradation, radionuclide transport
- Initiating Event
  - RHR MOVs assumed to open simultaneously
- Dynamic Event Tree (DET) analysis with ADAPT
  - Branching rules define uncertainties to be explored
  - Upon reaching branching condition, new branches are created and run with sampled parameter values
  - Less computationally costly than Monte Carlo sampling
Analysis of Dynamic Accident Progression Trees (ADAPT)

- Simulator results drive progression of DET
- Past codes linked:
  - MELCOR 1.8/2.1
  - RELAP5
  - SAS4A
  - MAAP4
  - RADTRAD
Uncertainties of Interest (1/3)

- RHR component capacity
  - Occurrence and extent of ISLOCA
  - Potential for flooding
- Mitigating action timing
  - Isolation of ISLOCA
  - Recovery of key systems
Uncertainties of Interest (2/3)

- RHR component capacity for static overpressure

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentile</th>
<th>Capacity (MPa)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipe</td>
<td>5\textsuperscript{th}</td>
<td>4.2</td>
</tr>
<tr>
<td>Pipe</td>
<td>50\textsuperscript{th}</td>
<td>8.9</td>
</tr>
<tr>
<td>Pipe</td>
<td>95\textsuperscript{th}</td>
<td>16.0</td>
</tr>
<tr>
<td>HX Tube</td>
<td>5\textsuperscript{th}</td>
<td>7.8</td>
</tr>
<tr>
<td>HX Tube</td>
<td>50\textsuperscript{th}</td>
<td>11.0</td>
</tr>
<tr>
<td>HX Tube</td>
<td>95\textsuperscript{th}</td>
<td>16.0</td>
</tr>
<tr>
<td>HX Shell</td>
<td>5\textsuperscript{th}</td>
<td>6.1</td>
</tr>
<tr>
<td>HX Shell</td>
<td>50\textsuperscript{th}</td>
<td>9.4</td>
</tr>
<tr>
<td>HX Shell</td>
<td>95\textsuperscript{th}</td>
<td>15.0</td>
</tr>
</tbody>
</table>
Uncertainties of Interest (3/3)

• Timing for operator actions outside of control room
  • Min. time reflects delay to don protective equipment and travel through aux. building
  - Isolate RCS from RHR
  - Isolate flooding source
  - Isolate CCW from RHR

<table>
<thead>
<tr>
<th>Percentile</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5&lt;sup&gt;th&lt;/sup&gt;</td>
<td>393.0</td>
</tr>
<tr>
<td>50&lt;sup&gt;th&lt;/sup&gt;</td>
<td>608.0</td>
</tr>
<tr>
<td>95&lt;sup&gt;th&lt;/sup&gt;</td>
<td>1050.0</td>
</tr>
</tbody>
</table>
Results (1/8)

• DET run on small cluster
  • 39 branching conditions programmed, only 17 active due to computational burden
  • 38,000 total branches, 18,400 unique sequences
  • 450 processor-days, 9 calendar days (56 threads)
Results (2/8)

- Conditional core damage probability $2.9 \times 10^{-6}$
  - Traditional PRA output

- Figure of merit: hydrogen transport to aux. building
  - Reflects core damage
  - Reflects level of contamination in aux. building
  - Continuous parameter
Results (3/8)

- No RHR failures
- RCS isolated, PORVs closed
- ISLOCA start
- RHR failures
Results (4/8)

Top of active fuel
### Results (5/8)

- Using dynamic importance measures (DIMs)
  - Reveal relationships between branching values and output figures of merit (FOMs)
  - Define FOM as peak, final, or all values of a parameter

<table>
<thead>
<tr>
<th>Importance Measure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$DIM1 = \frac{R(x = 1)}{R(x = 0)}$</td>
<td>Consequence ratio of event occurrence to non-occurrence</td>
</tr>
<tr>
<td>$DIM2(i) = \frac{R(x = 1_i)}{R(x = 0)}$</td>
<td>Consequence ratio of value $x=1_i$ to non-occurrence</td>
</tr>
<tr>
<td>$DIM3(i) = \frac{R(x = 1_i)}{R(x = 1)}$</td>
<td>Consequence ratio of value $x=1_i$ to average of occurrence</td>
</tr>
</tbody>
</table>

$R()$: weighted average FOM, such as hydrogen in aux. building, for set ()

$x=0$: set of sequences where event $x$ does not occur

$x=1$: set where event $x$ occurs

$x=1_i$: set with value $i$ of parameter $x$
Results (6/8)

- Example calculation
  - $\text{H}_2$ accumulation in aux. building when RHR intake pipe fails
  - Indicator of core damage and potential for radionuclide release past containment

\[
DIM1 = \frac{R(x = 1)}{R(x = 0)} = \frac{\sum_{j}^{n_{x=1}} P_j \cdot R_j}{\sum_{j}^{n_{x=1}} P_j} = \frac{\frac{6.2 \times 10^{-7}}{1.4 \times 10^{-7}}}{\frac{7.8 \times 10^{-6}}{(1 - 1.4 \times 10^{-7})}} = 5.7 \times 10^5
\]

- Interpretation
  - Expected $\text{H}_2$ accumulation when RHR intake pipe fails is $5.7 \times 10^5$ times the expected accumulation when the pipe does not fail.
Results (7/8)

- Occurrence of failure events:

<table>
<thead>
<tr>
<th>Event</th>
<th>DIM1</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHR pipe break</td>
<td>5.7*10^5</td>
</tr>
<tr>
<td>RHR HX tube break</td>
<td>Inf</td>
</tr>
<tr>
<td>RHR HX shell break</td>
<td>Inf</td>
</tr>
</tbody>
</table>

- No H_2 in aux. building without both RHR HX failures
- Combined RHR HX failure disables HPSI and LPSI early

- Uncertain physical parameter:

<table>
<thead>
<tr>
<th>Event</th>
<th>DIM3</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHR Pipe Capacity (5th)</td>
<td>1.6*10^{-6}</td>
</tr>
<tr>
<td>RHR Pipe Capacity (50th)</td>
<td>7.9*10^{11}</td>
</tr>
<tr>
<td>RHR Pipe Capacity (95th)</td>
<td>2.4*10^{-7}</td>
</tr>
</tbody>
</table>

- Highest consequences for pipe capacity in middle of range
Results (8/8)

• Success of response:
  
  Event | DIM1
  -------|-------
  RHR HX shell isolation | 0.69

  • Overall, small benefit to performing isolation

• Timing of response

  Event | DIM3
  -------|-------
  RHR HX shell isolation (5th) | 0.08
  RHR HX shell isolation (50th) | 1.4
  RHR HX shell isolation (95th) | 1.5

  • Early isolation leads to significantly better outcome
  • Later isolation is counter-productive
  • Insensitive to timing for most of range
Conclusions

• Dynamic ISLOCA case
  • Control system failure opening RHR isolation valves
  • Efficiently-sampled uncertainties in component capacity and timing of mitigating actions

• Flexible measures of importance
  • Accommodate non-binary branching conditions
  • Continuous values for figures of merit
  • Assess differences between sets of sequences

• RHR ISLOCA consequences sensitive to HX failures
  • Can affect CCW, disabling other dependent systems
  • Timely recovery actions reduce impact
  • If early recovery attempts fail, may be more effective to try other actions