Incorporation of a Dynamic Reliability Model into an Existing Plant PRA

Tony Mangan

The Ohio State University

Outline

- Background
- Objectives
- About SAPHIRE
- The Existing Plant PRA
- The Dynamic Model
- Methodology
- Results
- Conclusions
- References

Background

- Every U.S. plant has performed reliability studies and will have a Probability Risk Assessment (PRA) model
- Existing Nuclear Power Plants are replacing analog control systems with digital ones
- Any changes to the plant must be evaluated for safety concerns (10 CFR 50)
- Therefore, the plant PRA model must be updated to account for new digital control systems

Background

- Existing plant PRAs have been performed using traditional static methods such as the Fault Tree/Event Tree method
- Digital control systems should be modeled using dynamic methodologies
- Dynamic methods explicitly account for time and other process variables

Purpose

- Model digital control systems using dynamic methods
- Retain existing static plant PRA
- Link dynamic model of control systems with existing plant PRA
- Capture timing and other process variables of the digital control systems while avoiding need to remodel the entire plant

Objectives

- 1: digital component must retain dynamic information
- 2: shared components between the models must be recognized as such
- 3: dynamic model must be integrated to the existing plant PRA without making large changes

Objectives (cont)

- 4: the combined model must be capable of generating cut sets (minimum combination of events that lead to failure of the overall system)
- 5: the model must be capable of numeric quantification, and must be capable of performing additional analysis (Importance, Uncertainty, Sensitivity)

Procedure

- An existing plant PRA modeled in SAPHIRE has been obtained from INL
- Dynamic model of a digital control system was developed
- The dynamic model has been imported into SAPHIRE
- The dynamic model is linked to the plant PRA

About SAPHIRE

System Analysis Program for Hands-on Integrated Reliability Evaluations

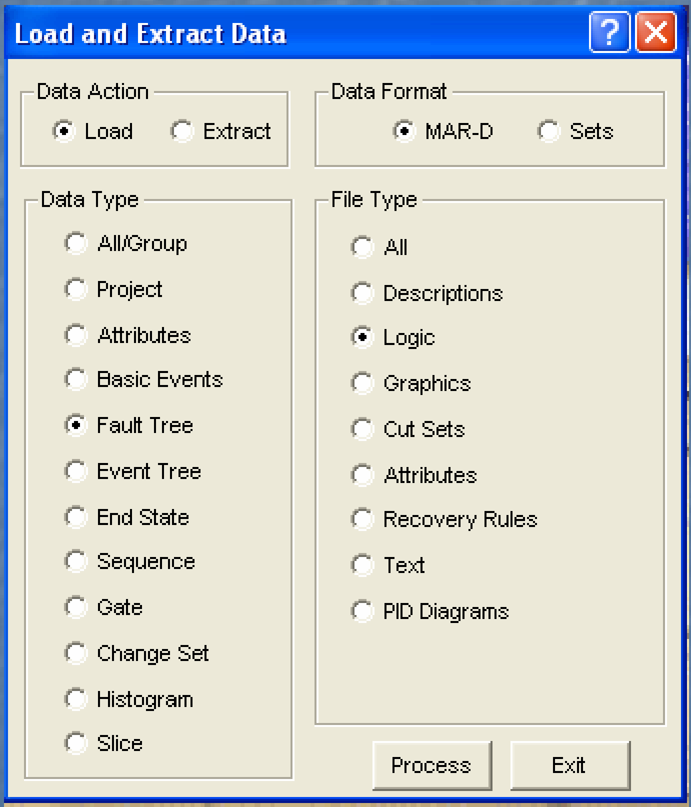
- SAPHIRE is a PRA software developed by INL
- Allows the user to create and analyze fault tree/ event tree models on a PC
- Uses graphical and text-based interface

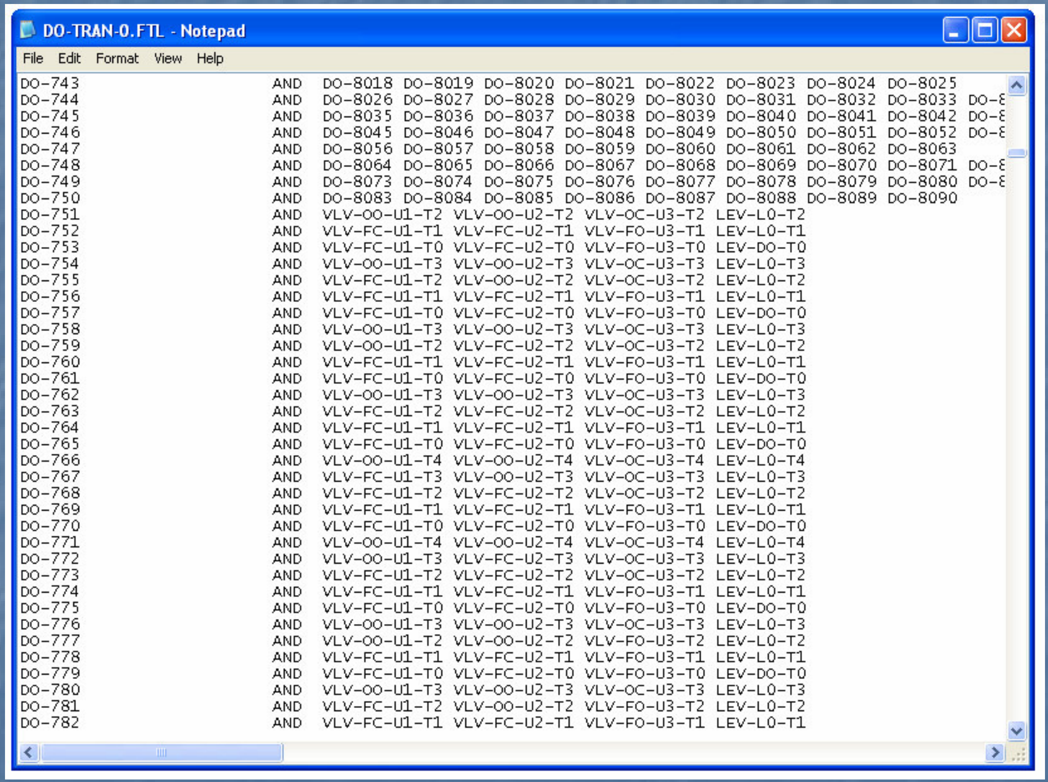
SAPHIRE Analysis

- Generate cut sets
- Quantify cut sets
- Additional Analysis Tools:
  - Uncertainty Analysis - calculates the variability of a fault tree top event resulting from uncertainties in the basic event probabilities
  - Importance Analysis - gives a measure of the significance of system components, components with a high relative importance should be closely monitored or, if possible, redesigned to improve reliability
  - Sensitivity Analysis - calculates the sensitivity of the system to specific changes to basic event attributes

SAPHIRE MAR-D Tool

Models and Results Database



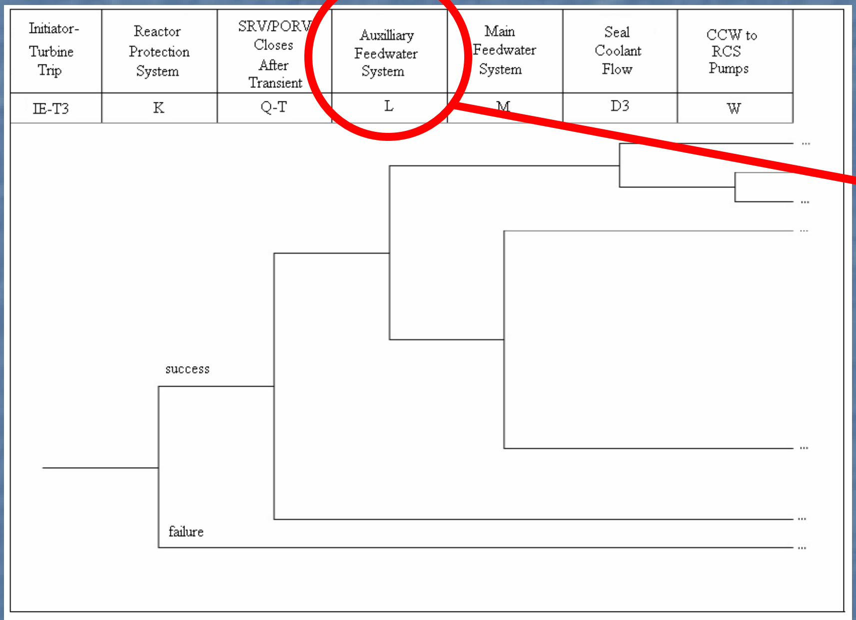


The Existing Plant PRA

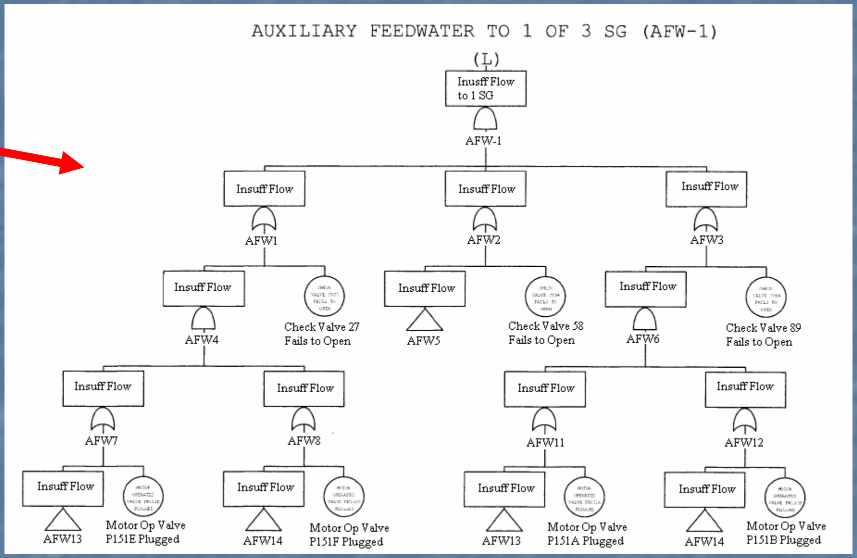
- Simplified model of an existing U.S. nuclear power plant, modeled in NUREG-1150
- Westinghouse design PWR
- 3 Steam Generators
- Approx. 800 MW(e)

Existing Plant PRA (cont)

Turbine Trip Event Tree



Auxiliary Feedwater (AFW) Fault Tree



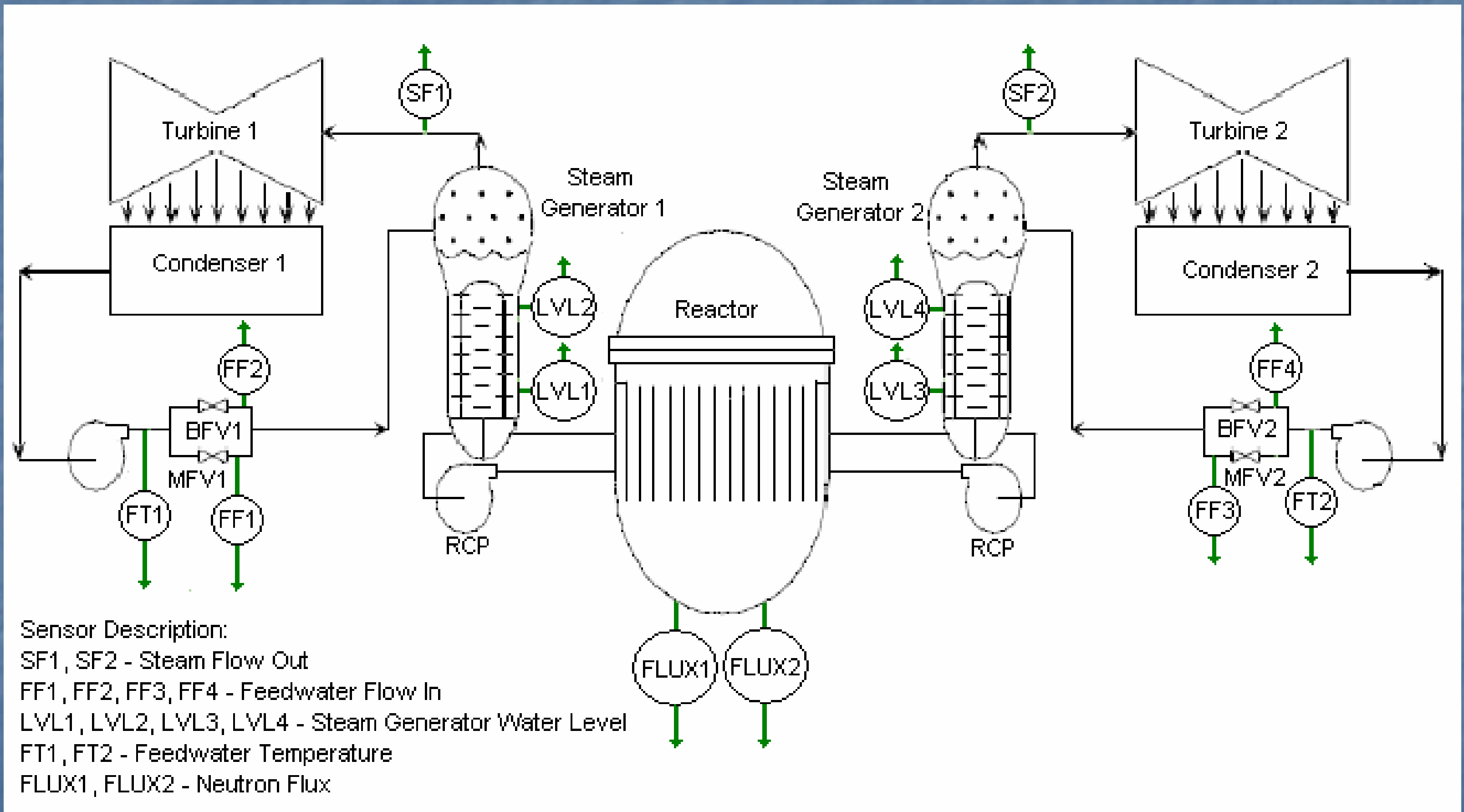
Dynamic Model

- Benchmark Digital Feedwater Control System
- Modeled using Markov Models
- assume to represent a Digital Feedwater Control System applicable to the example plant

Markov Models

- State-based model
- Each state represents a different combination of operating components, failed components, and components under repair
- Transition rates from state to state are used to determine the probability of failure

Benchmark Digital Feedwater Control System



Benchmark Digital Feedwater Control System (cont)

- Components:
  - Main Feedwater Regulating Valve (MFV)
  - Bypass Feedwater Regulating Valve (BFV)
  - Feedwater Pump (FP)
  - MFV Controller, BFV Controller, PDI Controller, Main Computer, Backup Computer

DFWCS Scenario: Turbine Trip

- Reactor shutdown, Power from decay heat
  - Low Power Mode (only BFV is used, MFV is closed)
- Feedwater flow is at a nominal level
- Offsite power is available
- Main computer has failed, backup in control

DFWCS Failure Sequences

Event Sequence	Time Step	State #	State Description	Level
1	0	1	OK	0
	1	5	Arbitrary Output	-1
	2	5	Arbitrary Output	-1
	3	5	Arbitrary Output	-2
2	0	1	OK	0
	1	5	Arbitrary Output	-1
	2	5	Arbitrary Output	-1
	3	6	Zero Volt Output	-2
3	0	1	OK	0
	1	5	Arbitrary Output	-1
	2	5	Arbitrary Output	-1
	3	7	Controller Stuck	-2
4	0	1	OK	0
	1	5	Arbitrary Output	-1
	2	6	Zero Volt Output	-1
	3	6	Zero Volt Output	-2
5	0	1	OK	0
	1	5	Arbitrary Output	-1
	2	6	Zero Volt Output	-1
	3	7	Controller Stuck	-2
6	0	1	OK	0
	1	5	Arbitrary Output	-1
	2	7	Controller Stuck	-1
	3	7	Controller Stuck	-2
7	0	1	OK	0
	1	6	Zero Volt Output	-1
	2	6	Zero Volt Output	-1
	3	6	Zero Volt Output	-2

Methodology Overview

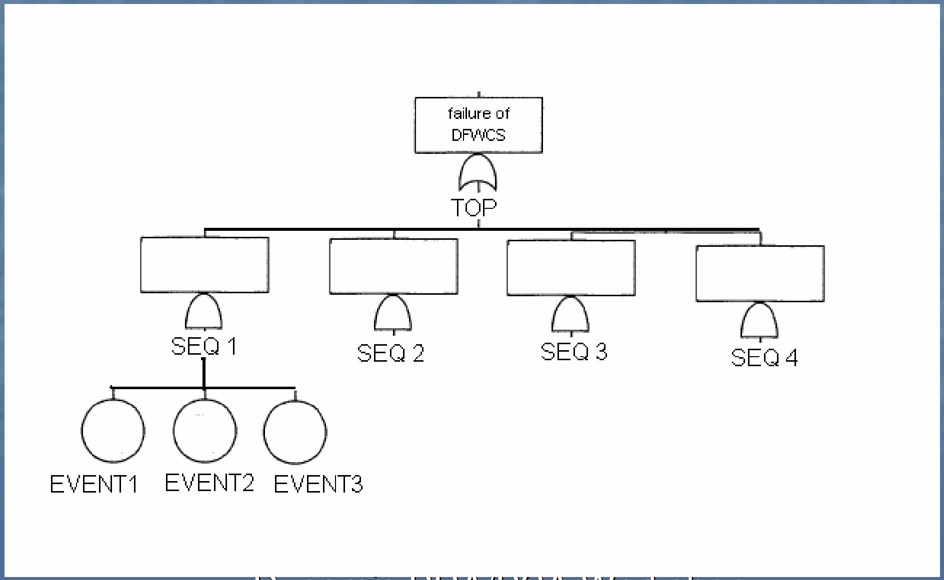
- 1) Construct Fault Tree from Markov Model
- 2) Create text file to import Fault Tree into SAPHIRE
- 3) Link dynamic model to existing plant PRA in SAPHIRE editor
- 4) Identify common components between the dynamic model and the existing plant PRA
- 5) Write Recovery Rules to relate common components, remove inconsistent cut sets, add detail, etc
- 6) Solve the combined model

Methodology Assumptions

- 1) Assume the Benchmark DFWCS represents an actual DFWCS designed for the example plant
- 2) Assume that Feedwater Control is tied to the AFW System (traditionally, it only controls the MFW system)

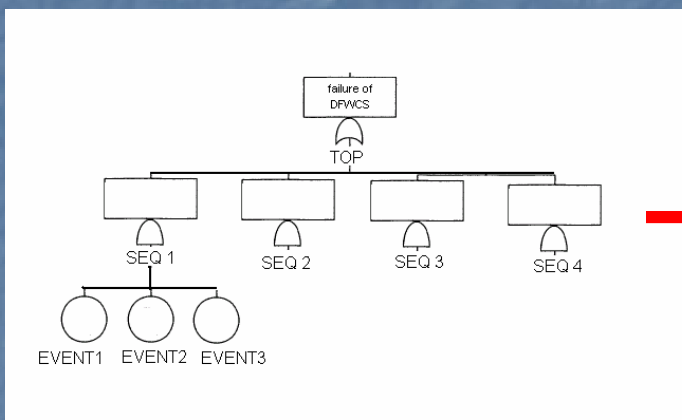
Markov Model to Fault Tree

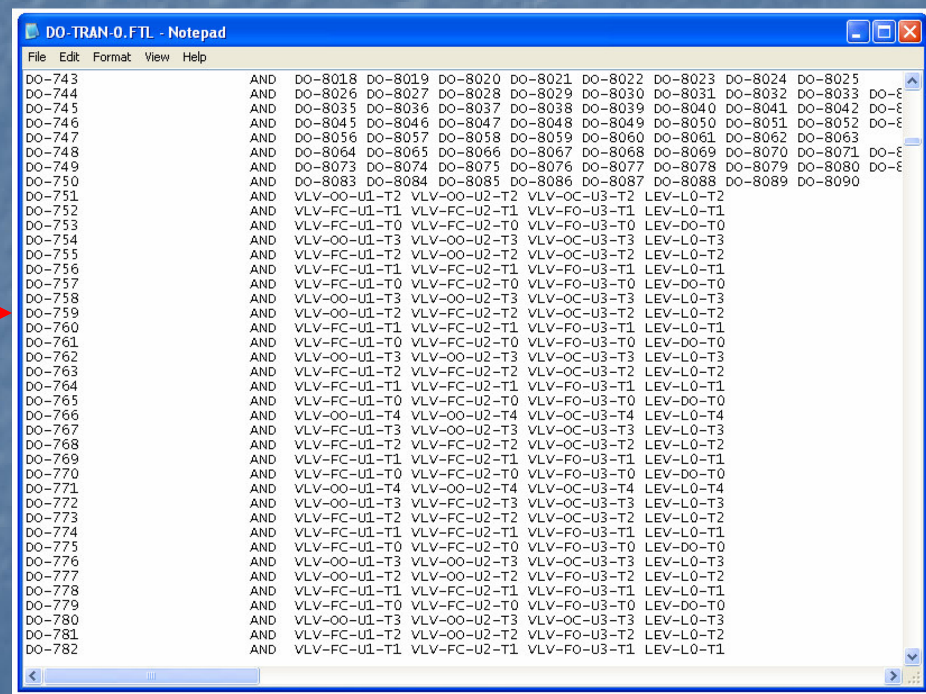
- 1) Construct Fault Tree from Markov Model
  - A Cell-to-Cell mapping technique is used to generate event sequences from the Markov Model
  - Event sequences are time-tagged to retain timing information
  - Each event sequence is stated as a series of events, which can be converted to a large fault tree



Create Import File

- 2) Write fault trees into text file (.FTL) to import into SAPHIRE using MAR-D tool



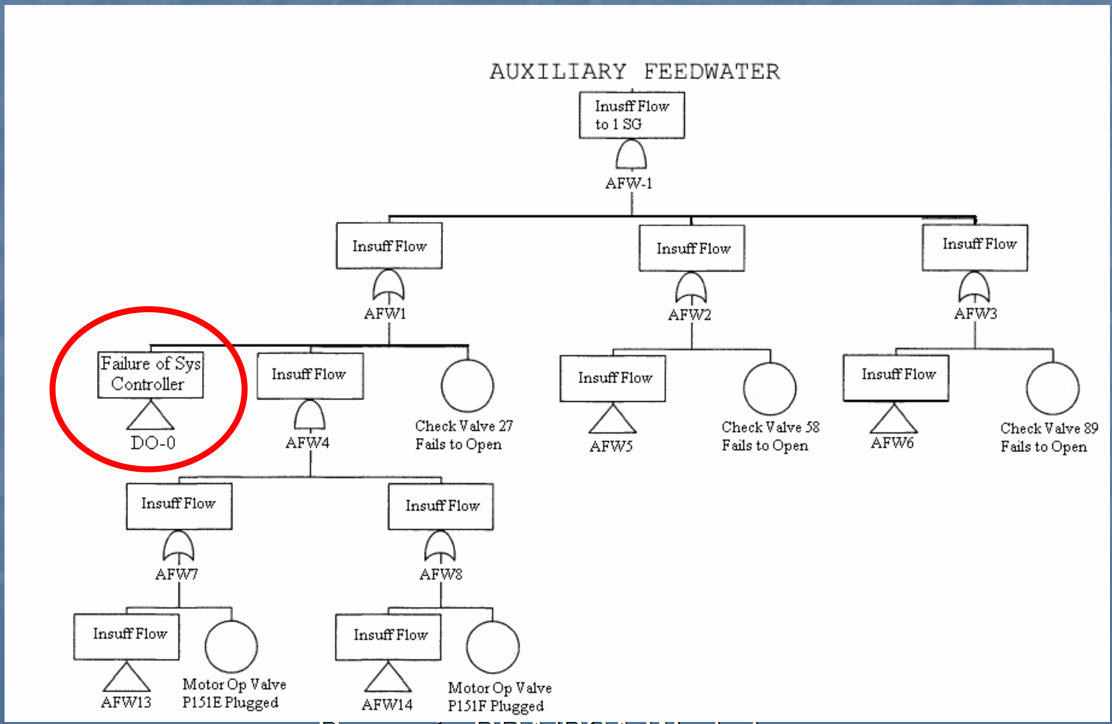

DO-TRAN-0.FTL - Notepad

File Edit Format View Help

```
DO-743                      AND   DO-8018 DO-8019 DO-8020 DO-8021 DO-8022 DO-8023 DO-8024 DO-8025
DO-744                      AND   DO-8026 DO-8027 DO-8028 DO-8029 DO-8030 DO-8031 DO-8032 DO-8033 DO-
DO-745                      AND   DO-8035 DO-8036 DO-8037 DO-8038 DO-8039 DO-8040 DO-8041 DO-8042 DO-
DO-746                      AND   DO-8045 DO-8046 DO-8047 DO-8048 DO-8049 DO-8050 DO-8051 DO-8052 DO-
DO-747                      AND   DO-8056 DO-8057 DO-8058 DO-8059 DO-8060 DO-8061 DO-8062 DO-8063
DO-748                      AND   DO-8064 DO-8065 DO-8066 DO-8067 DO-8068 DO-8069 DO-8070 DO-8071 DO-
DO-749                      AND   DO-8073 DO-8074 DO-8075 DO-8076 DO-8077 DO-8078 DO-8079 DO-8080 DO-
DO-750                      AND   DO-8083 DO-8084 DO-8085 DO-8086 DO-8087 DO-8088 DO-8089 DO-8090
DO-751                      AND   VLV-OO-U1-T2 VLV-OO-U2-T2 VLV-OC-U3-T2 LEV-LO-T2
DO-752                      AND   VLV-FC-U1-T1 VLV-FC-U2-T1 VLV-FO-U3-T1 LEV-LO-T1
DO-753                      AND   VLV-FC-U1-T0 VLV-FC-U2-T0 VLV-FO-U3-T0 LEV-DO-T0
DO-754                      AND   VLV-OO-U1-T3 VLV-OO-U2-T3 VLV-OC-U3-T3 LEV-LO-T3
DO-755                      AND   VLV-FC-U1-T2 VLV-OO-U2-T2 VLV-OC-U3-T2 LEV-LO-T2
DO-756                      AND   VLV-FC-U1-T1 VLV-FC-U2-T1 VLV-FO-U3-T1 LEV-LO-T1
DO-757                      AND   VLV-FC-U1-T0 VLV-FC-U2-T0 VLV-FO-U3-T0 LEV-DO-T0
DO-758                      AND   VLV-OO-U1-T3 VLV-OO-U2-T3 VLV-OC-U3-T3 LEV-LO-T3
DO-759                      AND   VLV-OO-U1-T2 VLV-FC-U2-T2 VLV-OC-U3-T2 LEV-LO-T2
DO-760                      AND   VLV-FC-U1-T1 VLV-FC-U2-T1 VLV-FO-U3-T1 LEV-LO-T1
DO-761                      AND   VLV-FC-U1-T0 VLV-FC-U2-T0 VLV-FO-U3-T0 LEV-DO-T0
DO-762                      AND   VLV-OO-U1-T3 VLV-OO-U2-T3 VLV-OC-U3-T3 LEV-LO-T3
DO-763                      AND   VLV-FC-U1-T2 VLV-FC-U2-T2 VLV-OC-U3-T2 LEV-LO-T2
DO-764                      AND   VLV-FC-U1-T1 VLV-FC-U2-T1 VLV-FO-U3-T1 LEV-LO-T1
DO-765                      AND   VLV-FC-U1-T0 VLV-FC-U2-T0 VLV-FO-U3-T0 LEV-DO-T0
DO-766                      AND   VLV-OO-U1-T4 VLV-OO-U2-T4 VLV-OC-U3-T4 LEV-LO-T4
DO-767                      AND   VLV-FC-U1-T3 VLV-OO-U2-T3 VLV-OC-U3-T3 LEV-LO-T3
DO-768                      AND   VLV-FC-U1-T2 VLV-FC-U2-T2 VLV-OC-U3-T2 LEV-LO-T2
DO-769                      AND   VLV-FC-U1-T1 VLV-FC-U2-T1 VLV-FO-U3-T1 LEV-LO-T1
DO-770                      AND   VLV-FC-U1-T0 VLV-FC-U2-T0 VLV-FO-U3-T0 LEV-DO-T0
DO-771                      AND   VLV-OO-U1-T4 VLV-OO-U2-T4 VLV-OC-U3-T4 LEV-LO-T4
DO-772                      AND   VLV-OO-U1-T3 VLV-FC-U2-T3 VLV-OC-U3-T3 LEV-LO-T3
DO-773                      AND   VLV-FC-U1-T2 VLV-FC-U2-T2 VLV-OC-U3-T2 LEV-LO-T2
DO-774                      AND   VLV-FC-U1-T1 VLV-FC-U2-T1 VLV-FO-U3-T1 LEV-LO-T1
DO-775                      AND   VLV-FC-U1-T0 VLV-FC-U2-T0 VLV-FO-U3-T0 LEV-DO-T0
DO-776                      AND   VLV-OO-U1-T3 VLV-OO-U2-T3 VLV-OC-U3-T3 LEV-LO-T3
DO-777                      AND   VLV-OO-U1-T2 VLV-OO-U2-T2 VLV-FO-U3-T2 LEV-LO-T2
DO-778                      AND   VLV-FC-U1-T1 VLV-FC-U2-T1 VLV-FO-U3-T1 LEV-LO-T1
DO-779                      AND   VLV-FC-U1-T0 VLV-FC-U2-T0 VLV-FO-U3-T0 LEV-DO-T0
DO-780                      AND   VLV-OO-U1-T3 VLV-OO-U2-T3 VLV-OC-U3-T3 LEV-LO-T3
DO-781                      AND   VLV-FC-U1-T2 VLV-OO-U2-T2 VLV-FO-U3-T2 LEV-LO-T2
DO-782                      AND   VLV-FC-U1-T1 VLV-FC-U2-T1 VLV-FO-U3-T1 LEV-LO-T1
```

Link Models

- 3) Link dynamic model to existing plant PRA in SAPHIRE editor

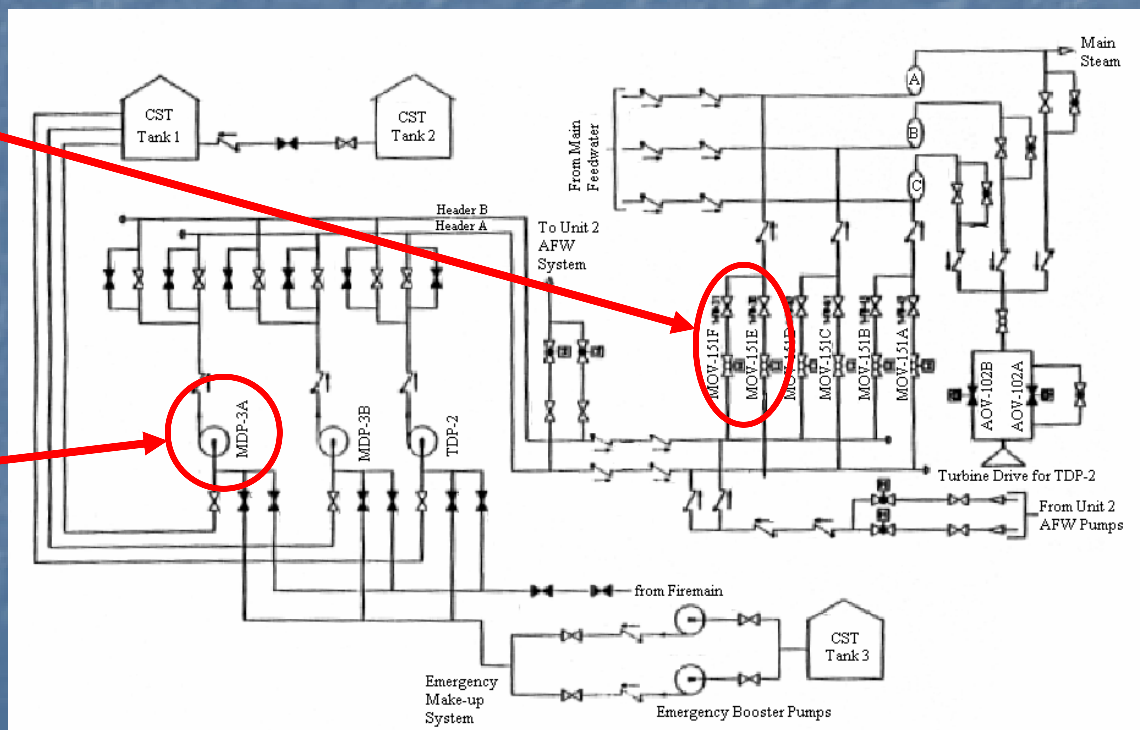


Shared Components

- 4) Identify common components between the dynamic model and the existing plant PRA

MFV and BFV Valves

Feedwater pump



Shared Components

- Need a way for SAPHIRE to recognize that components used by both the dynamic portion and the static portion are the same
- Complication – events from the dynamic portion are typically time tagged

EventA = EventA-1, EventA-2, EventA-3, …

Shared Components

Solution: SAPHIRE Recovery Rules

- Used to search and edit cut sets
- Written before cut sets are generated, but applied afterwards
- Can be used to remove basic events, add new basic events, copy entire cut sets, etc.

Shared Components

SAPHIRE Recovery Rules

- The Rules shown here remove all occurrences of the events AFW-MOV-PG-151E and AFW-MOV-PG-151F, replacing them with new events
  - This rule creates an implicit relationship between components from the imported dynamic model and the existing plant PRA
  - This rule assumes that any failure in the static PRA happens at time step 0

| Change MOV-151E to failed closed

if (AFW-MOV-PG-151E) then

AddEvent = VLV-FC-U1-T0;

DeleteEvent = AFW-MOV-PG-151E;

endif

| Change MOV-151F to failed closed

if (AFW-MOV-PG-151F) then

AddEvent = VLV-FC-U2-T0;

DeleteEvent = AFW-MOV-PG-151F;

endif

Inconsistent Cut Sets

SAPHIRE Recovery Rules

- The existing plant PRA's steam outlet valve has multiple failure modes:
  - Plugged, fails to open, common cause failure, etc
- Desirable to retain these failure modes, while still ensuring that no incorrect cut sets are present
- This rule searches all cut sets for a failure to the steam outlet valve occurring from both the static portion and the dynamic portion
- For any occurrences, the cut set is flagged.

```
A = (AFW-AOV-PG-102A + AFW-AOV-FT-102A + AFW-ACT-FA-VLVA +
       AFW- CCF-FT-102AB);
B = (VLV-FO-U3-T0 + VLV-FO-U3-T1
     + VLV-FO-U3-T2 + VLV-FO-U3-T3
     + VLV-FO-U3-T4 + VLV-FO-U3-T5
     + VLV-FO-U3-T6 + VLV-FO-U3-T7
     + VLV-FO-U3-T8 + VLV-FO-U3-T9
     + VLV-FO-U3-T10 + VLV-FO-U3-T11);

if (A*B) then
     AddEvent = FLAG-ME;
endif
```

Adding Detail

SAPHIRE Recovery Rules

- Add loss of electrical power failure modes to digital components
- Assume that loss of electrical power results in *Computer Down* failure state or *Zero Voltage (DC)* failure state

Adding Detail

```
if BC-DOWN-T2 then
      CopyCutSet;
      DeleteEvent = BC-down-T2;
      AddEvent = BC-BUSWORK-FAILS-T2;
      CopyRoot;
      DeleteEvent = BC-down-T2;
      AddEvent = LOSP;
      AddEvent = OEP-DGN-FS-DG01-T2;
      CopyRoot;
      DeleteEvent = BC-down-T2;
      AddEvent = LOSP;
      AddEvent = OEP-DGN-FR-DG01-T2;
      CopyRoot;
      DeleteEvent = BC-down-T2;
      AddEvent = LOSP;
      AddEvent = OEP-DGN-MA-DG01-T2;
      CopyRoot;
      DeleteEvent = BC-down-T2;
      AddEvent = LOSP;
      AddEvent = OEP-CRB-FT-15H3-T2;
endif
```

SAPHIRE Results

- Cut sets of the combined model have been successfully generated
- 169,740 cut sets from existing plant PRA
- 530 event sequences from Case 2 model
- 172,530 cut sets from combined model

Cut Sets

Static plant model

Event Sequence	Time Step	State #	State Description	Level
1	0	1	OK	0
	1	5	Arbitrary Output	-1
	2	5	Arbitrary Output	-1
	3	5	Arbitrary Output	-2

AFW-CKV-FT-CV58 * AFW-CKV-FT-CV89 * /BFV-CONT-FREEZE-T0 * /BFV-CONT-ARB-T0 * /BFV-CONT-ZERO-T0 * /BFV-CONT-STUCK-T0 * /BC-NOSIGNAL-T0 * /BC-DOWN-T0 * BFV-CONT-FREEZE-T1 * /BFV-CONT-ARB-T1 * /BFV-CONT-ZERO-T1 * /BFV-CONT-STUCK-T1 * BFV-CONT-FREEZE-T2 * /BFV-CONT-ARB-T2 * /BFV-CONT-ZERO-T2 * /BFV-CONT-STUCK-T2 * /BFV-CONT-FREEZE-T3 * /BFV-CONT-ARB-T3 * /BFV-CONT-ZERO-T3 * BFV-CONT-STUCK-T3

Conclusions

- The Methodology presented here successfully incorporates a dynamic model into an existing plant PRA

Conclusions (cont)

Recall from Objectives:

- 1: digital component must retain dynamic information → Dynamic information is discretized but retained through tagging of events
- 2: shared components between the models must be recognized as such → Recovery Rules create implicit relationship between shared events
- 3: dynamic model must be integrated to the existing plant PRA without making large changes → Single Gate added to Fault Tree

Conclusions (cont)

- 4: the combined model must be capable of generating cut sets
- 5: the model must be capable of numeric quantification, and must be capable of performing additional analysis (Importance, Uncertainty, Sensitivity)

Cut sets have been successfully generated

SAPHIRE is capable of performing all necessary calculations and analysis

Recommendations for Future Work

- Perform method using realistic models
- Add failure data to dynamic model
- Perform numerical comparison to failure rate of combined static/dynamic model to that of existing static model alone
- Streamline process
- Further study into possible inconsistencies in cut sets

References

- 1: (NUREG-1150) Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, U.S. Nuclear Regulatory Commission, Washington, D.C., 1990.
- 2: (NE 716 text) McCormick, N. J., Reliability and Risk Analysis: Methods and Nuclear Power Plant Applications, Academic Press, Inc, Boston, 1981.
- 3: Smith, C., Knudsen, J., Calley, M., Beck, S., Kvadfordt, K., Wood, S. T., SAPHIRE Basics, Idaho National Laboratory, Idaho Falls, ID, 2005.
- 4: Smith, C., Knudsen, Wood, S. T., Advanced SAPHIRE, Idaho National Laboratory, Idaho Falls, ID, 2005.

References

- 5: Bucci, P., Kirschenbaum, J., Aldemir, T., Smith, C., and Wood, T., "Constructing Dynamic Event Trees from Markov Models", 2006.
- 6: Aldemir, T., 1987, "Computer-Assisted Markov Modeling of Process Control Systems," *IEEE Trans. Reliability*, R-36, 133-144.
- 7: Kirschenbaum, J., Bucci, P., Stovsky, M., Mandelli, D., Aldemir, T., Yau, M., Guarro, S., Ekici, E., Arndt, S.A., "A Benchmark System for Comparing Reliability Modeling Approaches for Digital Instrumentation and Control Systems", not yet published.

References

- 8: NUREG/CR-6901 - T. Aldemir, D. W. Miller, M. P. Stovsky, J. Kirschenbaum, P. Bucci, A. W. Fentiman , L. A. Mangan, S. A. Arndt, Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901, U.S. Nuclear Regulatory Commission, Washington, D.C., 2006.
- 9: NUREG/CR-6942 - T. Aldemir, M. P. Stovsky, J. Kirschenbaum, D. Mandelli, P. Bucci, L. A. Mangan, , D. W. Miller, A.W. Fentiman, E. Ekici, S. Guarro, M. Yao, B. Johnson, C. Elks, S. A. Arndt, Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments, NUREG/CR-**????**, U.S. Nuclear Regulatory Commission, Washington, D.C., not yet published.

Acknowledgements

- This work has been performed as part of project sponsored by the U.S. NRC. The information and conclusions presented here in are those of the author and do not necessarily represent the views or positions of the U.S. NRC. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assume any legal liability or responsibility for any third party’s use of this information.