PSAM 9 Session # C9 : PRA Modeling of Digital Instrumentation and Control Systems II (paper #502)

Integrated Software Hazard Analysis Method for Digital I&C Systems

Hui-Wen Huang, Chunkuan Shih, and Long-Chen Wang, etc.

Presented by Tsu-Mu Kao

Institution of Nuclear Energy Research (INER), Taiwan

Kowloon Shangri-La Hotel, Hong Kong

May 21, 2008

Outline

I. Introduction

II. Software Fault Tree Analysis

III. Sequence Tree Method

IV. Simulator Based Analysis

V. Conclusions

I. Introduction (1/6)

Many recent NPP designs utilize digital control systems. Digital control systems have the following advantages:

- **1) No setpoint drifting**
- **2) Automatic calibration**
- **3) Various improvement capabilities, such as fault tolerance, self-testing, signal validation and process system diagnostics**
- **4) Much detailed information helping operators to discover the plant status**

I. Introduction (2/6)

While I&C system being digitalized, three issues are encountered:

- 1) Software common-cause failure
- 2) Interaction failure between operator and digital instrumentation and control system interface
- 3) Non-detectability of software failure

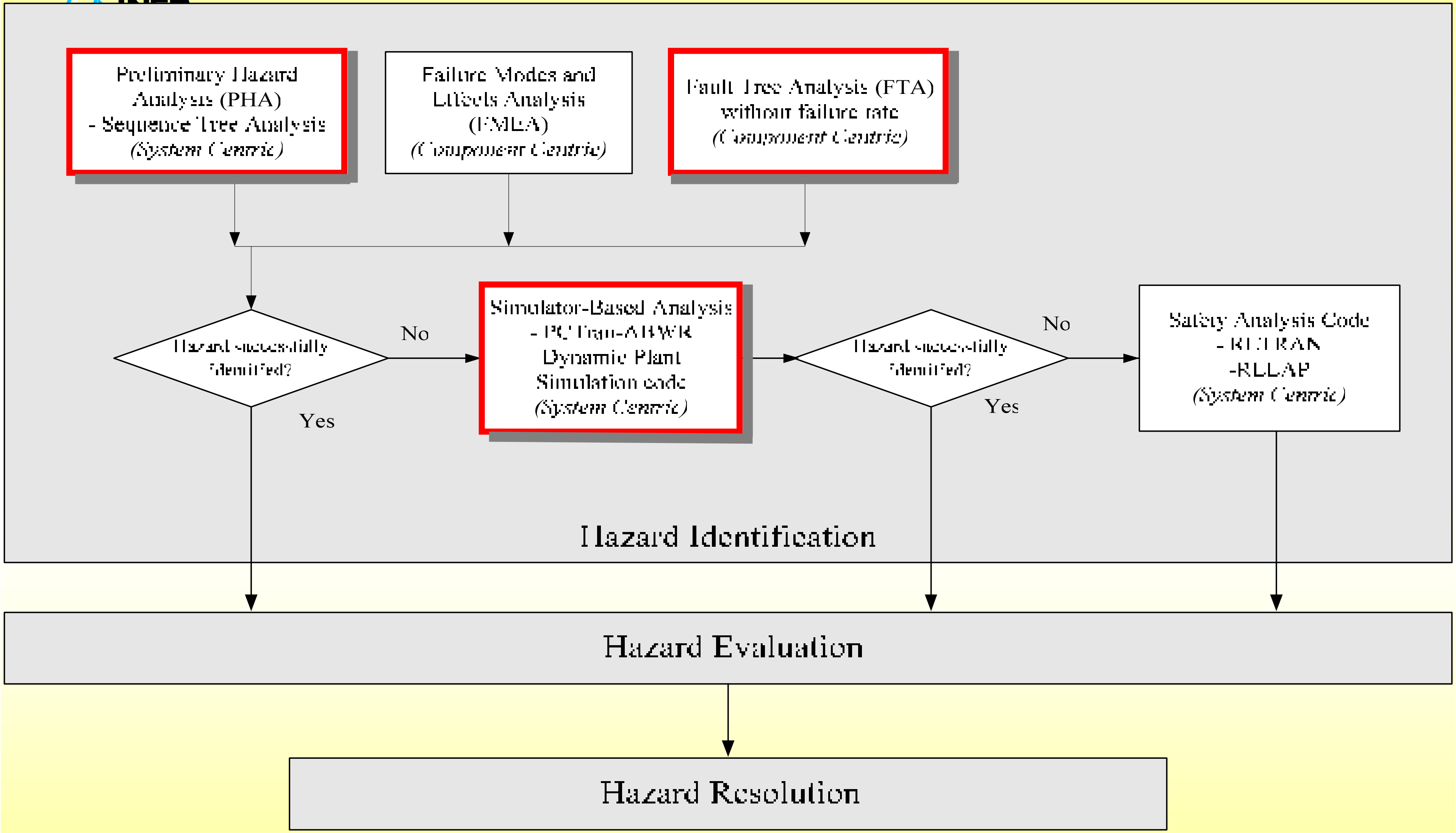
I. Introduction (3/6)

- **The software of nuclear power plant digital I&C systems**
  - Improving software reliability by reducing software faults
    - Software Verification and Validation (SV&V)
    - Software Configuration Management (SCM)
    - Software Test
  - Enhancing system safety by mitigating the consequences of software failure
    - **Software Safety Analysis (SSA)**
    - **Diversity and Defense-in-Depth (D3) Analysis**

I. Introduction (4/6)

- **Annex D of IEEE 7.4.3.2-2003, “Identification and resolution of hazards ” proposes several Software Safety Analysis (SSA) techniques.**
  - **Preliminary Hazard Analysis (PHA)**
    - **Sequence Tree Method**
  - Failure Modes and Effects Analysis (FMEA)
  - **Fault Tree Analysis (FTA)**
  - System modeling
  - Software requirements hazard analysis
  - Walkthroughs
  - **Simulator/plant model testing**

I. Introduction (5/6)



Hazard Identification Application Strategy

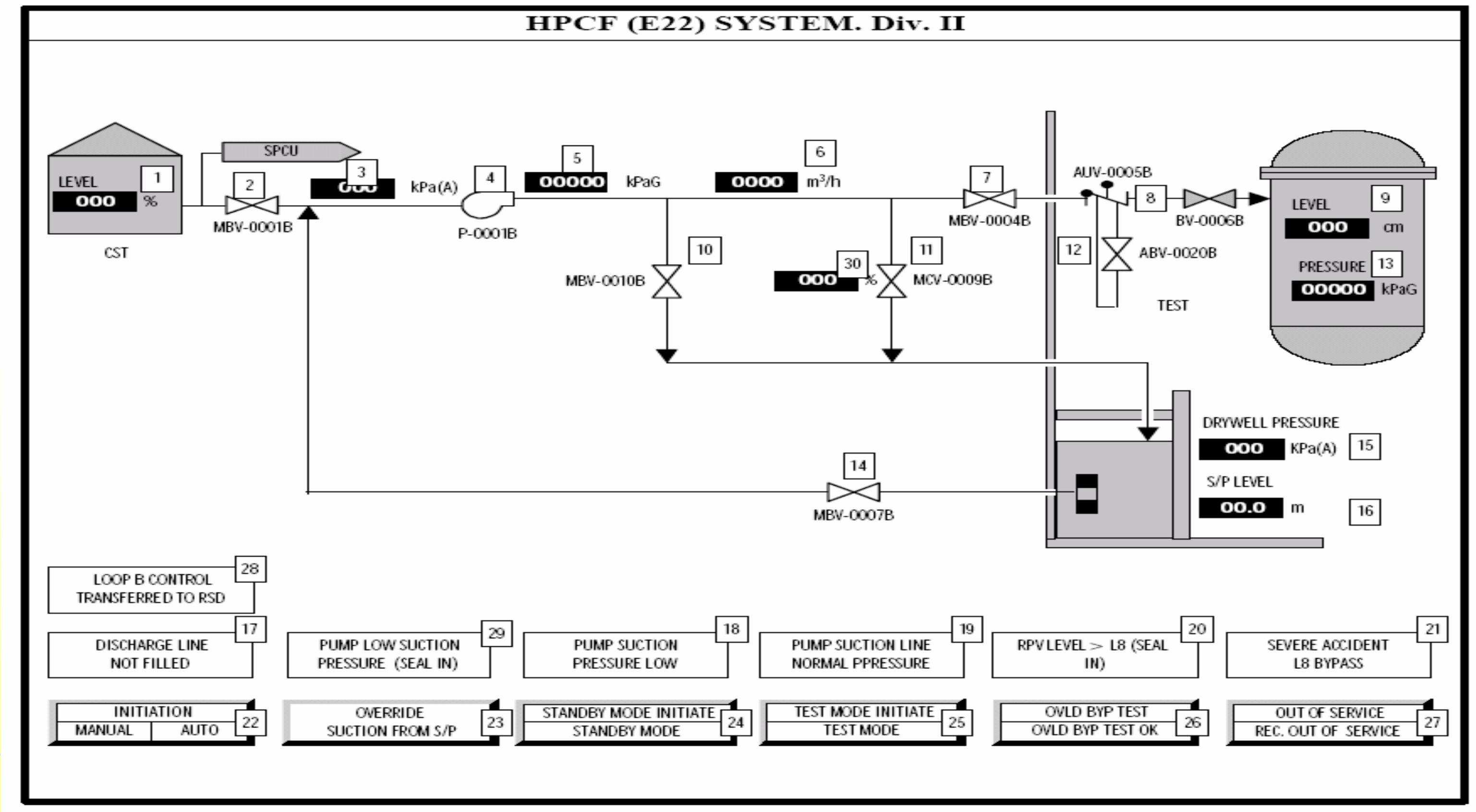
I. Introduction (6/6)

- **Integrated Software Safety Analysis Method**
  - Software Fault Tree Analysis
    - to analyze component level software fault
  - Sequence Tree Method
    - to analyze the interactions and effects among I&C systems and operators
  - Simulator Based Analysis
    - to analyze the time dependent effect for some specific cases
- **Case Study**
  - ABWR
  - LOCA, Steam Line Break Inside Containment
- **USNRC is concerning the operator-I&C systems interaction issue.**

II. Software Fault Tree Analysis (1/8)

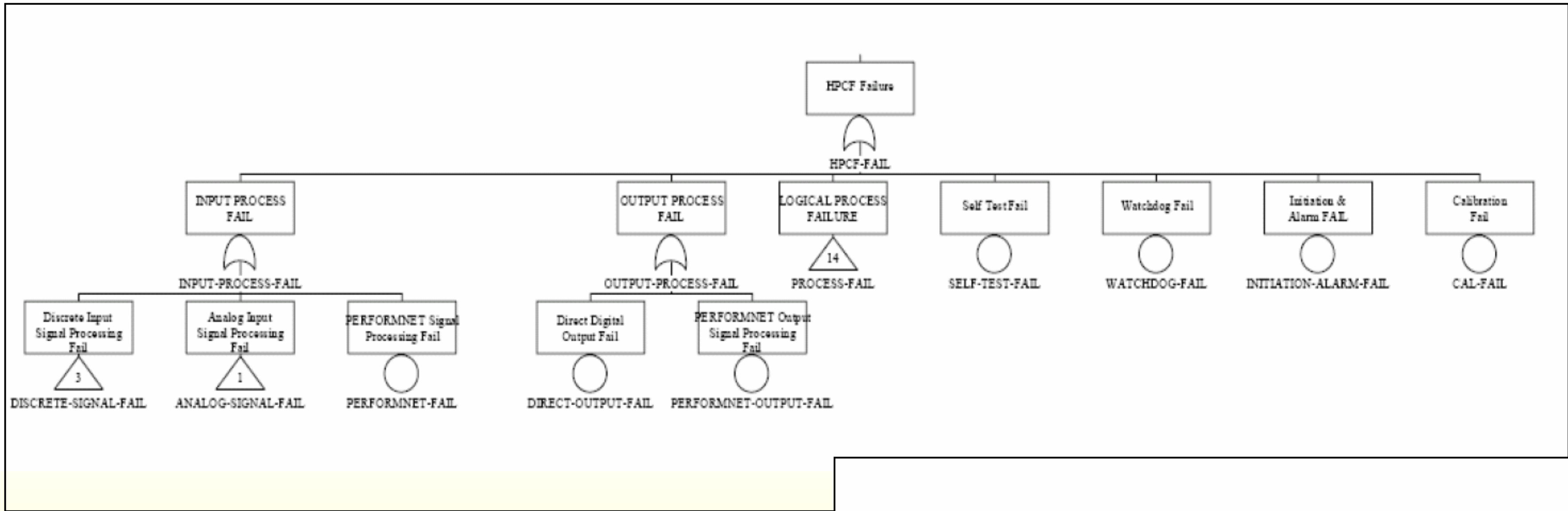
Software development life cycle							
Planning phase	Requirement phase	Design phase	Coding phase	Integration phase	Validation phase	Installation phase	Operation and Maintenance phase

Study HPCF software requirement specifications

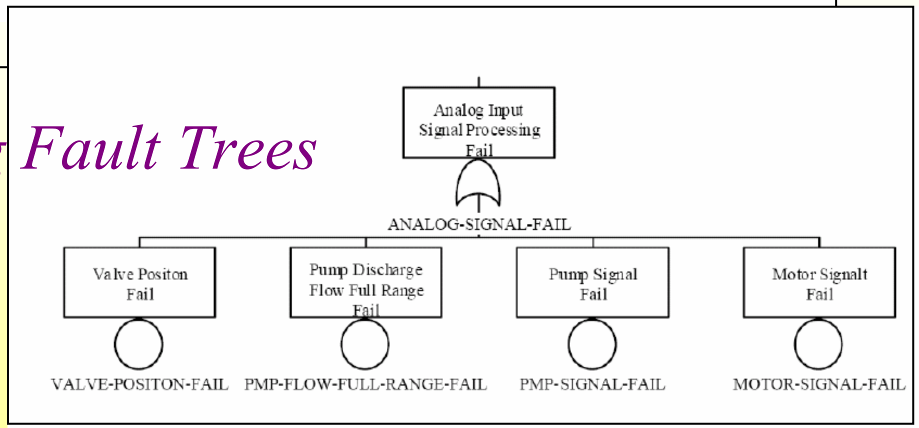


II. Software Fault Tree Analysis (2/8)

Software HPCF requirement fault trees

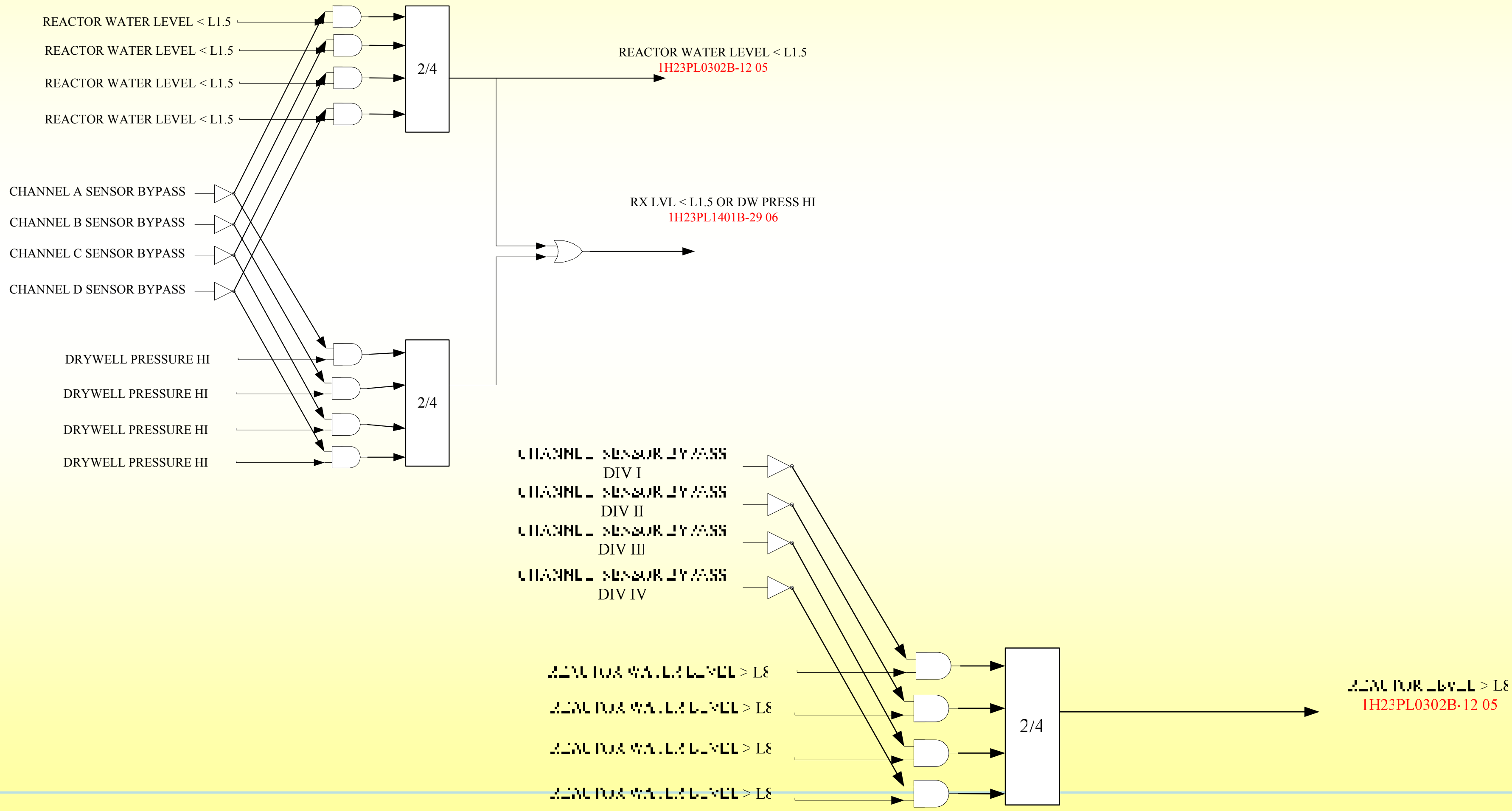


Traditional Analog Fault Trees



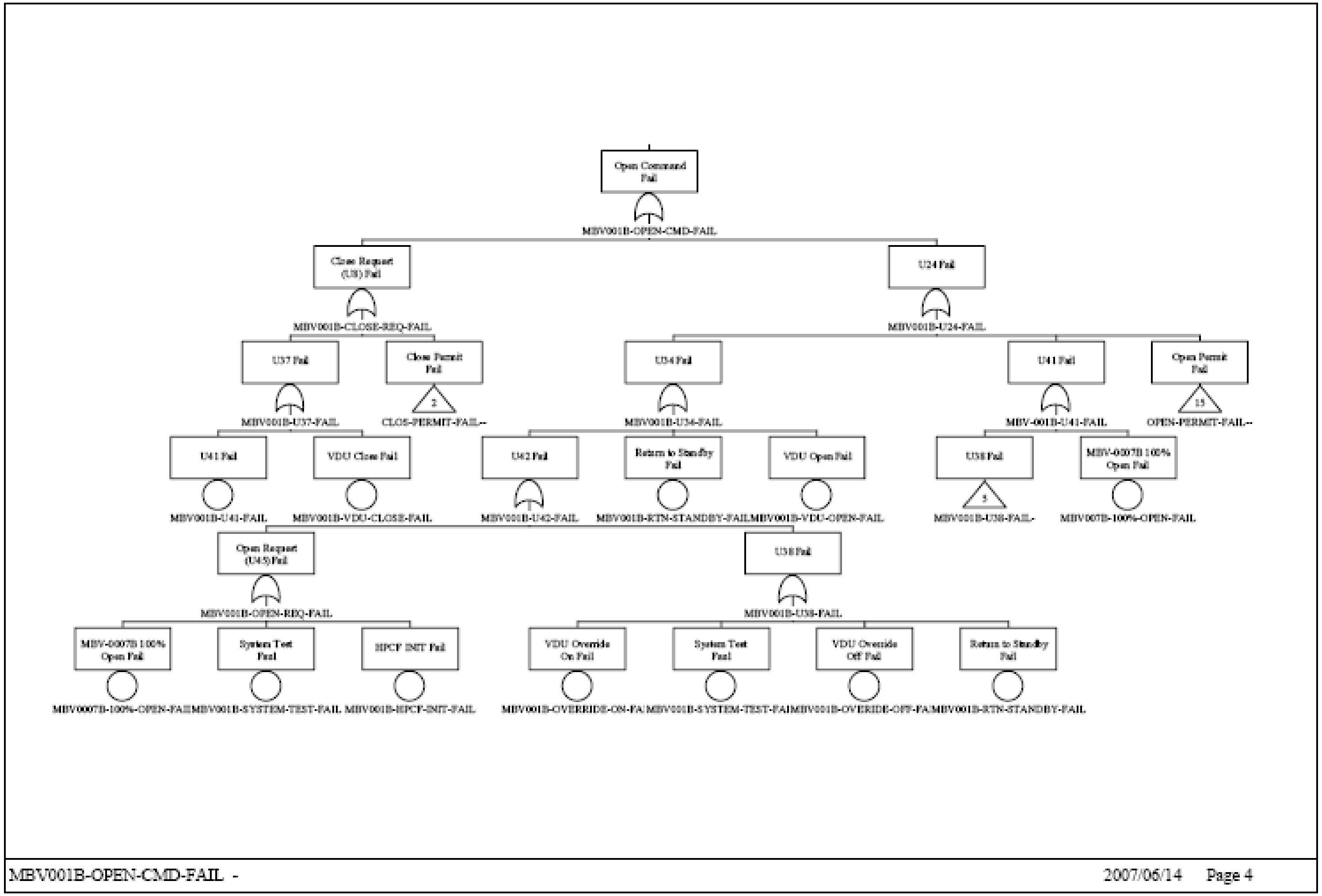
II. Software Fault Tree Analysis (3/8)

Study HPCF software design specifications



II. Software Fault Tree Analysis (4/8)

Software HPCF Design Fault Tree (Example)



II. Software Fault Tree Analysis (5/8)

- **Software Fault Tree**
  - can clarify the software failure structure for a digital I&C system
  - cannot describe the interactions and affects among the systems
- **Sequence Tree Method and Simulator Based Analysis are required to further identify the hazards induced by interactions among the I&C systems and operator manual actions**

II. Software Fault Tree Analysis (6/8)

- USNRC (BTP-19), Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, has identified four echelons of defense against software common-mode failures:
  - Control system
  - Reactor Trip System (RTS)
  - Engineered Safety Features Actuation System (ESFAS)
  - Monitoring and Indicators

III. Sequence Tree Method (7/8)

IEEE Std 1228-1994 Software Safety Plan

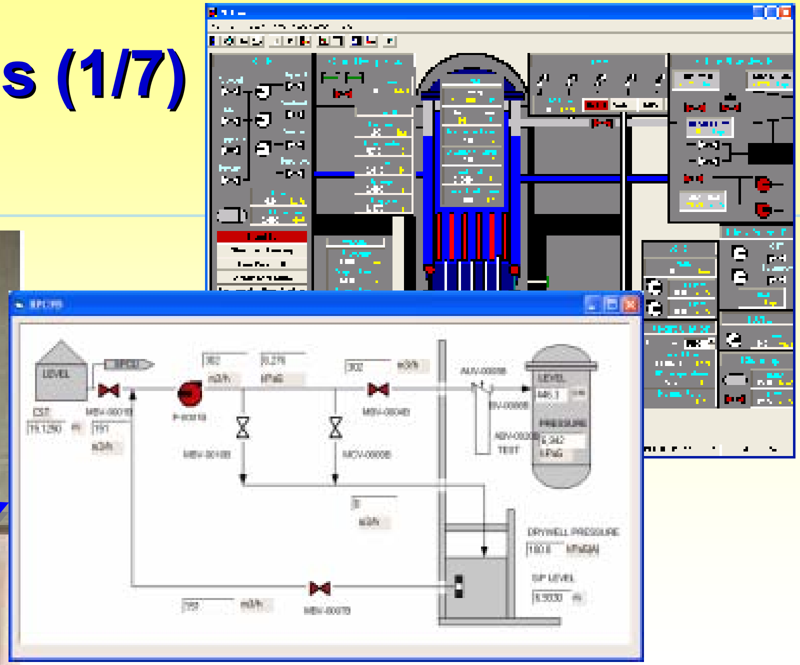
A Preliminary Hazard Analysis (PHA) and any additional hazard analyses performed on the entire system or any portion of the system that identifies

1) Hazardous system states
2) Sequences of actions that can cause the system to enter a hazardous state
3) Sequences of actions intended to return the system from a hazardous state to a nonhazardous state
4) Actions intended to mitigate the consequences of accidents

III. Sequence Tree Method (8/8)

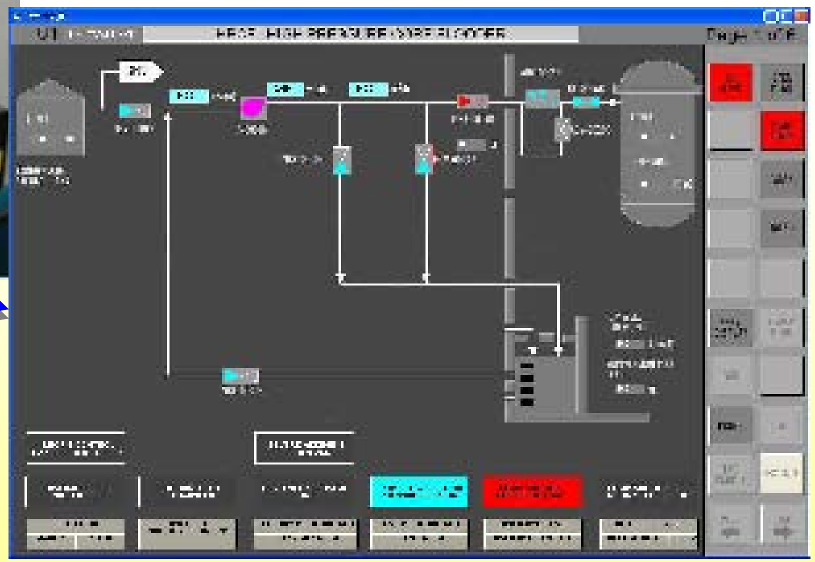
- **Sequence Tree Method**
  - can describe the relationship between the operator manual action and the systems
  - cannot analyze the time dependent effect, e.g., the affect of manual action timing.
- **Simulator Based Analysis is necessary to clarify the latest allowable time for ECCS manual initiation.**

IV. Simulator Based Analysis (1/7)



PCTran-ABWR Plant Simulation Code

Software Fault Injection Facility



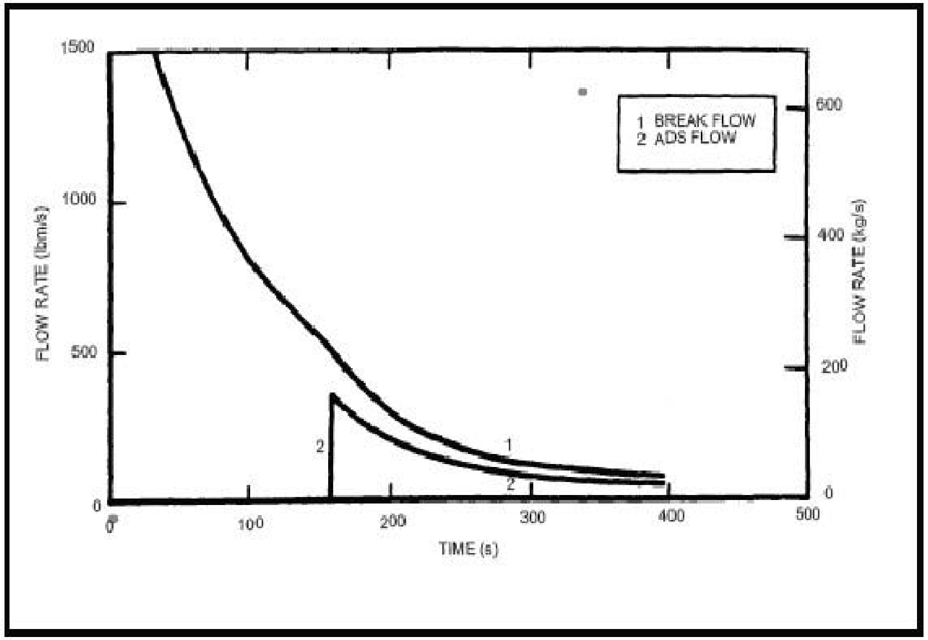
Video Display Unit of
High Pressure Core Flooder

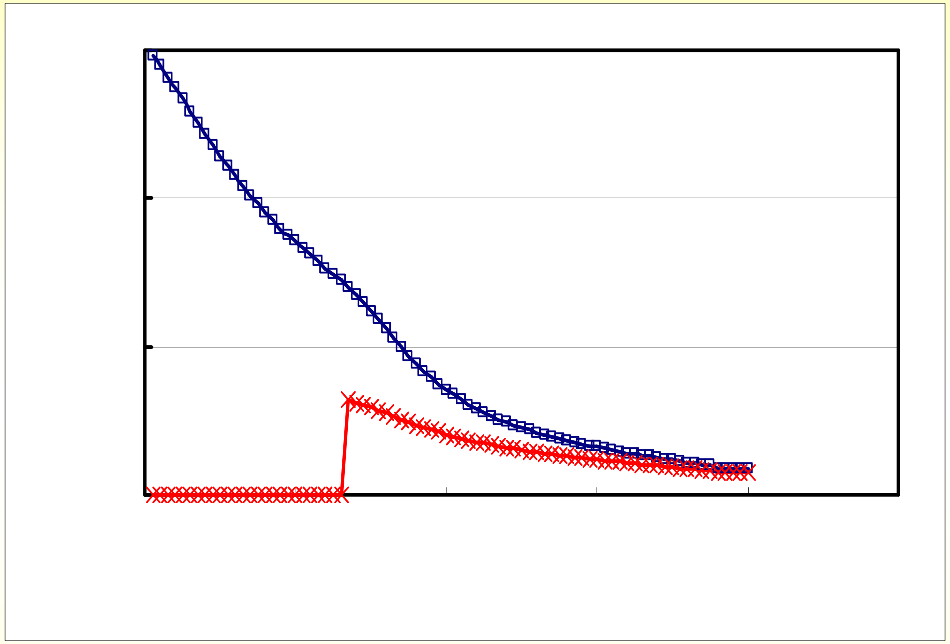
IV. Simulator Based Analysis (2/7)

Initiation condition and flow rate of each ECCS system

	Initiation condition of low Rx water level	Initiation condition of high drywell pressure	Core Injection flow rate (m^3/h)	Numbers (Trains)
RCIC	Level 2 233.2 cm above TAF	0.014 MPaG	182 High pressure core Injection	1
HPCF	Level 1.5 88.5 cm above TAF	0.014 MPaG	182 to 727 High pressure core Injection	2
ADS	Level 1 5.1 cm above TAF	0.014 MPaG	-	8
RHR/LPFL	Level 1 5.1 cm above TAF	0.014 MPaG	954 Low pressure core Injection	3

IV. Simulator Based Analysis (3/7)





PSAR-LOCA, Steam Line Break Inside Containment- break flow and ADS flow