A. JAMES CLARK
SCHOOL OF ENGINEERING

FRAMEWORK FOR ASSESSING INTEGRATED SITE RISK OF SMALL MODULAR REACTORS USING DYNAMIC PROBABILISTIC RISK ASSESSMENT SIMULATION

Mohammad Modarres
Nicole Y. Kim Eminent Professor of Engineering




ESREL 2015
Zürich, Switzerland

September 9, 2015

A. JAMES CLARK
SCHOOL OF ENGINEERING

Outline

- Motivation and objective
- Dynamic multi-unit PRA (MUPRA) methodology
- Hardware reliability analysis
- Simulation tool development

A. JAMES CLARK
SCHOOL OF ENGINEERING

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 2012 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].

A. JAMES CLARK
SCHOOL OF ENGINEERING

Purpose

Today

- 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]

→

Tomorrow

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

Objective

- Develop dynamic MUPRA (D-MUPRA) framework
- Enhance the current simulation tools for D-MUPRA
- Establish a framework for system dependency classification and assessment of *relative site risk*
- Apply the D-MUPRA framework and tools to a multi-module concept

A. JAMES CLARK
SCHOOL OF ENGINEERING

Probabilistic Estimation of Dependencies

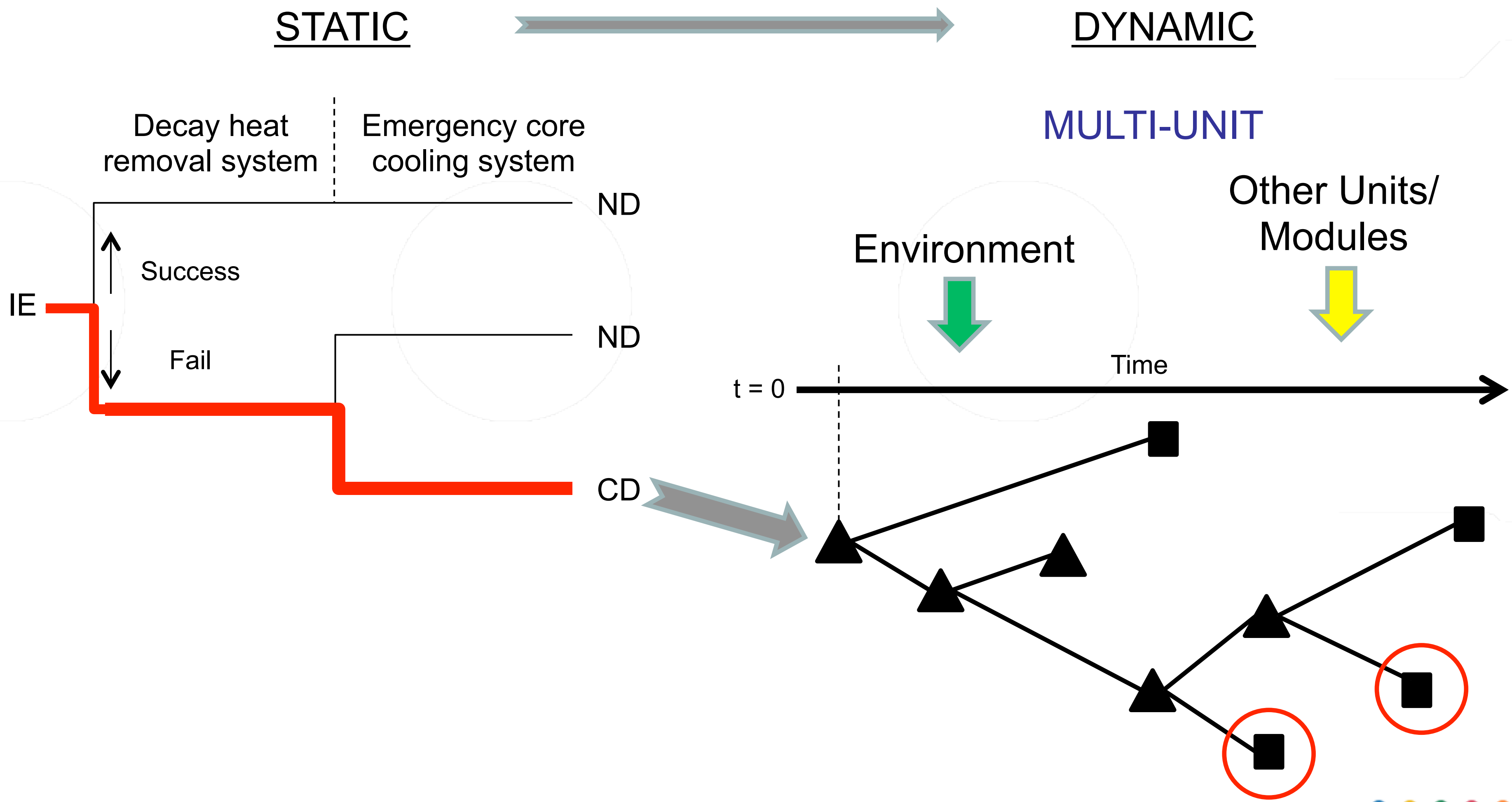
- Assume events $CD_1,\ldots,CD_n$ represent random variables describing the "events of a core damage" in units 1 to n.
- Site CDF as summation of individual unit CD_i's: *Expressed as either:*
  - *marginal CDF* for *all* conditions in the other unit(s)
  - *conditional* CDF of a unit, given a condition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

A. JAMES CLARK
SCHOOL OF ENGINEERING

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. Expand fault trees to include dependencies
7. Develop ADS-IDAC 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 D-MUPRA accident sequences

Expansion of static PRA accident sequences



Base PRA Usage – System Identification

Dedicated and Shared Systems

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

Dependency Classification Matrix

Accident Sequence Classifications	Definition	Potential Systems Belonging to Classification
Initiating Events	Single events that have the capacity to affect multiple units	Loss of Offsite Power, Loss of Ultimate Heat Sink, seismic event (including seismically-induced tsunami), external fire, external flood, hurricane, high wind, extreme temperature
Shared Connections	Links that physically connect SSCs of multiple units	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
Identical Components	Components with same design, operations or operating environment	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
Proximity Dependencies	A single environment has the potential to affect multiple units	Reactors, ultimate heat sink, containment, non-safety DC electrical and essential AC distribution system, control room HVAC
Human Dependencies	A person's interaction with a machine affects multiple units	Shared control room, operator staffing more than one reactor
Organizational Dependencies	Connection through multiple units typically by a logic error that permeates the organization	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

A. JAMES CLARK
SCHOOL OF ENGINEERING

D-MUPRA Analyses

- 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 will inform 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

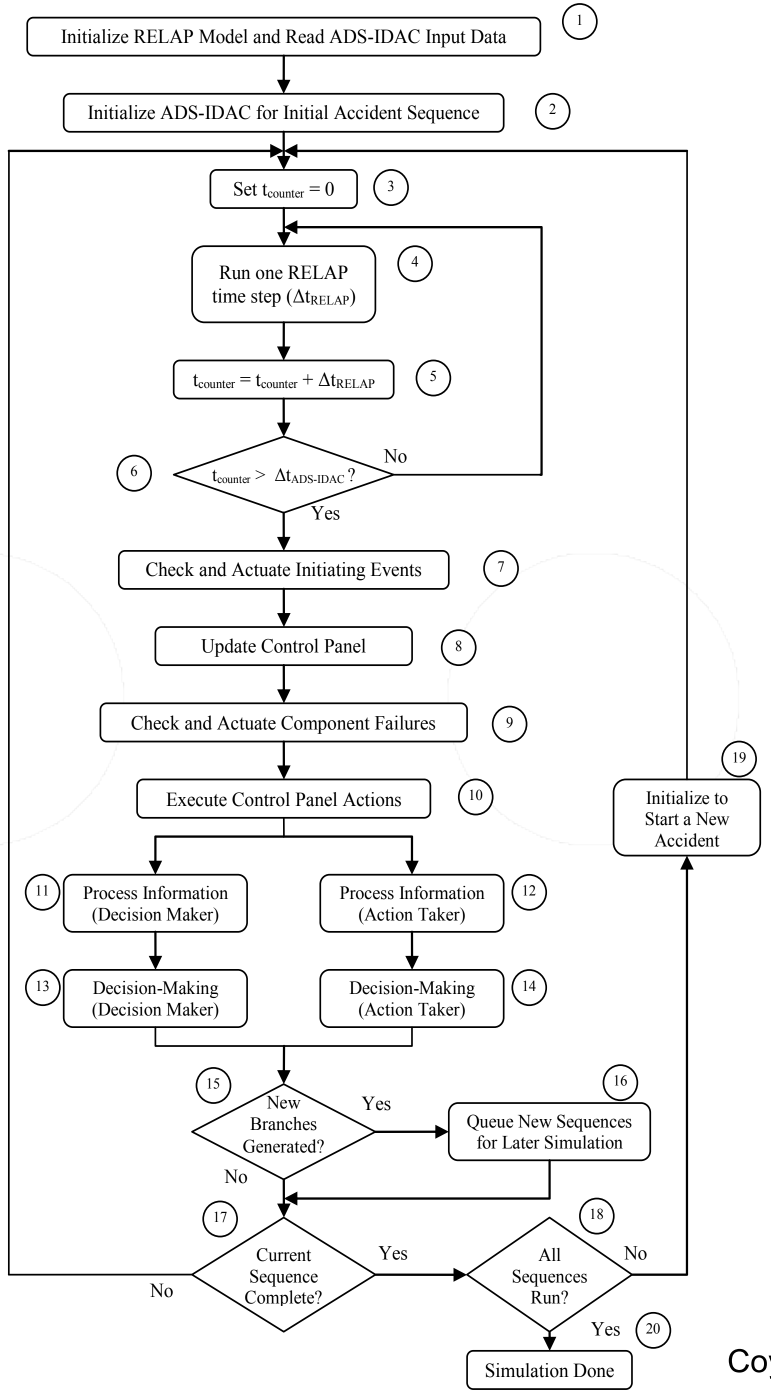
A. JAMES CLARK
SCHOOL OF ENGINEERING

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

A. JAMES CLARK
SCHOOL OF ENGINEERING

ADS-IDAC Process Overview



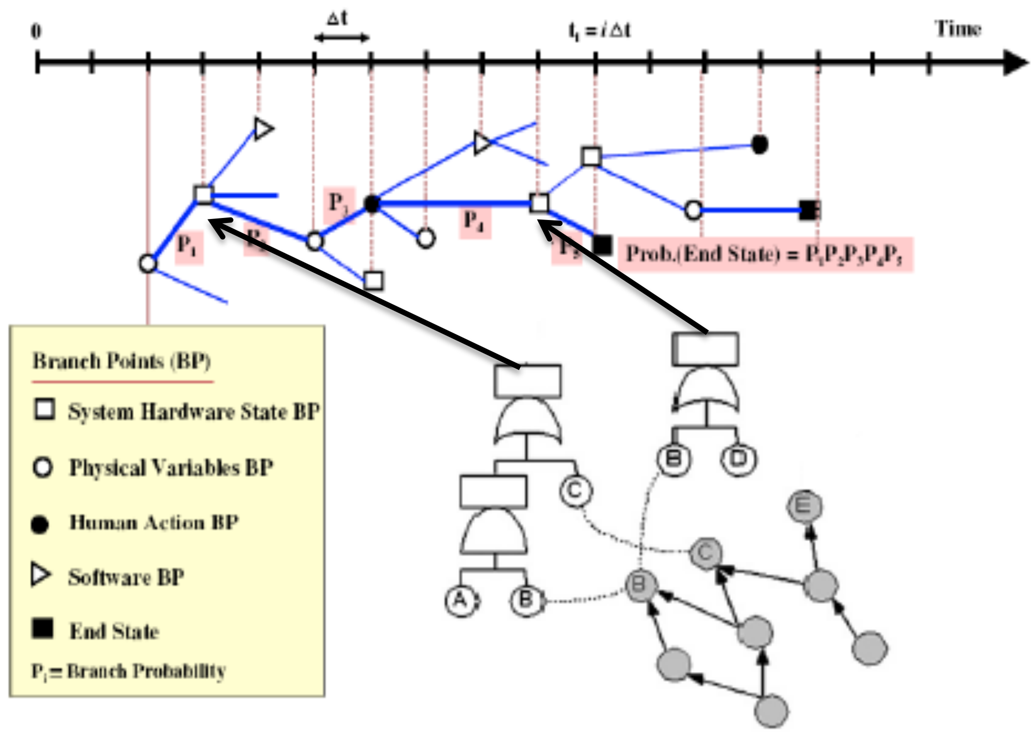
Coyne, 2008

Current Hardware Reliability Model

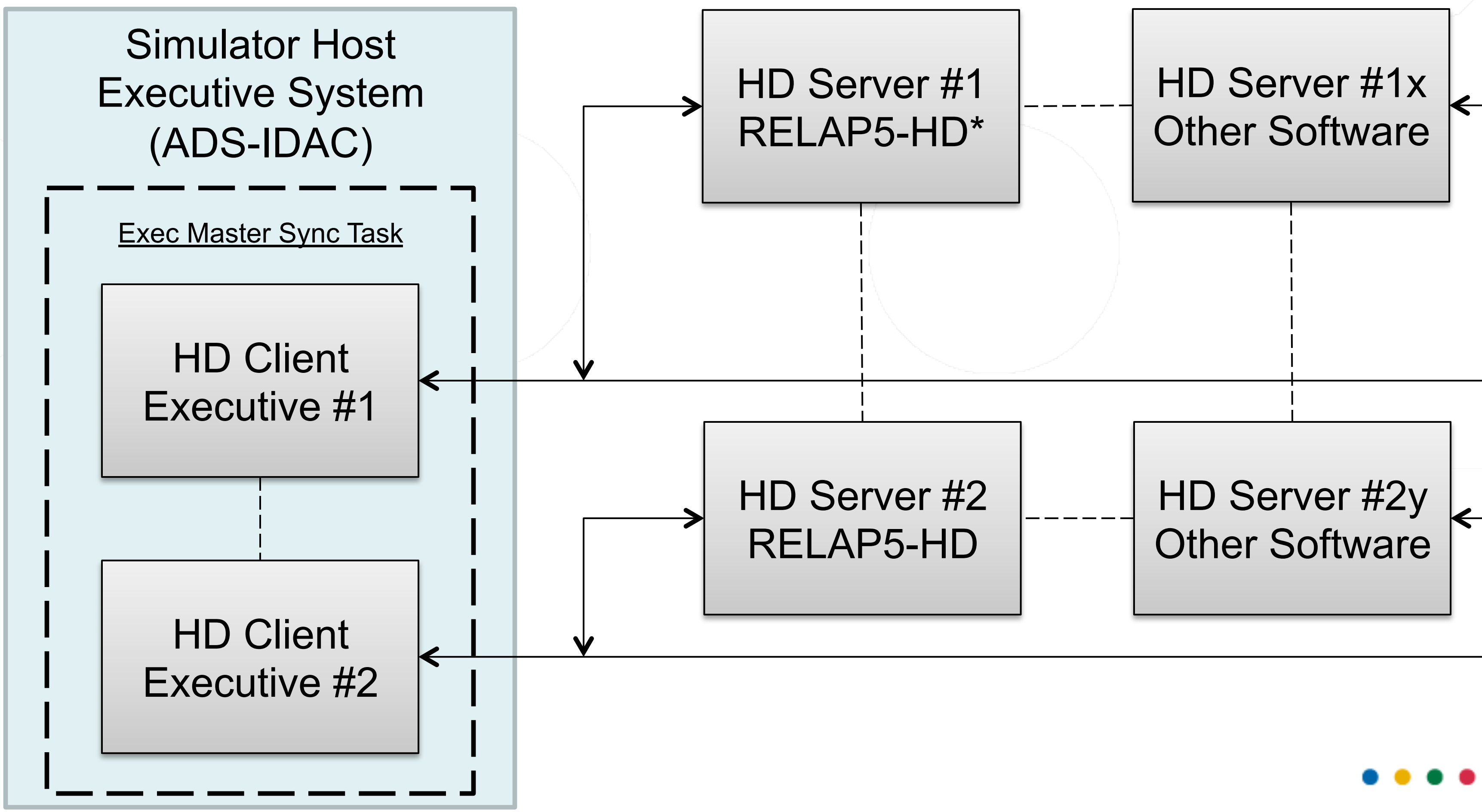
- Time dependent failures occur at a prescribed time during the simulation evolution--used to reflect hardware failures (e.g., pump or valve failure at time *t*) or an accident initiating event.
- Conditional failures occur when a component changes operating state to a pre-selected target value, thereby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

Enhancing Hardware Reliability Analysis

- Hybrid Causal Logic Dynamic PRA
- Mimic traditional fault tree analysis
- Integrates fault tree and Bayesian belief network from into the discrete dynamic event tree



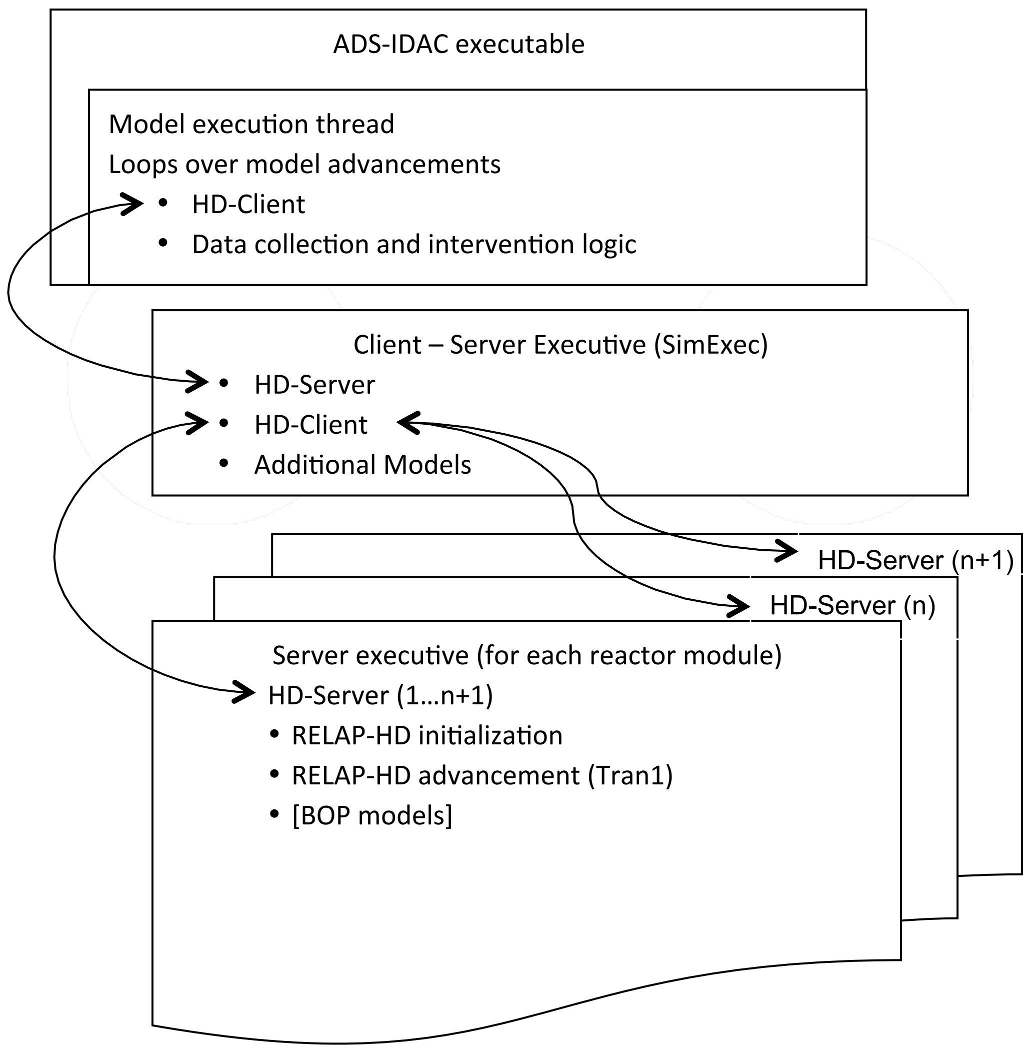
Thermal-Hydraulic Model Improvement



*(GSE, 2013)

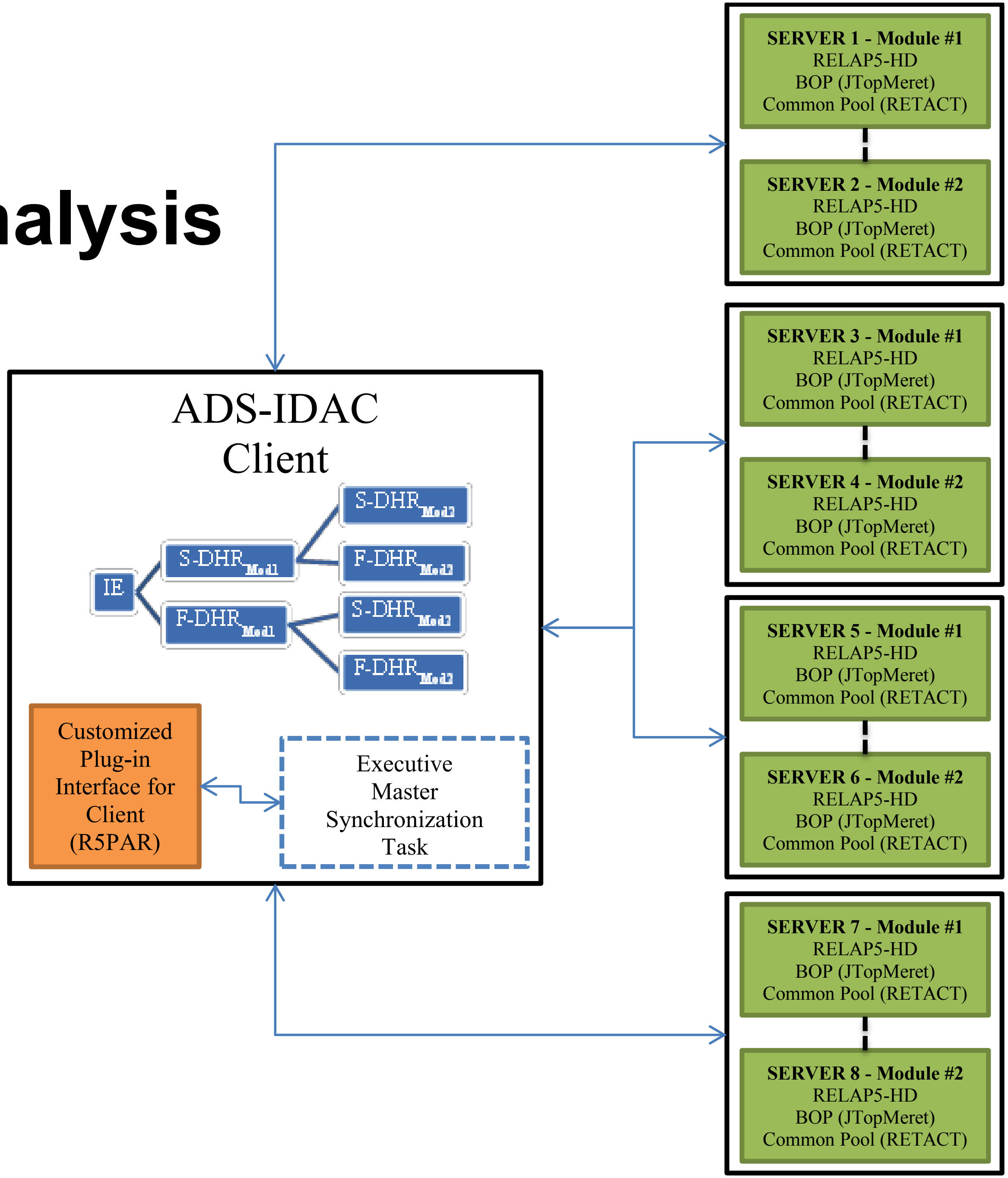
A. JAMES CLARK
SCHOOL OF ENGINEERING

ADS-IDAC Multi-Unit Data Flow



Event Tree Analysis

- Fault tree linking
- Marginal event tree for one unit
- Conditional event tree for more than one unit



Exploratory, stylized accident sequences

Initiating Event	Top Events				
Seismically-induced loss of offsite power with degraded ultimate heat sink	Safety DC Electrical	Reactor Protection System	Chemical Volume and Control System	Decay Heat Removal System	Emergency Core Cooling System
Seismically-induced LOCA (CVCS inside containment) with degraded Decay Heat Removal System	Safety DC Electrical	Reactor Protection System	Decay Heat Removal System	Emergency Core Cooling System	--
External flood with loss of offsite power	Safety DC Electrical	Reactor Protection System	Chemical Volume and Control System	Decay Heat Removal System	Emergency Core Cooling System

Research Summary

Simulation

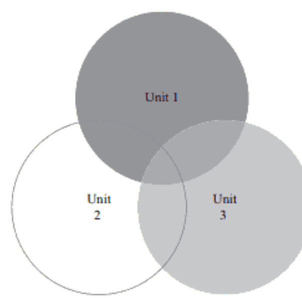
- Dynamic PRA code enhancement
- RELAP5 update
- T-H plant model development

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

A. JAMES CLARK
SCHOOL OF ENGINEERING

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.