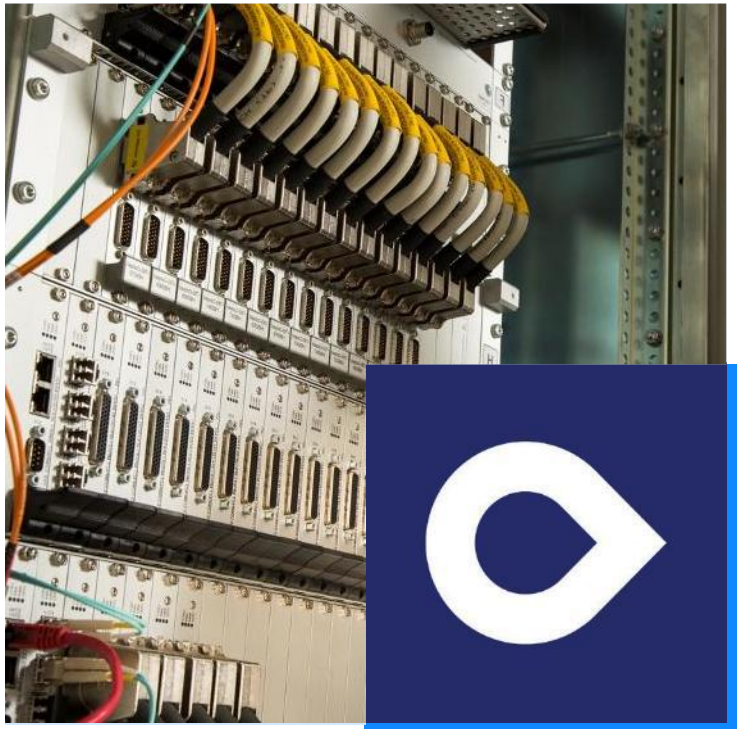
framatome



Simulation-Based Probabilistic Reliability Techniques for Complex Nuclear Safety Systems

Taha ABDELNAEEM, I&C Solution Lead

Confidentiality

X ⚠ Check the boxes corresponding to the document's confidentiality level and indicate the applicable export control markings.

☐ **This document contains *Framatome's know-how***
When the box is checked, add the information in the 'Footer'

Export Control COEDM

EU EC country code = XX marking code = N	US EC marking code = N	OTH EC country code = XX marking code= N

Goods marked EU EC different to "N" are subject to export authorization of the States members of the European Union (EU) in case of export outside EU, and also for certain sensitive goods (e. g. goods marked "EU EC": "0E001") in case of transfer within UE ; they cannot be reexported nor transferred back without a prior agreement from the State of the first export. Goods marked US EC different to "N" are subject to export, re-export or transfer authorization of the United States of America. Goods marked OTH EC (country code(s)) different to "N" are subject to export, re-export or transfer authorization of the mentioned county(ies). Even for goods marked "EU EC: N" and "US EC: N" and "OTH EC: N", an export authorization may be required depending on their final destination or end-use.

Export Control Other

AL = N	ECCN = N

Goods labeled with "AL not equal to N" are subject to European or German export authorization when being exported within or out of the EU.
Goods labeled with "ECCN not equal to N or EAR99" are subject to U.S. reexport authorization. Even without a label, or with label: "AL: N" or "ECCN: N" or "ECCN: EAR99," authorization may be required due to the final whereabouts and purpose for which the goods are to be used.

Framatome's information protection rules

☐ **C1 :** This document and any and all information contained therein and/or disclosed in discussions supported by this document are **restricted**.

X **C2 :** This document and any and all information contained therein and/or disclosed in discussions supported by this document are sensitive and **Framatome confidential,** such as its disclosure, alteration or loss are detrimental with a significant-to-high impact for Framatome.

The document, if disclosed, and any information it contains are intended for the sole attendees. The disclosure or reference to such information or document shall be made only on a proper judgment basis and by mentioning expressly "this information shall not be disclosed / transferred without prior consent".

☐ **C3 :** This document and any and all information contained therein and/or disclosed in discussions supported by this document are classified **Framatome Secret**. **Each one must commit to keep secret any written or oral information disclosed during the meeting. It is forbidden to disclose it to any legal entity and any individual (including within Framatome) without prior consent of the meeting chairman.**

Dissemination scope: specify a perimeter as narrow as possible.

Content

framatome

1.

The Need for Dynamic PRA

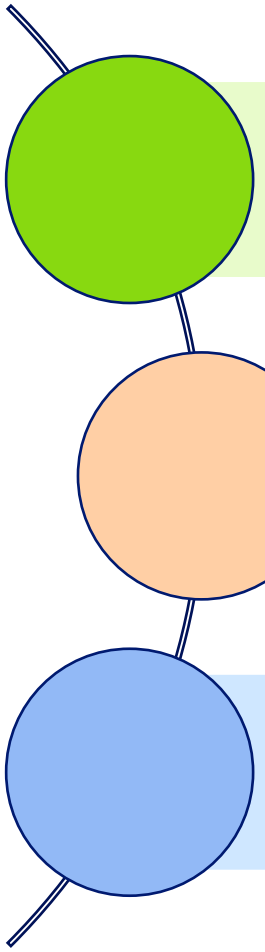
framatome

The Need for Dynamic PRA

Probabilistic Risk Assessment (PRA): Lessons from NUREG-1150

Key takeaway:
Today's highly integrated digital I&C systems introduce dynamic interactions, software behavior, diagnostics, communication networks, and time-dependent dependencies that motivate the use of **simulation-based probabilistic reliability techniques** to complement traditional PRA approaches.

We will discuss techniques that accurately represent, under a **dynamic event tree** (DET) structure, detailed evolutions of transient events without restrictions placed on preselected groups of events.



PRA integrates Fault Trees (FTs) and Event Trees (ETs) to systematically model initiating events, system failures, accident progression, and their associated risk for nuclear power plants.

NUREG-1150 represented one of the first comprehensive Level 1–3 PRA studies, evaluating severe accident risks for **five U.S. commercial nuclear power plants** and establishing many of the methodologies still used in modern PRA.

Due to the **large number of initiating events and accident sequences**, NUREG-1150 organized accident scenarios into representative **Plant Damage States (PDSs)**, **Accident Progression Bins (APBs)**, and **Source Term Groups (STGs)**, significantly reducing computational complexity while preserving essential accident characteristics.

framatome

2.

Basic Features of Discrete Dynamic Event Tree Analysis

framatome

Basic Features of Discrete Dynamic Event Tree Analysis

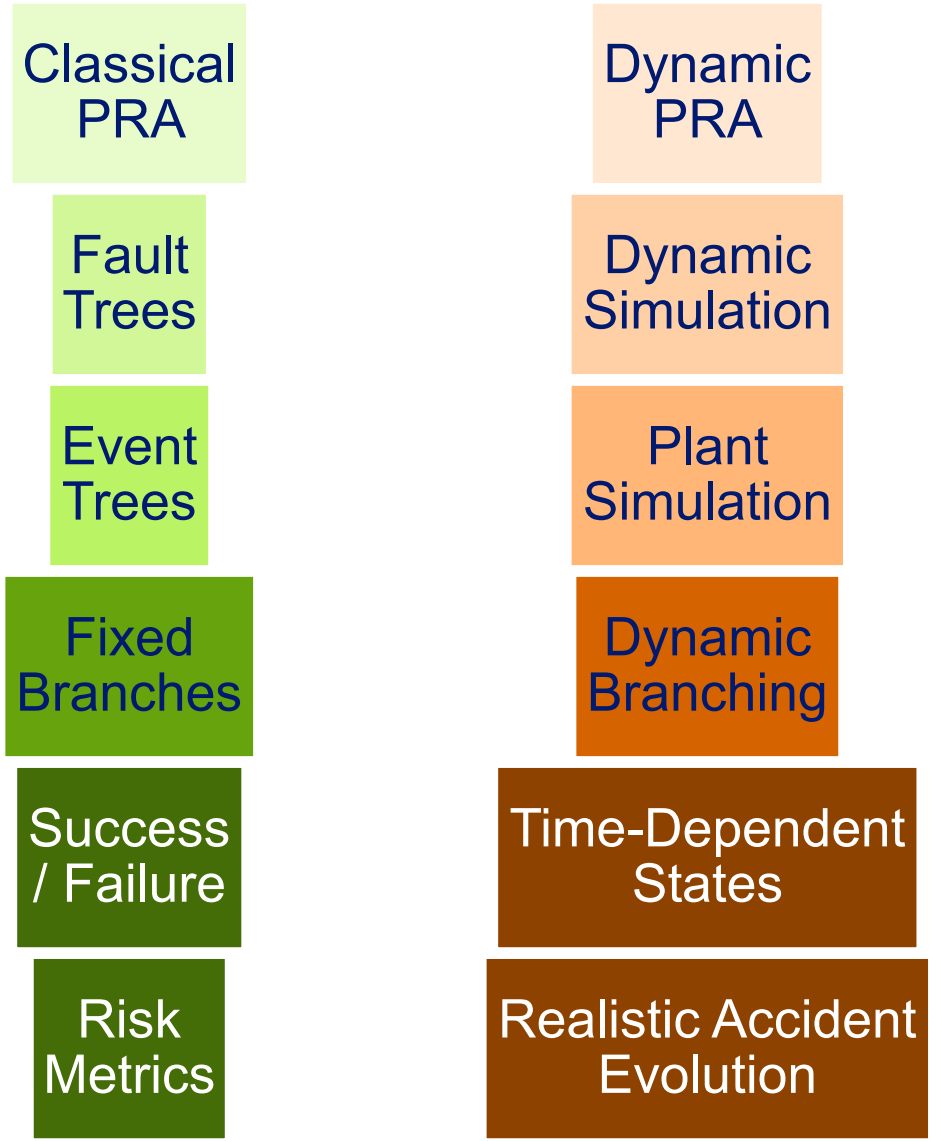
Why Was Dynamic PRA Needed?

- **Traditional PRA (FT/ET)** provides a structured and efficient framework for nuclear risk assessment.
- **NUREG-1150** demonstrated the effectiveness of PRA for evaluating severe accident risk using representative Event Trees and probabilistic sampling.
- Modern digital safety systems introduce **dynamic interactions** that are difficult to capture using static analytical models.

Limitations of Classical PRA

- Static event tree structure
- Binary success/failure modeling
- Fixed branching times
- Limited representation of operator actions
- Simplified treatment of dynamic system behavior

Dynamic simulation complements traditional PRA by capturing time-dependent interactions, equipment degradation, operator actions, and complex dependencies that are difficult to represent using conventional Fault Tree and Event Tree methods.



framatome

Basic Features of Discrete Dynamic Event Tree Analysis

Dynamic Event Tree (DET) Advantages

Dynamic Event Tree methods enhance traditional PRA by replacing fixed accident sequences with simulation-driven accident evolution, providing a more realistic representation of complex nuclear safety systems.

Dynamic branching

Event Tree branches are generated **during the simulation** based on the evolving plant conditions, rather than at predefined branch points.

Realistic system behavior

Realistic system behavior: DET explicitly models **operator actions, equipment degradation, safety system actuation, and recovery actions** as the accident progresses.

Improved modeling fidelity

By simulating individual accident scenarios, DET captures **time-dependent interactions, dependent failures, and dynamic relationships** between component states and overall system behavior more accurately than traditional Event Trees.

framatome

Basic Features of Discrete Dynamic Event Tree Analysis

Dynamic Event Tree Analysis: Time-Dependent Accident Evolution

Illustrative Example: Loss-of-Flow Accident (Sodium-Cooled Fast Reactor)

- **Initiating Event:** Pump coastdown reduces core coolant flow (time constant ≈ **5.7 s**).
- **Dynamic Simulation:** Simultaneously models plant response, sensor failures, control logic, and scram system actions.
- **Multiple Accident Paths:** Accident progression depends on the **timing of equipment failures** and **operator/system responses**, resulting in different accident outcomes

In DET, accident evolution is determined dynamically by the simulated plant state—not by predefined Event Tree branches.

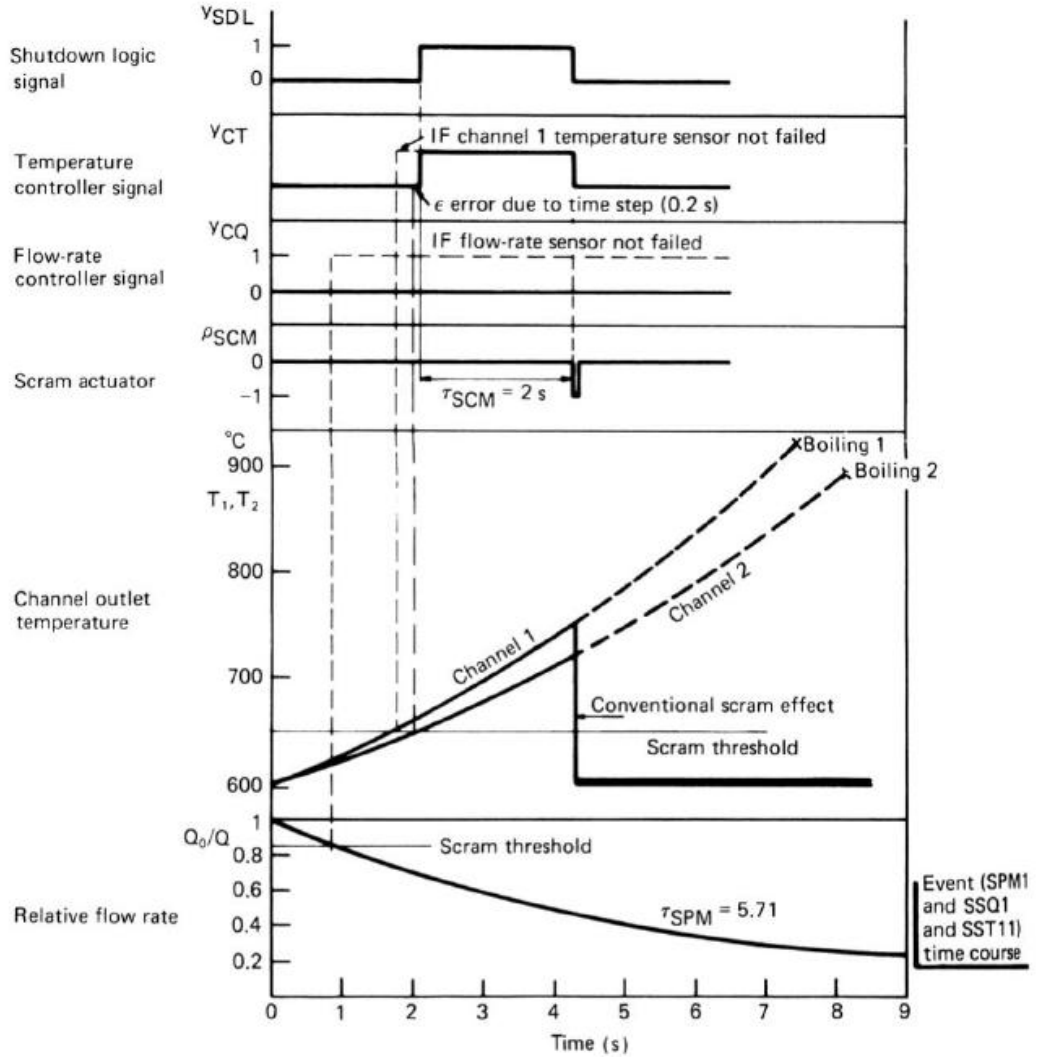
Dynamic Equipment States
- Sensor failures
- Control signals
- Scram logic
- Reactor protection actions

Continuous Plant Response
- Core outlet temperature
- Coolant flow rate
- Reactor reactivity

Multiple Possible Outcomes
- Successful reactor trip
- Delayed shutdown
- Fuel damage (if protection fails)

Why DET Is More Realistic

✓ Represents **continuous system evolution**
✓ Models **time-dependent failures and recoveries**
✓ Captures **dynamic interactions** between hardware, control systems, and plant behavior
✓ Generates **multiple accident trajectories** based on probabilistic events



Basic Features of Discrete Dynamic Event Tree Analysis

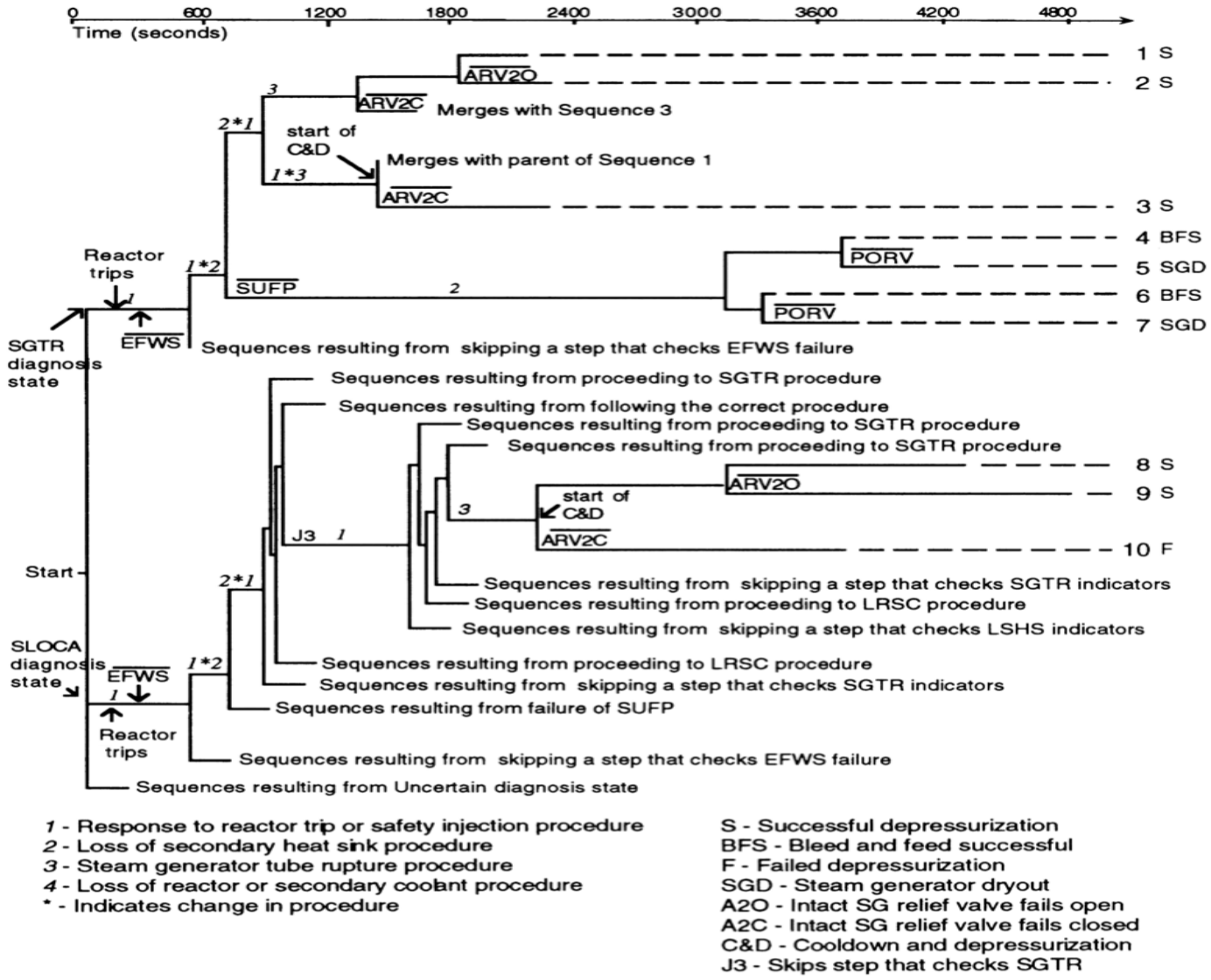
Dynamic Event Tree Analysis (DETAM): Modeling Operator Actions

Background

This example is based on a **Steam Generator Tube Rupture (SGTR)** accident in a **Pressurized Water Reactor (PWR)**.

SGTR was identified in **NUREG-1150** as one of the important contributors to **containment bypass sequences**, making it a suitable case study for demonstrating Dynamic Event Tree Analysis.

Unlike conventional PRA, DETAM explicitly models **operator diagnosis, decision-making, procedure execution, and timing** throughout the accident



framatome

Basic Features of Discrete Dynamic Event Tree Analysis

Dynamic Event Tree Analysis (DETAM): Modeling Operator Actions

1. Accident Initiation

The simulation begins with the **Start** node.

Two possible initiating conditions are considered:

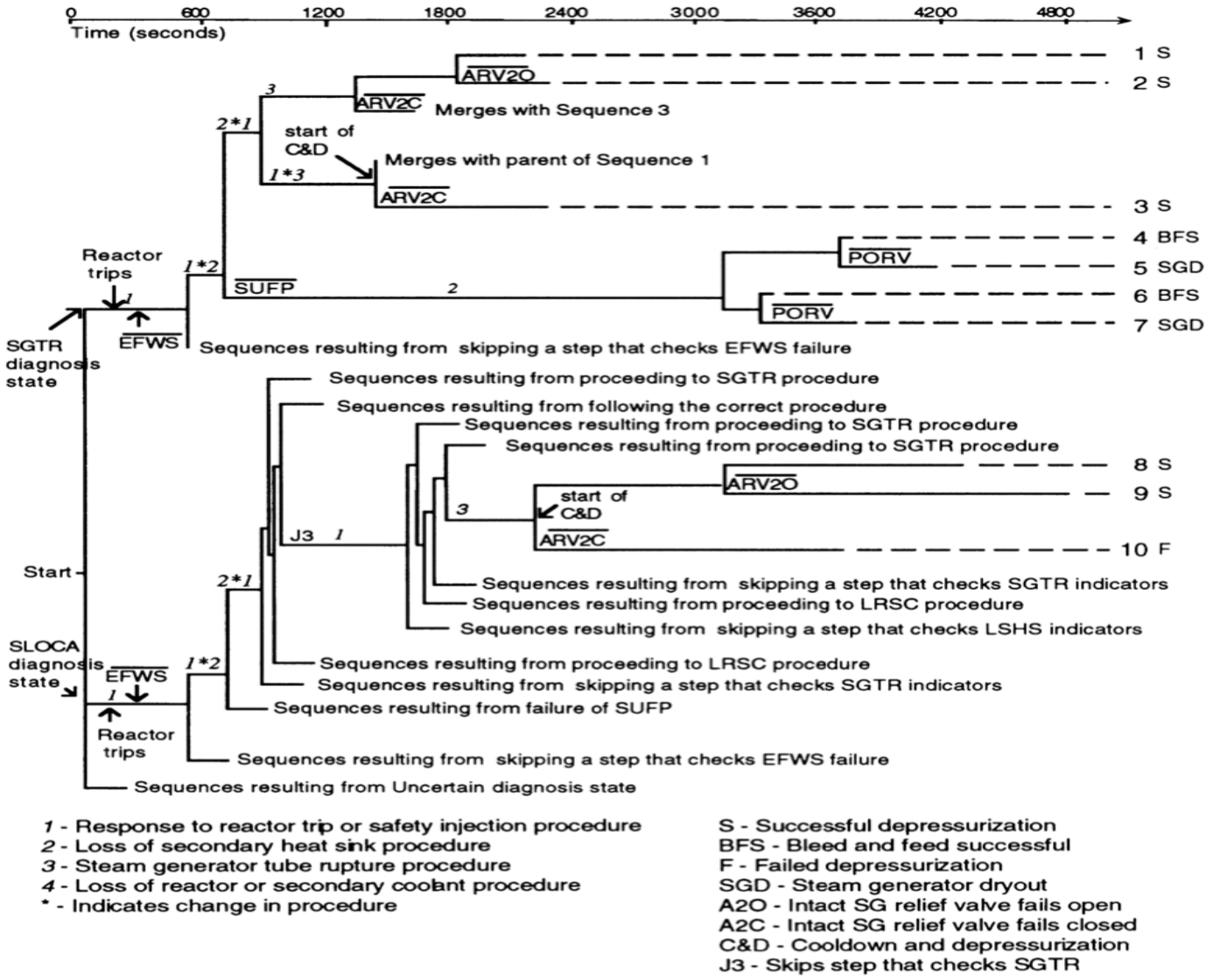
- **SGTR diagnosis state**
- **SLOCA (Small Loss-of-Coolant Accident) diagnosis state**

At this point, the operator has not yet correctly diagnosed the event.

The first challenge is:

Can the operator correctly identify what accident is occurring?

Incorrect diagnosis immediately changes the accident evolution.



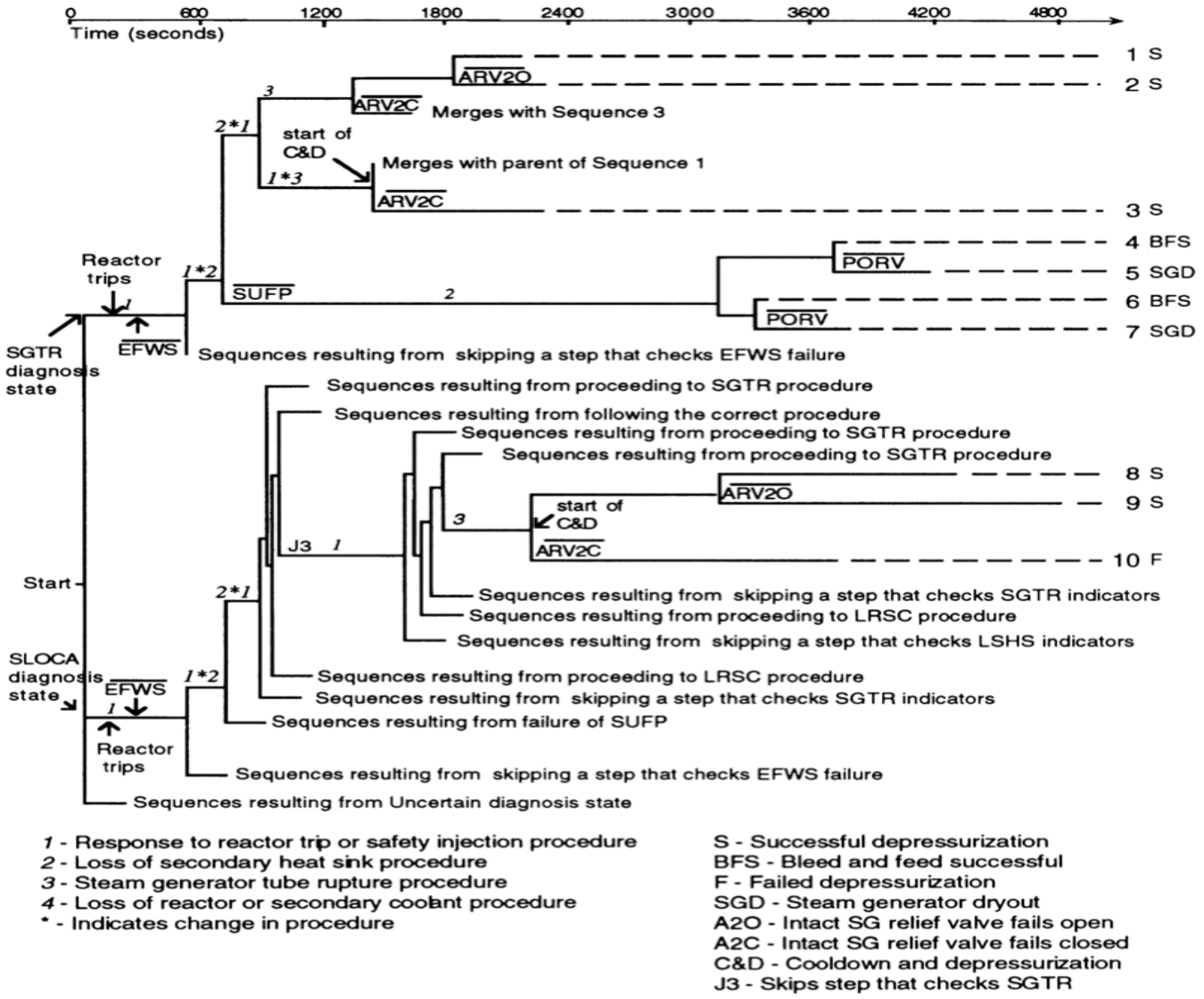
framatome

Basic Features of Discrete Dynamic Event Tree Analysis

Dynamic Event Tree Analysis (DETAM): Modeling Operator Actions

2. Reactor Trip
Once the event begins,
↓
The reactor automatically trips.
Immediately afterward,
operators begin executing Emergency Operating Procedures (EOPs).
This starts the sequence of operator decisions.

3. Emergency Feedwater System (EFWS)
One of the first operator decisions is related to the **Emergency Feedwater System (EFWS).**
Questions include:
•Did EFWS start correctly?
•Did the operator recognize EFWS failure?
•Was the proper recovery procedure followed?
Each answer creates a new branch.
Unlike classical Event Trees,
these branches occur
only when the operator reaches that decision point.



framatome

Basic Features of Discrete Dynamic Event Tree Analysis

Dynamic Event Tree Analysis: Time-Dependent Accident Evolution

NUREG-1150 recognized that **Steam Generator Tube Rupture (SGTR)** was an important contributor to containment bypass risk. However, traditional PRA represented operator actions with relatively simple event tree branches and fixed human error probabilities.

This example demonstrates that operator actions are dynamic processes, not single probabilistic events. Dynamic Event Tree Analysis explicitly models diagnosis, decision-making, procedure execution, recovery actions, and their timing, enabling a more realistic representation of human reliability and its impact on nuclear safety.

DETAM extended this approach by explicitly modeling the sequence and timing of operator actions throughout the accident. Instead of assigning a single probability to "operator success" or "operator failure," the analysis represented the evolving interaction between the plant, equipment, procedures, and operators, producing a much more realistic assessment of accident progression and risk.

framatome

3.

References

References

1- NUREG- 1150 Vol. 2 Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants
2- Risk and Safety Analysis of Nuclear Systems (RSANS) John C. Lee, Norman J. McCormick

framatome

Contacts

Taha ABDELNAEEM
taha-ibrahim.abdelnaeem@framatome.com