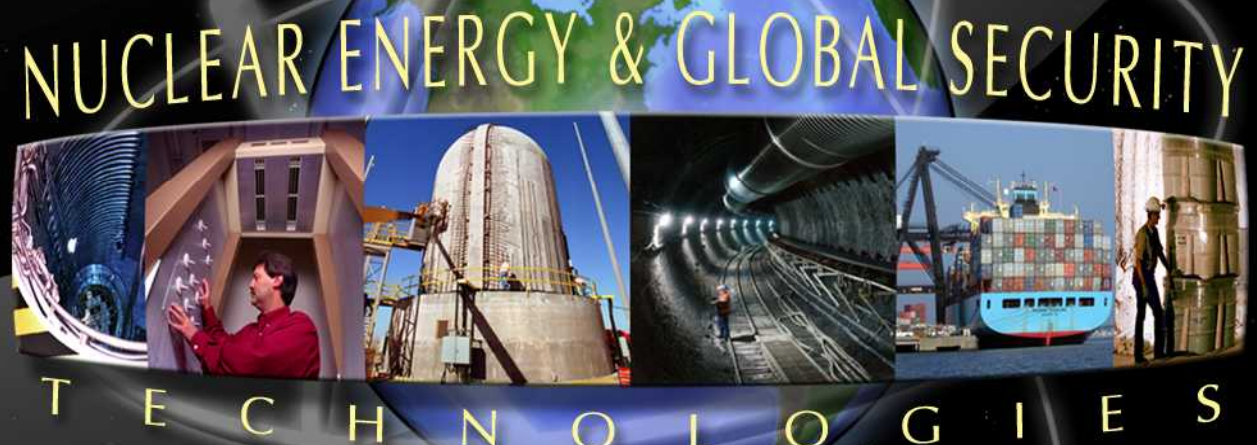
Lockheed Martin Corporation
Sandia National Laboratories

SAND2012-0894P

Probabilistic Safety Analysis

Shawn P. Burns, Manager Risk and Reliability Analysis
Sandia National Laboratories, spburns@sandia.gov



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration

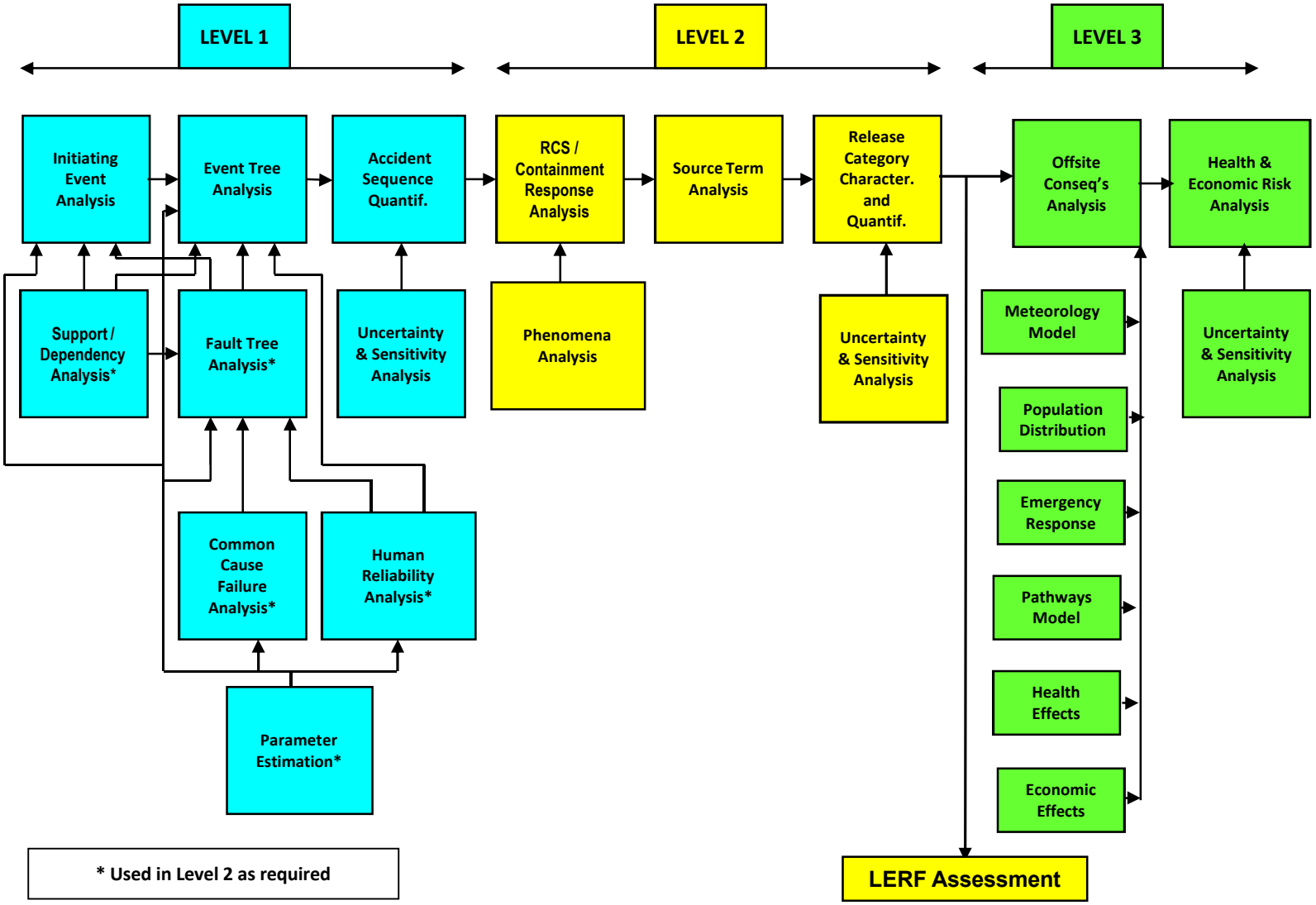
under contract DE-AC04-94AL85000

Table of Contents

- Accident sequence analysis
- Accident progression analysis
- Accident consequence analysis
- Path forward

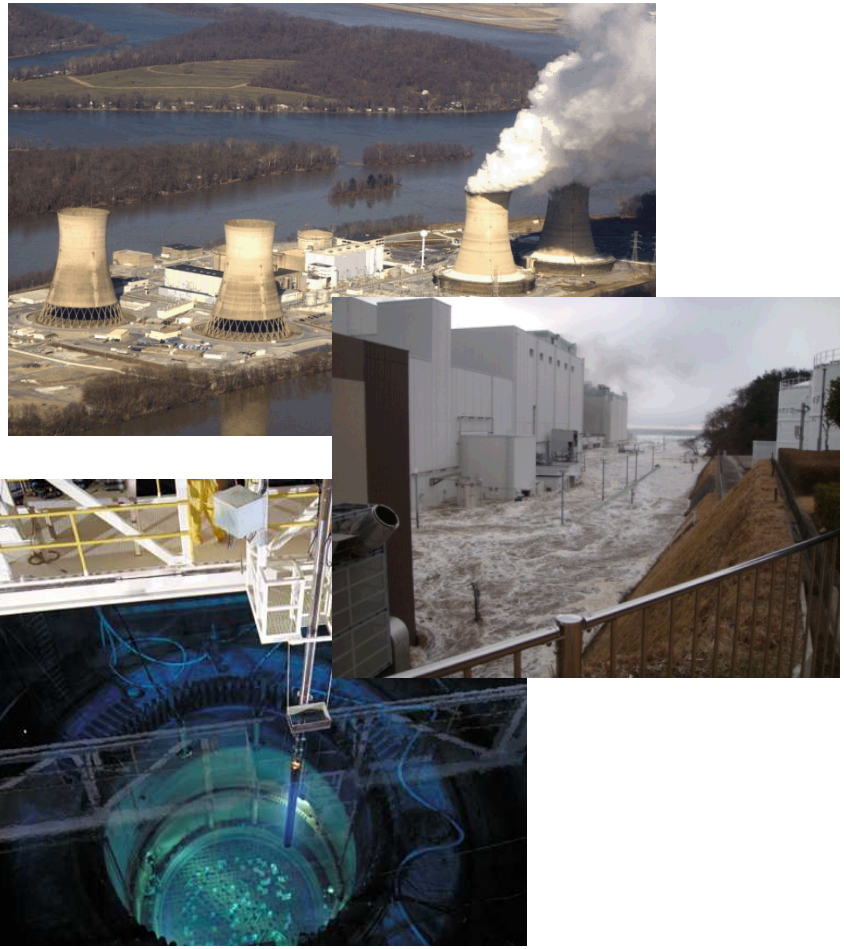
Sandia National Laboratories

Principal Steps in a Probabilistic Safety Analysis (PSA)

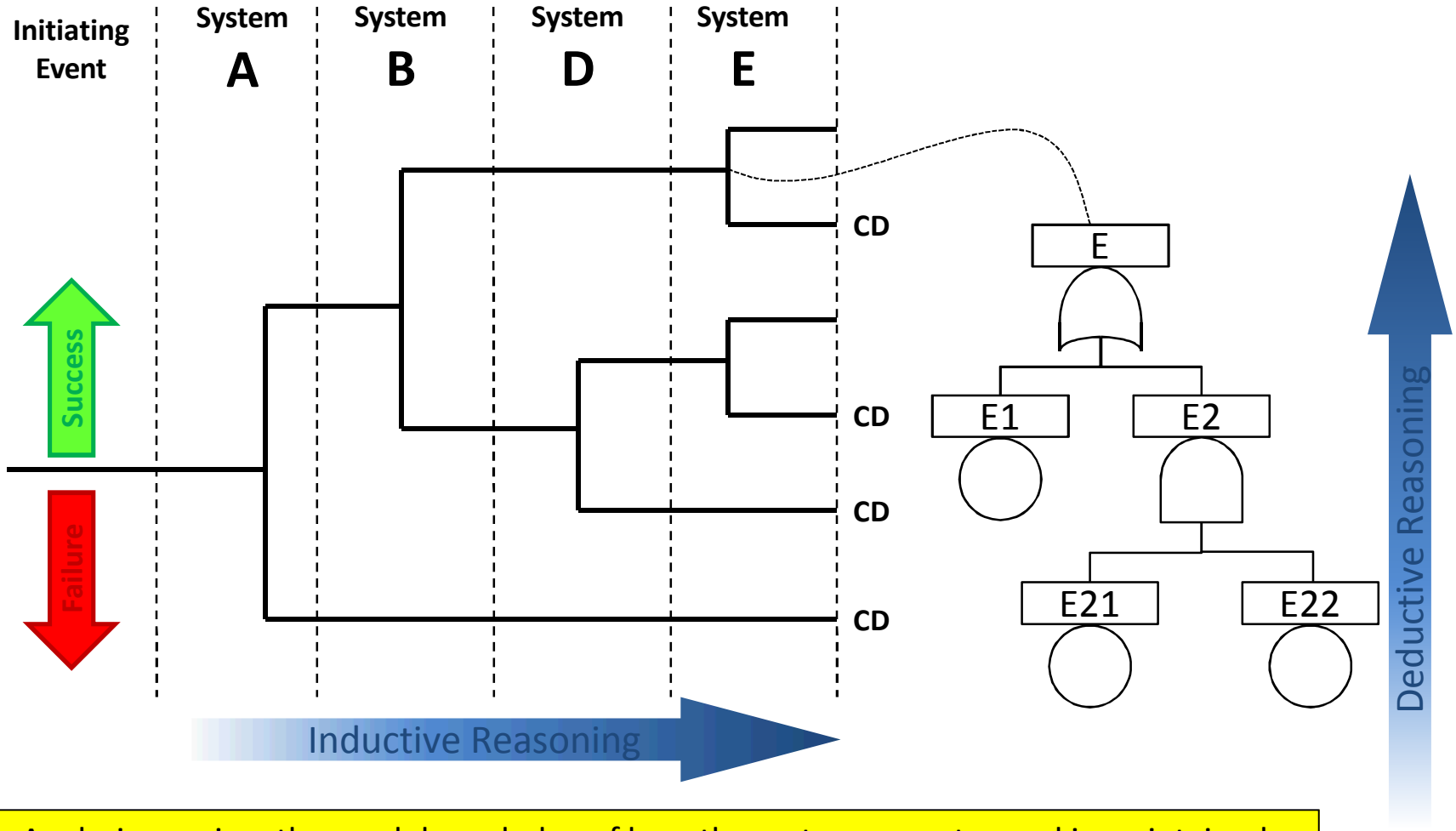


Types of Initiating Event

- Internal
  - Transients
  - Loss of coolant
  - Support system failures
  - Fire
- External
  - Seismic
  - Flood
  - Weather
- Operating State
  - Full power
  - Low power and shut down



Event Tree and Fault Tree Analysis

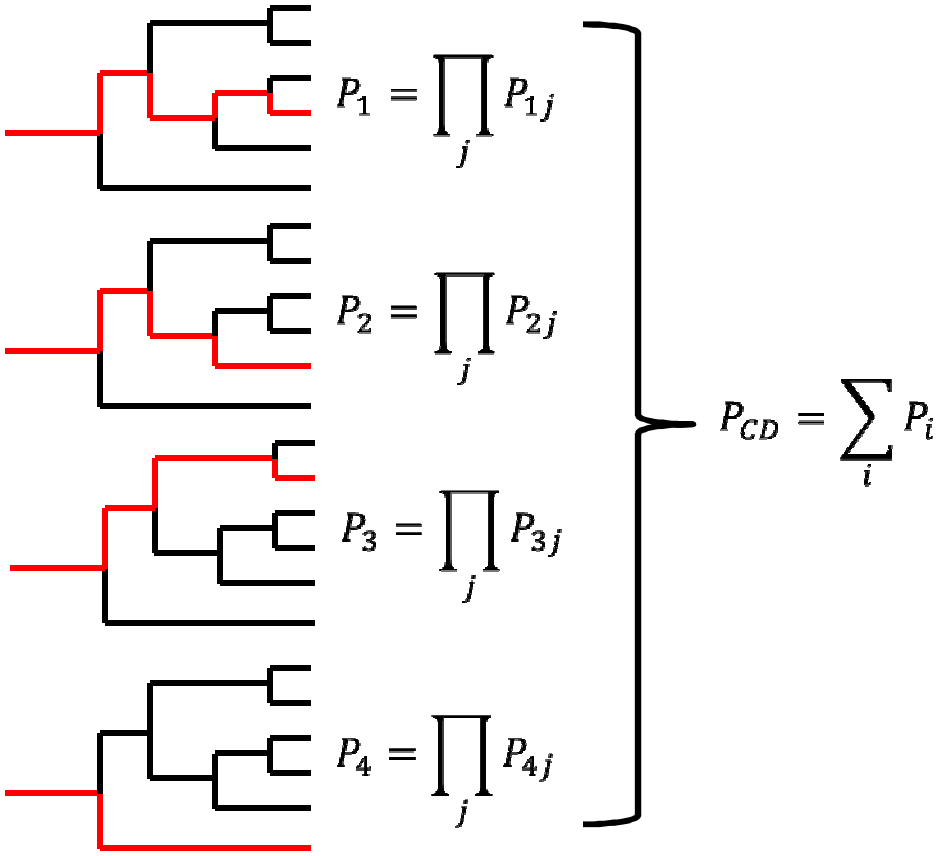


Analysis requires thorough knowledge of how the system operates and is maintained.

Data Analysis

- Sources
  - Generic data
  - Plant-specific data
- Specific challenges
  - Common cause failures
  - Human reliability
  - Time dependency
- Uncertainty
  - Random
  - State of knowledge

Accident Sequence Quantification

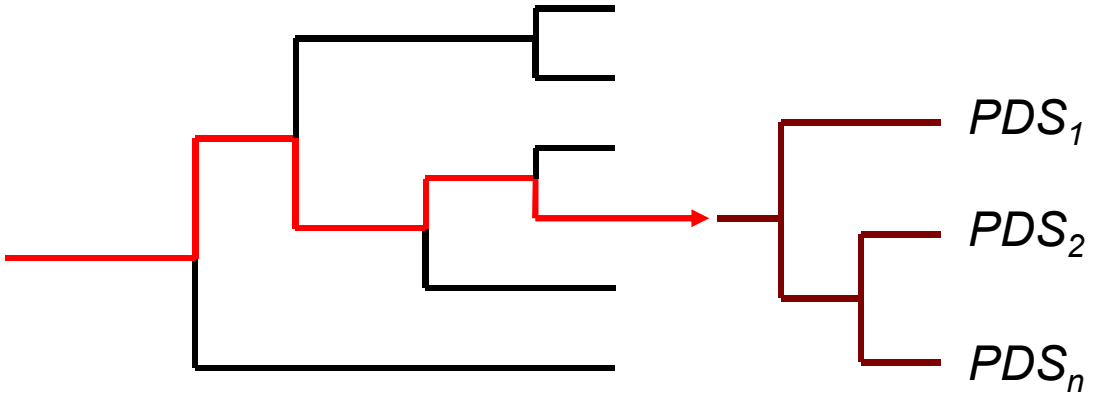


Core Damage Probability

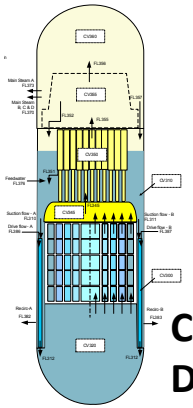
- Regulatory Metric
- Insufficient for accident progression analysis

Plant Damage State

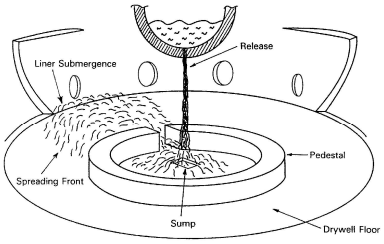
- Core damage insufficient for accident progression analysis
  - Containment status
  - Status of ignored systems



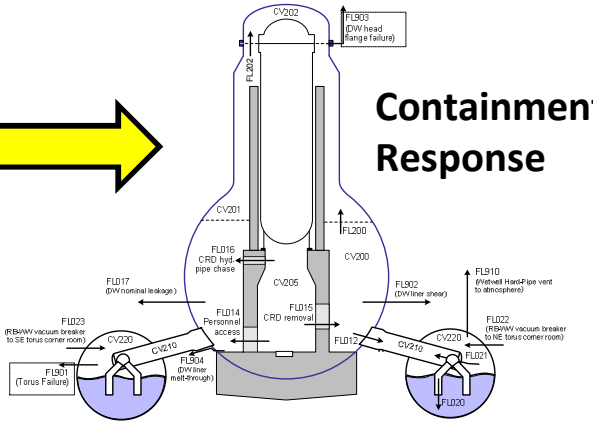
Source Term Analysis



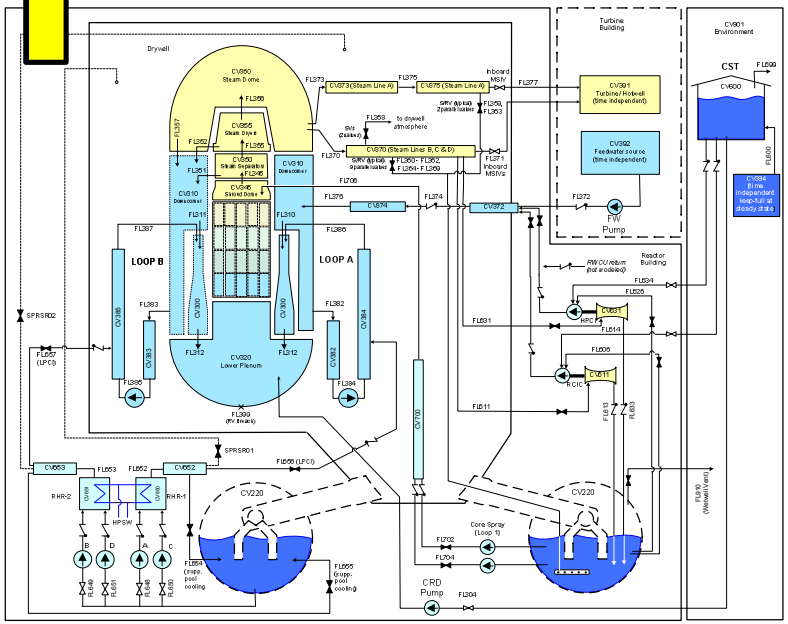
Core Damage



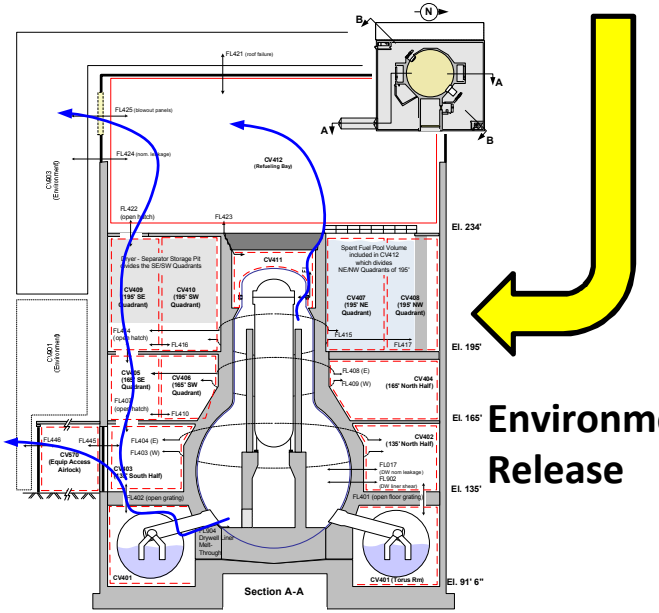
Vessel Release



Containment Response

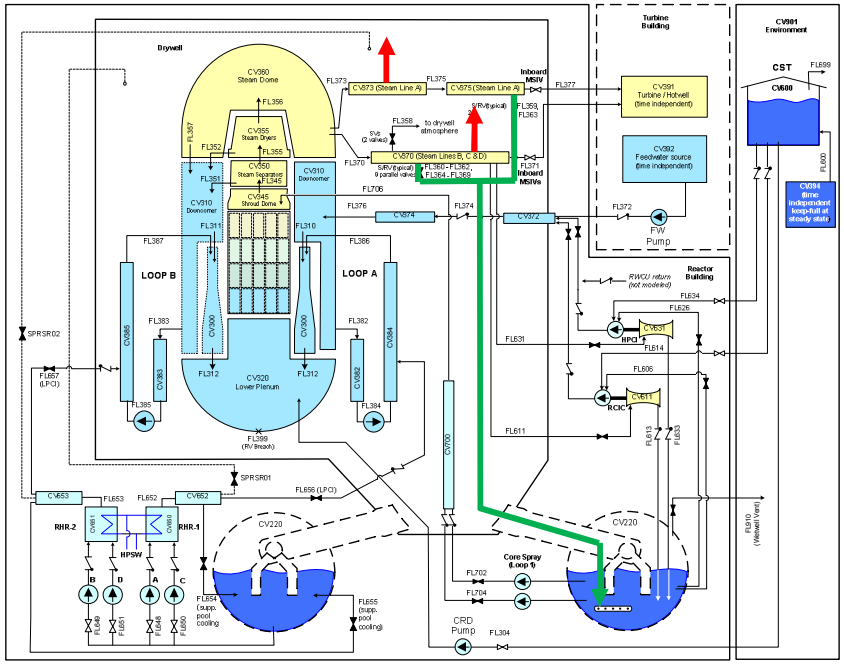


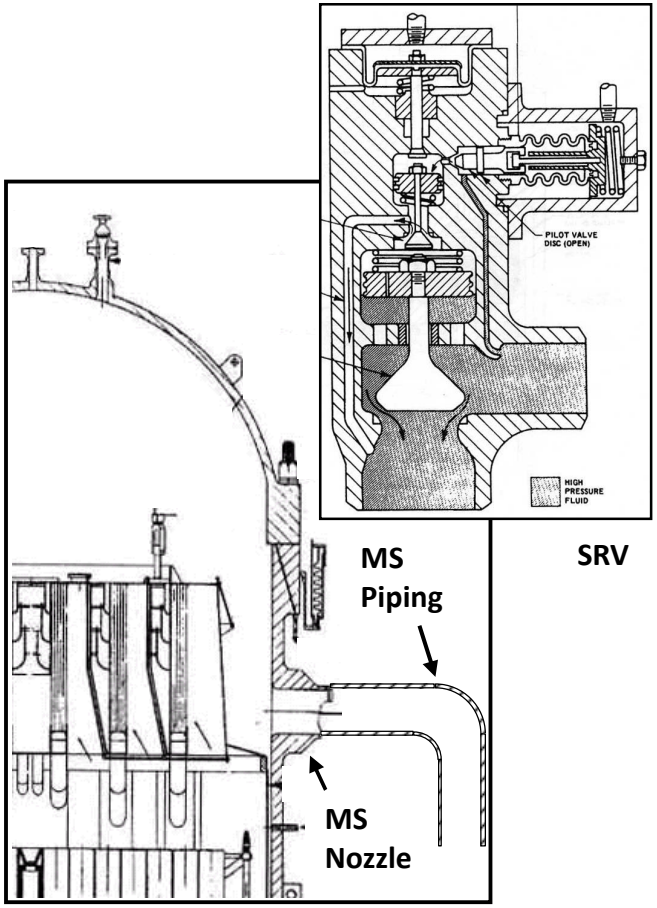
System Thermal Hydraulic Response



Environmental Release

Uncertainty and Sensitivity Analysis



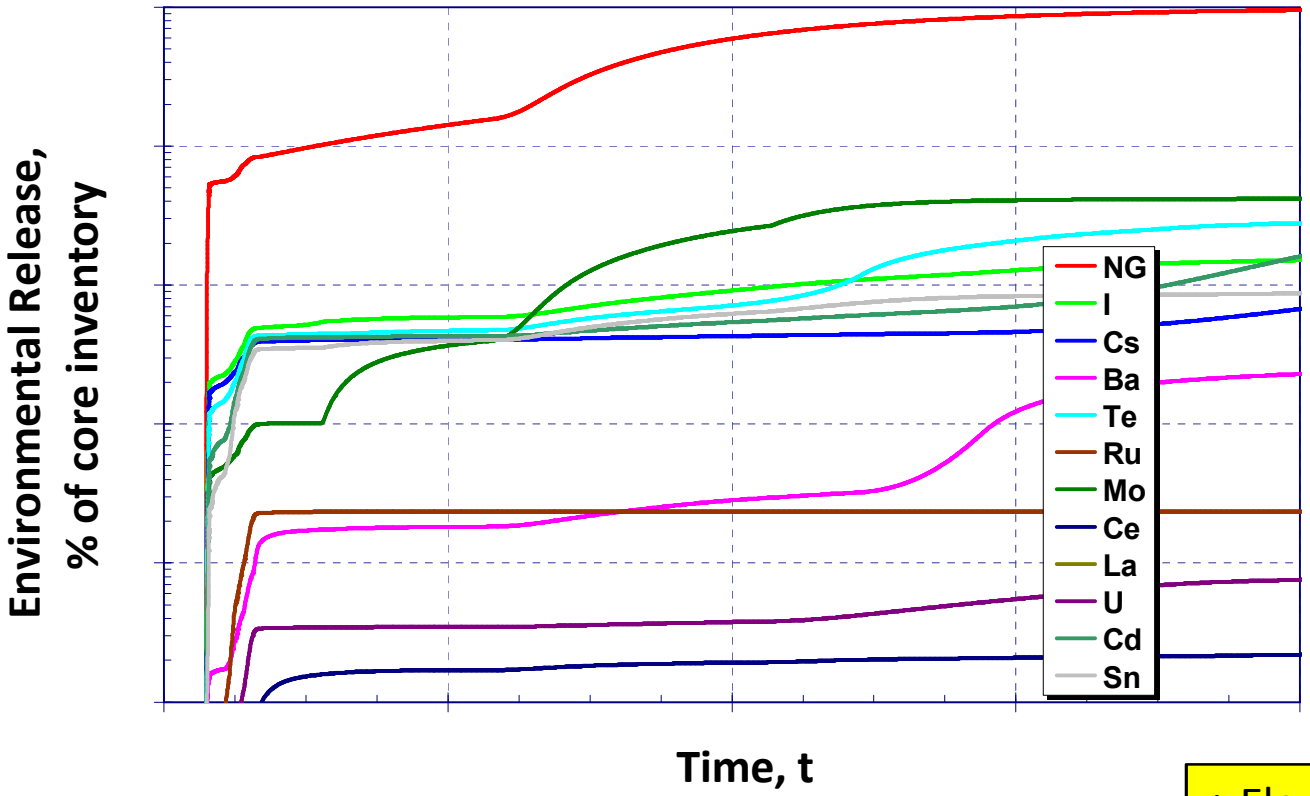


Main Steam (MS) Lines vent to the drywell (unscrubbed release)

Safety Release Valves (SRVs) vent to the wetwell (scrubbed release)

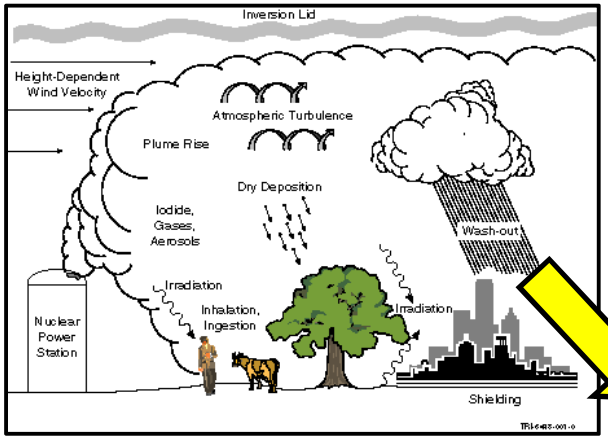
General Electric Mark-1 Boiling Water Reactor Example

Release Quantification

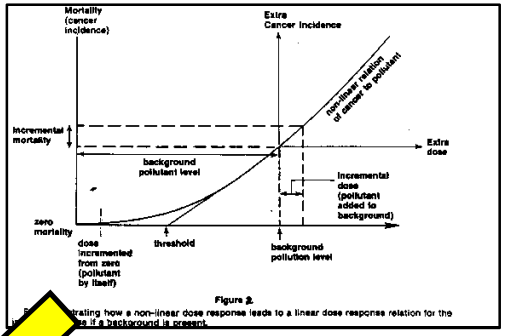


+ Elevation
+ Release Energy

Offsite Consequence Analysis

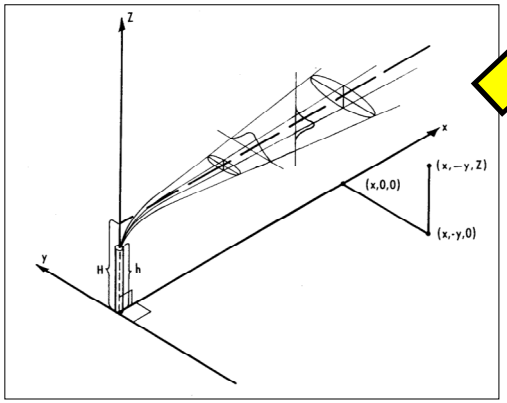


Deposition and Exposure Pathway

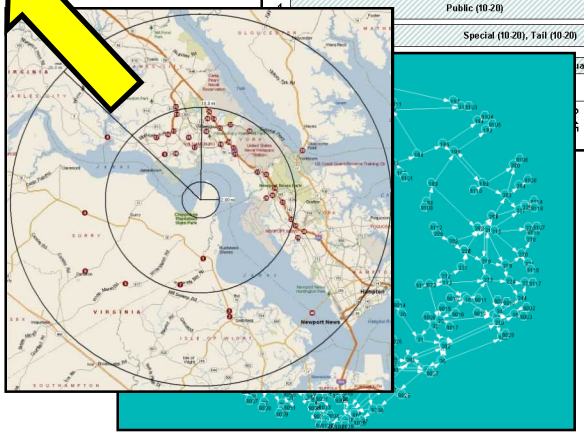


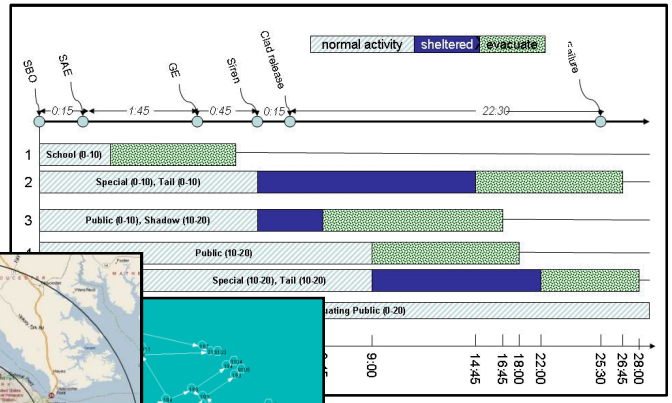
Dose Response

Latent Cancer Fatalities



Atmospheric Transport





Evacuation Modeling

Risk and Uncertainty Analysis

- Risk
  - Frequency
  - Consequence
- Uncertainty
  - Weather conditions
  - Dose response

Latent Cancer Fatalities/Reactor Year

Overview of PSA

- Strengths
  - Systematic analysis methodology
  - Qualitative and quantitative insights
  - Uncertainty and sensitivity evaluation
- Limitations
  - Availability of data
  - Dependency on analyst expertise
  - Static analysis

Research Directions

Challenges

- New technology
  - Digital instrumentation and control
- Novel operations
  - Multi unit
  - Passive safety
- Human factors
  - Man-machine interface
  - Cognitive models

Solutions

- Bayesian belief networks
  - Limited data
  - Human reliability
- Dynamic PSA
  - System response
  - Corrective actions
- System dynamics
  - Safety profile
  - Decision making

BACKUP SLIDES

Required Event Tree Information

- Knowledge of accident initiators
- Thermal-hydraulic response during accidents
- Knowledge of mitigating systems (frontline and support) operation
- Know the dependencies between systems
- Identify any limitations on component operations
- Knowledge of procedures (system, abnormal, and emergency)

Plant Damage State Definition

- Core Damage (CD) designation for end state not sufficient to support Level 2 analysis
  - Need details of core damage phenomena to accurately model challenge to containment integrity
- PDS relates core damage accident sequence to:
  - Status of plant systems (e.g., AC power operable?)
  - Status of Reactor Coolant System or RCS (e.g., pressure, integrity)
  - Status of water inventories (e.g., injected into Reactor Pressure Vessel?)

Fault Tree Analysis Definition

*"An analytical technique, whereby an **undesired state** of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed **in the context of its environment and operation** to find all **credible** ways in which the undesired event can occur."*

NUREG-0492

Common Cause Failures

- Conditions which may result in failure of more than one component, subsystem, or system
- Concerns:
  - Defeats redundancy and/or diversity
  - Data suggest high probability of occurrence relative to multiple independent failures

Minimal Cut Set Definition

A group of basic event failures (component failures and/or human errors) that are ***collectively necessary*** and ***sufficient*** to cause the TOP event to occur.