IAEA 60 Years
Atoms for Peace and Development

Joint IAEA-ICTP Essential Knowledge Workshop on Nuclear Power Plant Design Safety

ICTP/Trieste, 9 – 20 October 2017

Probabilisitc Safety Assessment

Javier YLLERA
Safety Assessment Section
Division of Nuclear Installation Safety

PSA Objectives

- PSA is intended to gain probabilistic estimates of the occurrence of undesired events in technical systems or installations, such a NPP, when statistical experience is insufficient or not useful.

- Undesired events in a NPP can be:
  - Reactor core damage (level 1 PSA)
  - Fuel element damage during fuel manipulation
  - A large early release of radioactivity to the environment (level 2 PSA)
  - Fatalities, other consequences following a large radioactivity release (level 3 PSA)

- Probabilistic estimates would be: system failure frequencies or probabilities. Specifically in NPP PSA core damage frequency, expected amount radioactivity releases, are results of interest
- Not only overall numerical results are obtained. Their analyses allows to identify important contributors to risk, plant vulnerabilities, etc.

Classification of Risk Analysis Methods

Many risk analysis techniques have been developed over the time.

They can be classified according to a series of attributes:

- Reasoning process: Deductive or inductive
- Scope of the analysis: Hazard identification, hazard assessment
- Nature of the process and results: Qualitative and quantitative

- Qualitative analysis were developed first
- Quantitative methods (strictly speaking) are of probabilistic nature. Some risk indexing methods have been also developed. Quantitative risk assessment is not mandatory for many types of facilities.
- Hazard identification is previous to any other type of analysis

Classification of Risk Analysis Methods

Qualitative

- **Preliminary hazard analysis. Check lists.**
- **Risk Indexes: Mond, Dow**
- **Failure Mode and Effects (and criticality) analysis (FMEA)**
- **Hazard and Operability Analysis (HAZOP)**

(Qualitative methods don't consider in general multiple failures)

Quantitative (Probabilistic)

- **Event tree analysis**
- **Fault Tree Analysis**
- **Markov and Semi Markov models**
- **Others**

A blend of qualitative and quantitative methods is used in a PSA

Types of Quantitative Risk Assessment Methods

- **Boolean methods:** They make use of Boolean Algebra. Each component, system, subsystem, etc., e.g. a valve, has 2 possible states:
  - the component works as new, i.e. it is capable to perform the required mission, or
  - the component is failed

  Examples: Fault trees and event trees

- **Non Boolean methods**
  - Allow the consideration of several component/system states
  - Allow more detailed calculations of certain issues that Boolean models cannot address with ease, but
    - adequate data is often lacking
    - Are only solvable for very small systems with simplifications.

  Examples: Markov models

Boolean reliability models

- All standard PSAs for NPPs use Boolean reliability models. Other techniques have been used for analyses of very limited scope.

- Boolean models make use of Boolean algebra: The state of each component, subsystem, system or event is associated to a Boolean variable that takes the following values:
  - TRUE: if the event has occurred, e.g.component or system has failed
  - FALSE: if the event has not occurred, e.g.component or system has not failed

1 and 0 or other binary set of values can be used instead of TRUE and FALSE

- The state of the whole system is related to the state of its components through the system "structure function" which is built up with Boolean operators.

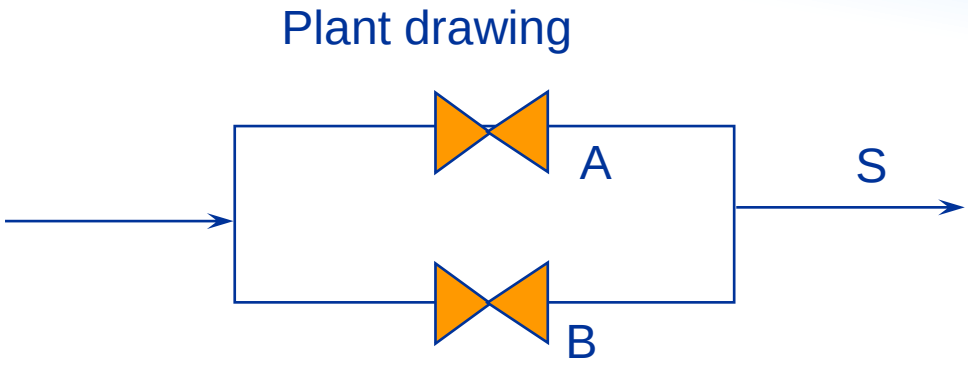
Classification according to the reasoning process

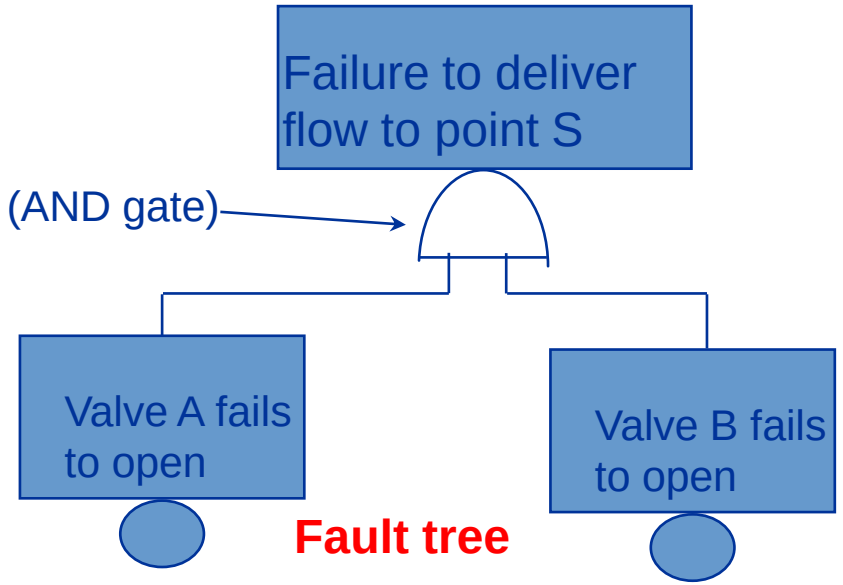
- **Deductive methods**: An undesired event is postulated and is related the the immediate causes leading to it. These in turn are further analysed in the same way until this recurrent process finally allows to establish a relation between the undesired event and the failures of single components in the plant, such as pumps or valves. Fault tree analysis is a deductive modelling method. The question "how can this happen" is asked through the process.

- **Inductive methods**: An event is postulated in a plant and the consequences of that event are analysed depending on whether the some other events happen at the same time or not. Event tree analysis is an inductive modelling method. The question "what happen if" is asked along the process.

PSA combines both deductive and inductive methods.

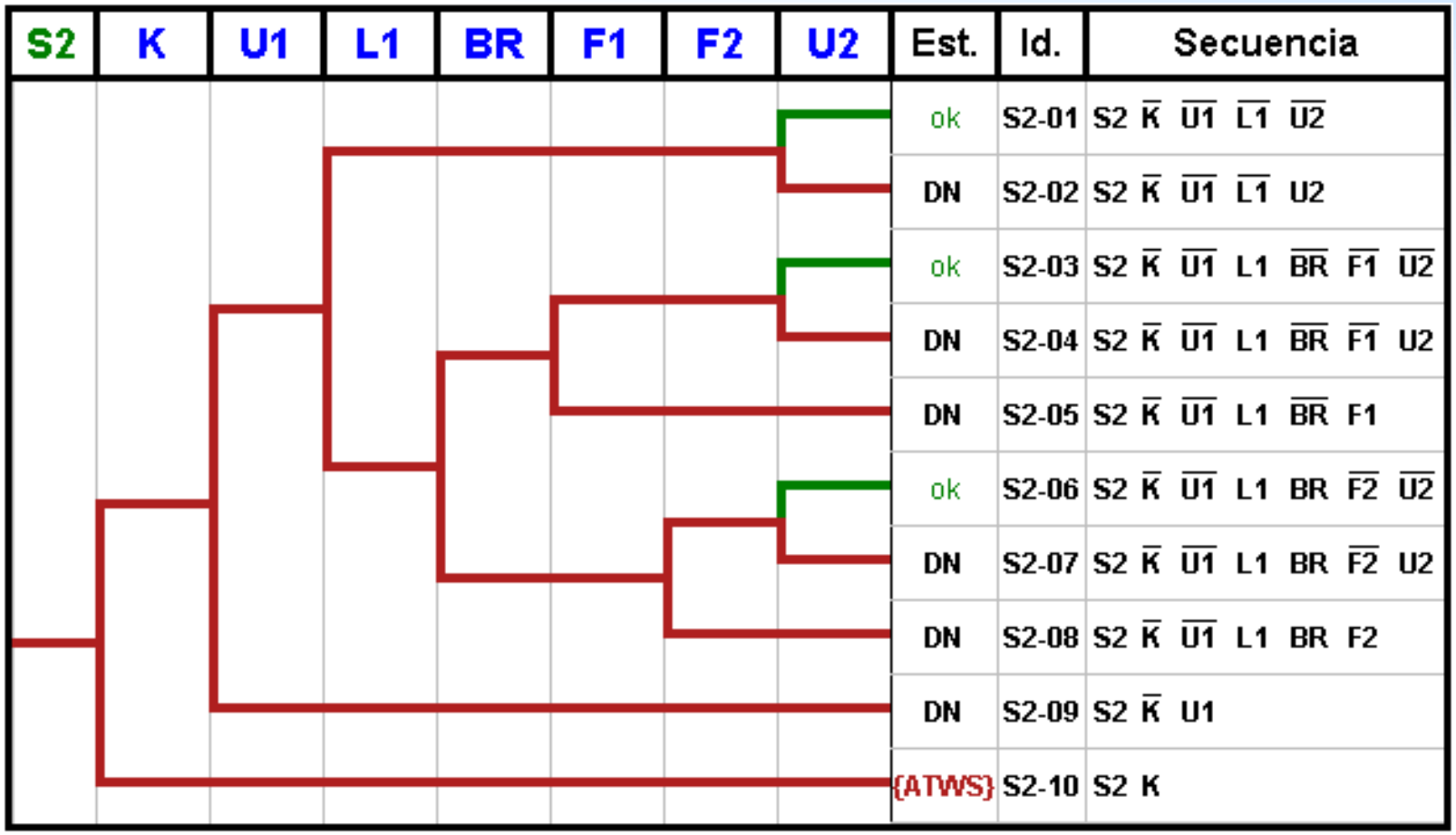
Deductive methods. Case example





Fault tree

Inductive Methods. Case example



S2	K	U1	L1	BR	F1	F2	U2	Est.	Id.	Secuencia
								ok	S2-01	S2 $\overline{K}$ $\overline{U1}$ $\overline{L1}$ $\overline{U2}$
								DN	S2-02	S2 $\overline{K}$ $\overline{U1}$ $\overline{L1}$ U2
								ok	S2-03	S2 $\overline{K}$ $\overline{U1}$ L1 $\overline{BR}$ $\overline{F1}$ $\overline{U2}$
								DN	S2-04	S2 $\overline{K}$ $\overline{U1}$ L1 $\overline{BR}$ $\overline{F1}$ U2
								DN	S2-05	S2 $\overline{K}$ $\overline{U1}$ L1 $\overline{BR}$ F1
								ok	S2-06	S2 $\overline{K}$ $\overline{U1}$ L1 BR $\overline{F2}$ $\overline{U2}$
								DN	S2-07	S2 $\overline{K}$ $\overline{U1}$ L1 BR $\overline{F2}$ U2
								DN	S2-08	S2 $\overline{K}$ $\overline{U1}$ L1 BR F2
								DN	S2-09	S2 $\overline{K}$ U1
								{ATWS}	S2-10	S2 K

Event tree

Scope of a NPP PSA

- **Sources of radioactivity considered:** ***Reactor core***, fuel ponds, fuel manipulation accidents, etc.

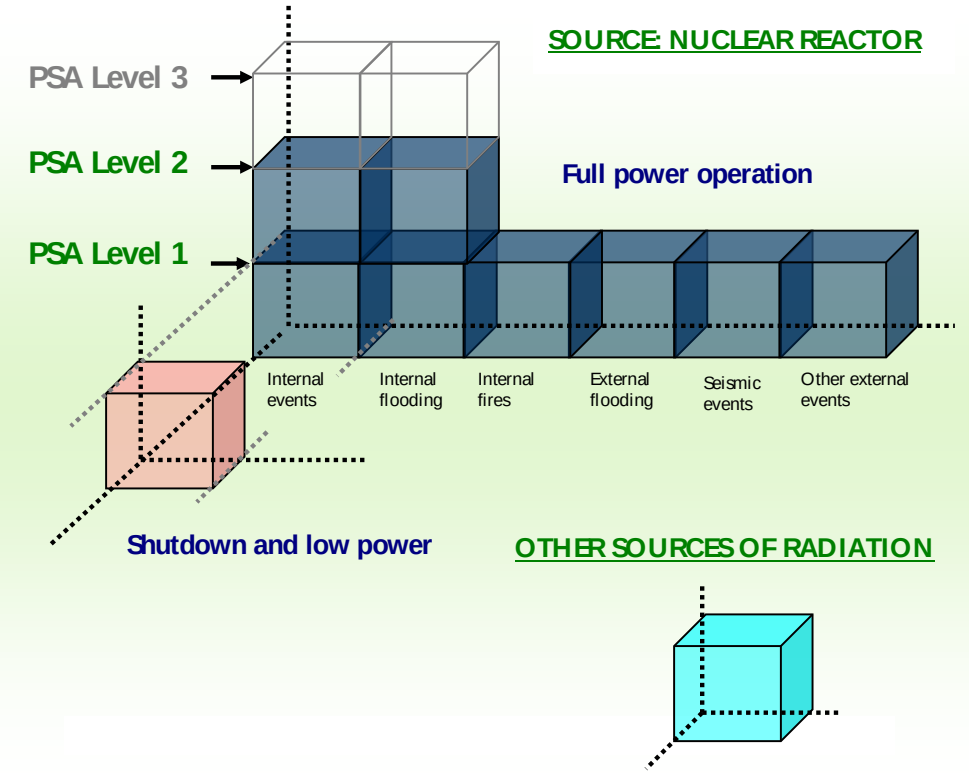
- **Undesired event and calculated consequences (PSA level):** Core damage (level 1), large radioactivity releases (level 2), consequences to the environment (level 3)

- **Modes of operation before the accident:** Full power, low power operation modes and shutdown modes

- **Type of initiating events considered**:
  - Internal initiating events
  - Internal hazards (area events): Internal fires, internal floods
  - External hazards: Earthquakes, external fires and floods, tornados, aircraft crash, etc.

Overview of PSA Scope

In an NPP PSA, the radiological risk arising from major damage to the reactor core, but also from other potential sources, is assessed



PSA: models considers together:

- Explicitly considers a broad set of potential challenges to safety (IEs), logically groups them and analyzes the mitigation measures,
- Considers plant design, physical phenomena, component reliability & plant experience, operational practices and human performance
- Assesses the sensitivity of results to key assumptions and identifies and potentially quantify uncertainties in results

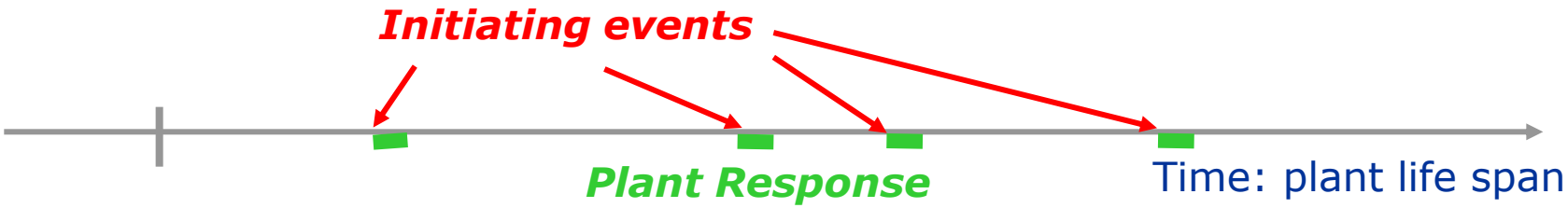
Level-1: Core damage frequency

Level-2: Release categories and their frequencies

Level-3: Individual risk of death for a member of the public, early and late health effect

Overview of a NPP PSA (level 1): Model construction

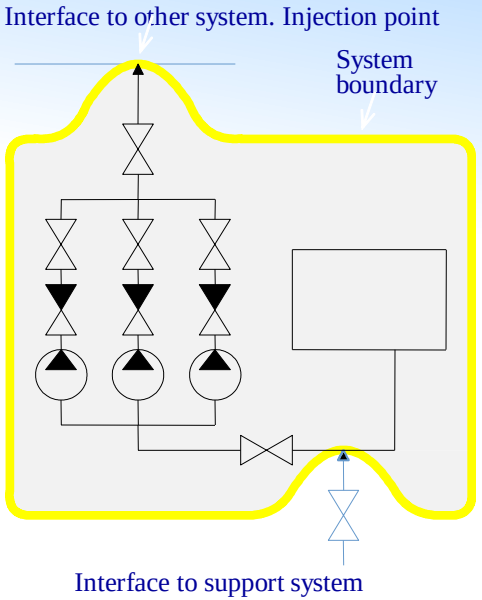
- **Definition of Initiating events:** Those events requiring the prompt activation of the rector protection system and the intervention of the safety systems to achieve a safe shutdown state are identified and grouped according to their similar impact on the plant response.



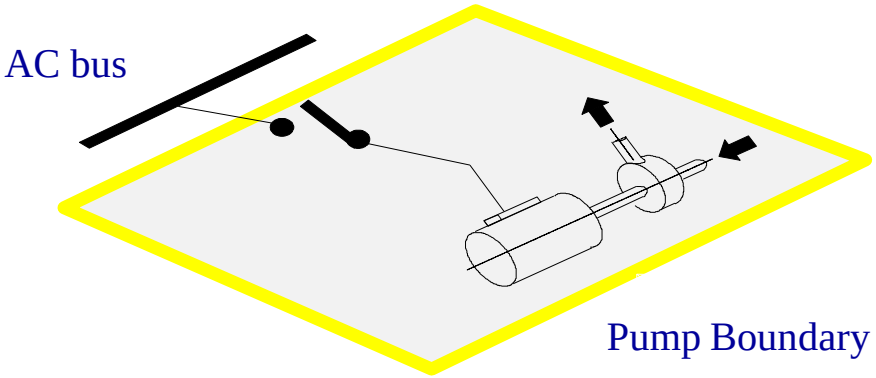
- **Accident sequence development :** The accident progress is analysed depending of the successful or unsuccessful actuation of the safety systems and human actions needed to mitigate an initiating event. Success criteria are needed to define the conditions required for the successful actuation of the safety systems. (Event tree analysis)
- **System analysis:** The safety systems considered in the accident sequence development are analysed by developing fault tree models. The necessary support systems are analysed as well. (Fault tree analysis)

Overview of a NPP PSA: Model boundaries

- **External boundaries:** Systems and installations are not isolated from the world. External boundaries define the object of the analysis.

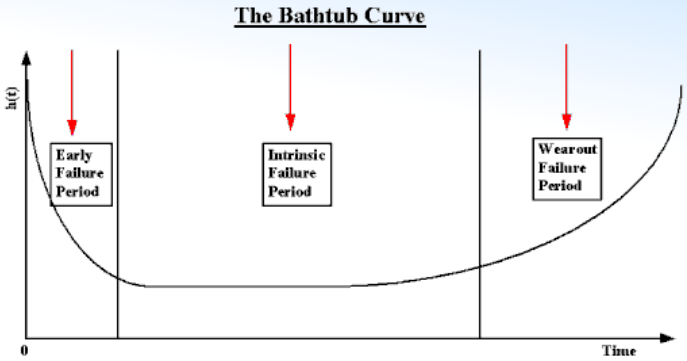


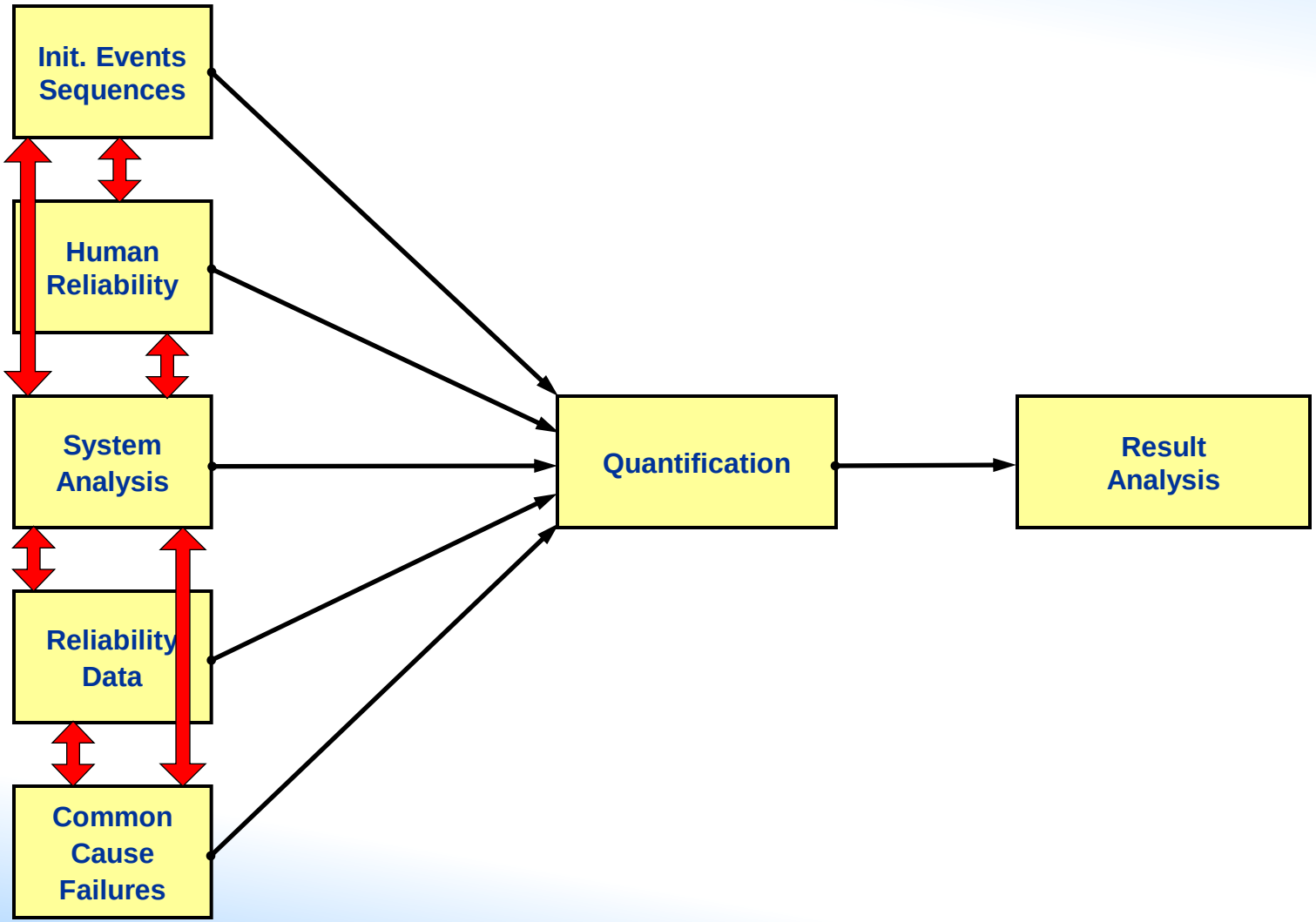
- **Internal boundaries:** Definition of level of detail, commensurate with the objectives of the analysis, and availability of resources and reliability data for the parts of the model.



Overview of a NPP PSA: Basic event probabilities

- **Reliability data analysis:** Failure rates or failure probabilities need to be obtained for component failures, initiating events and other special events postulated in the PSA models. A particular important type of component failures are the common cause failures. They are analysed separately taking into account statistical data and plant design features, ands using special models.
- **Human reliability analysis :** Human actions or human errors postulated in the accident sequence and system analysis are analysed with human reliability models to obtain human error probabilities.



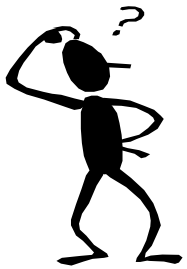


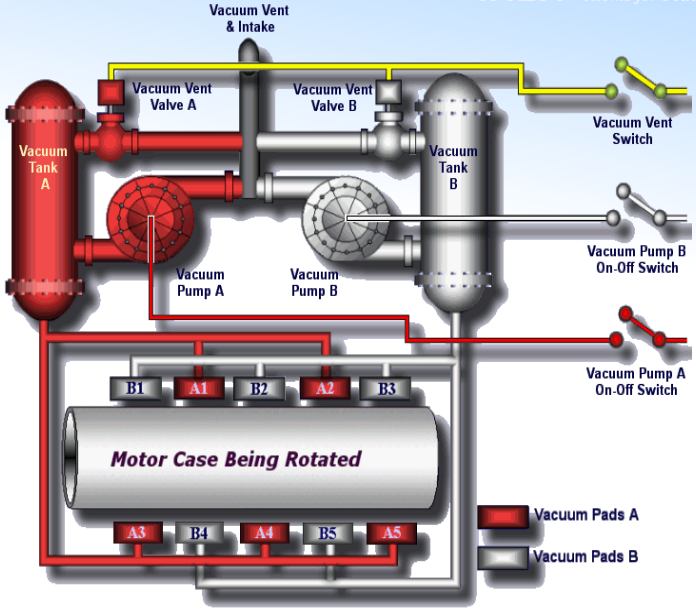
Overview of a NPP PSA: Risk calculation

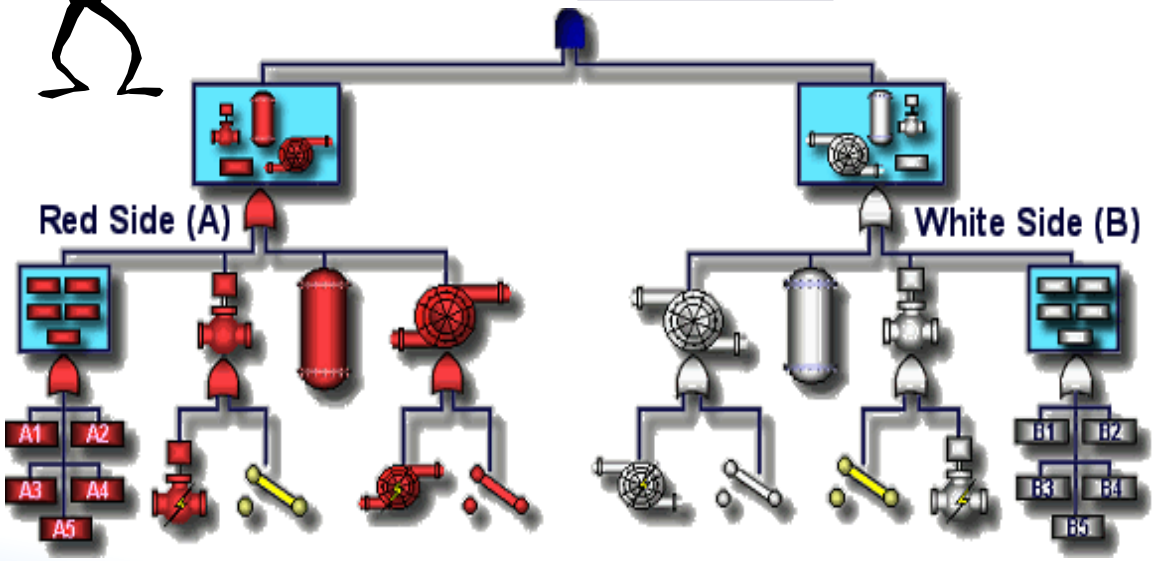
Model quantification:
Based on the basic event probabilities, the PSA models are quantified using thereby suitable computer codes to obtain the core damage frequency of the plant**.**

Results are analysed to identify important risk contributors, plant vulnerabilities and to provide uncertainty bounds for the plant risk estimates.

10^{-6} /year







Other relevant PSA aspects

- PSA ORGANIZATION AND MANAGEMENT: **Proper measures are needed to set up a qualified set of experts. Procedures, task interfaces and responsibilities need to be established as a basis for a good team work . The full support and the involvement of technical plant staff is essential**
- PSA VERIFICATION AND QUALITY ASSURANCE: **An adequate programme of technical quality assurance with the involvement of the utility and independent experts is needed to ensure the adequacy of the PSA.**
- IMPLEMENTATION OF A LIVING PSA PROGRAMME: **After finishing the PSA the utility has to provide the resources and the organisation for maintaining the PSA updated and develop PSA applications on it.**

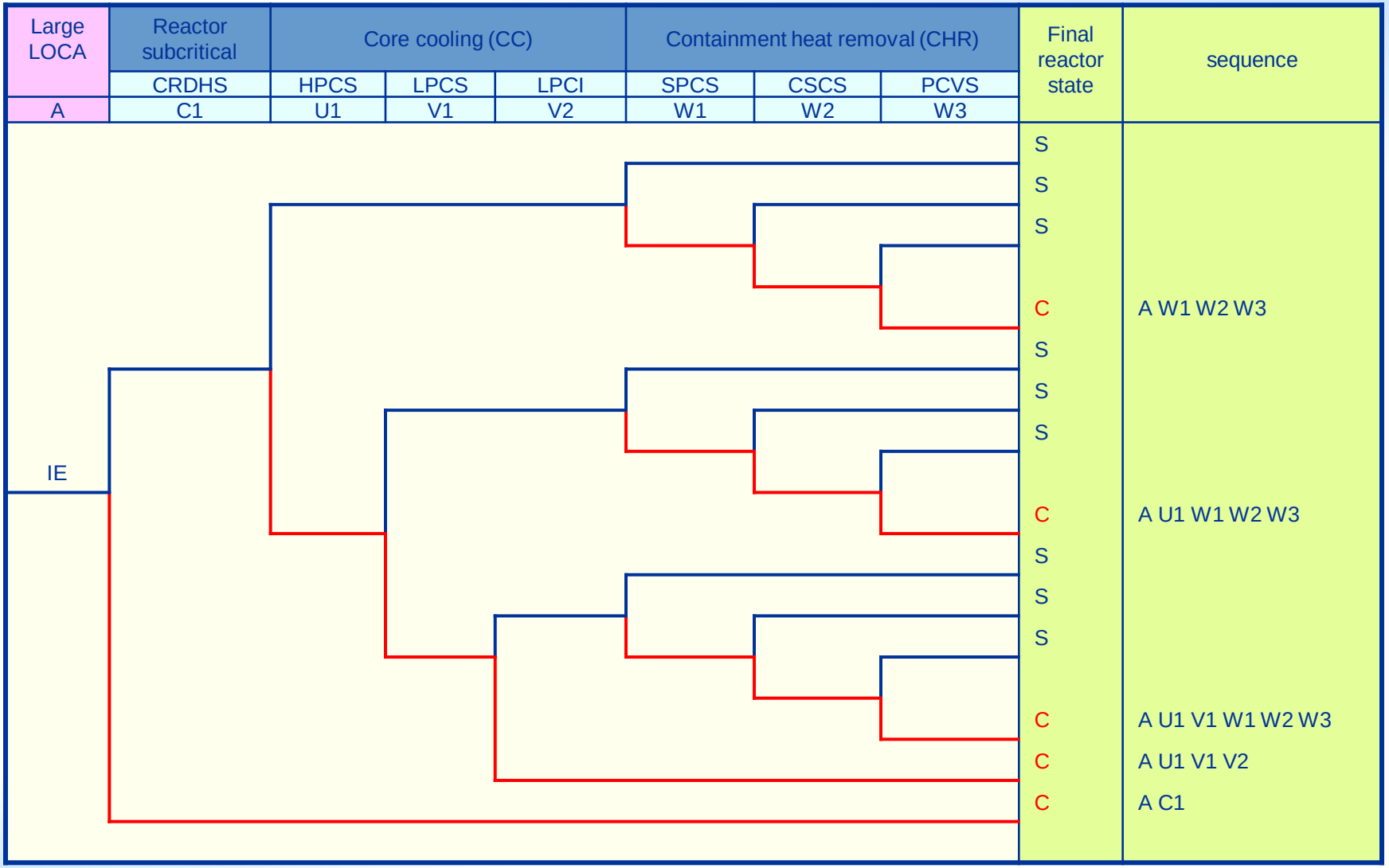
Accident Sequence Analysis

Methods and Tools

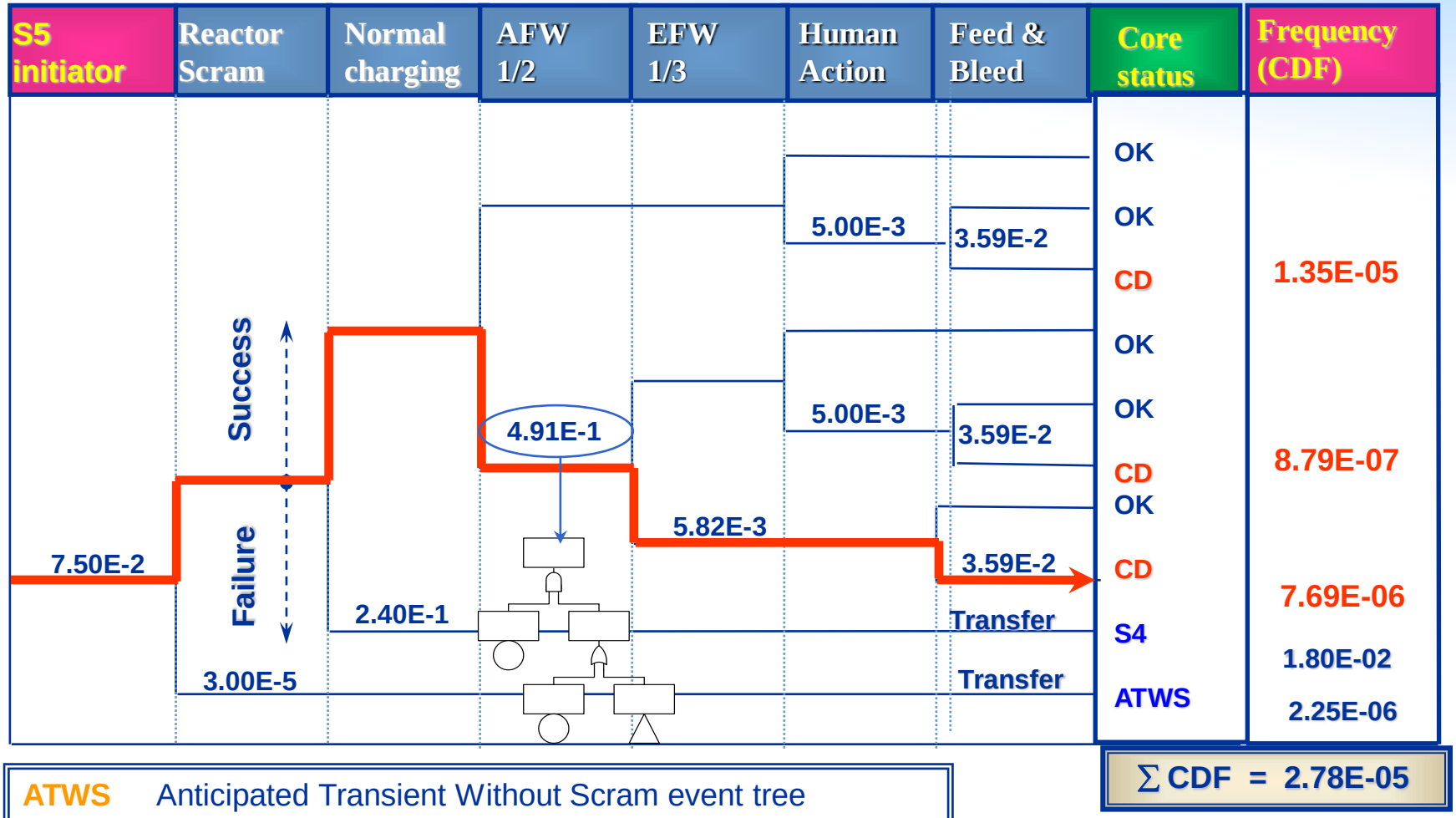
- Accident sequences consist of:
  - Initiating event (IE)
  - Modeling functions (mitigating safety functions and/or human interactions, given IE occurrence)
    - Safety Functions may result from an automatic or manual actuation of a system, from passive system performance, or from natural feedback
  - End State: Damage to the core or core damage prevented.

- Standard model:
  - Event trees for sequence modeling and fault trees for system modeling

Example of Small Event Tree for BWR (System Event Tree)



Example of System Event Tree - Very Small LOCA (PWR)



ATWS	Anticipated Transient Without Scram event tree
S4	Small LOCA initiator group event tree
S5	Initiating event (Very Small LOCA)

CD = Core Damage State

OK = Core Safe State

TH Analysis and Other Tools

- Appropriate thermal hydraulic analyses and other assessment means are used for the assessment of
  - Detailed success criteria
  - Event timing
  - Impact of IE on systems, structures, components and human interactions
- Computer codes used for the modelling of the course of accident sequences and for the derivation of associated success criteria
  - Applicable and proven
  - Conservative or Best estimate depending on the use
- Computation models
  - Reflects the specific design and operational features of the plant
    - The justification of the applicability and an assessment of associated uncertainties
- Analysis models and computer codes
  - Have sufficient capability to model the conditions and phenomena of interest
  - Provide results representative for the plant
  - Used within known limits of applicability

TH Analysis and Other Tools (cont.)

- The plant model and parameters used for T/H analyses
  - Provides sufficient resolution and reflects the actual design and operational features of the plant
- Calculated parameter values
  - When the function of safety related systems and operator actions are carried out
    - E.g. setpoints, limit points, trigger values, entry and exit values for procedures, and sets of parameter values which are used for control functions
  - Uncertainties, variabilities, and delays for measuring and actuating devices and for actuated equipment are taken into account
- The acceptability of thermal hydraulic, structural or other supporting engineering bases used to support success criteria
  - Comparison of results with results of similar analyses performed for similar plants, accounting for differences in unique plant features
  - Comparison with results of similar analyses with other codes
  - Check by other means, e.g. simplified engineering calculations

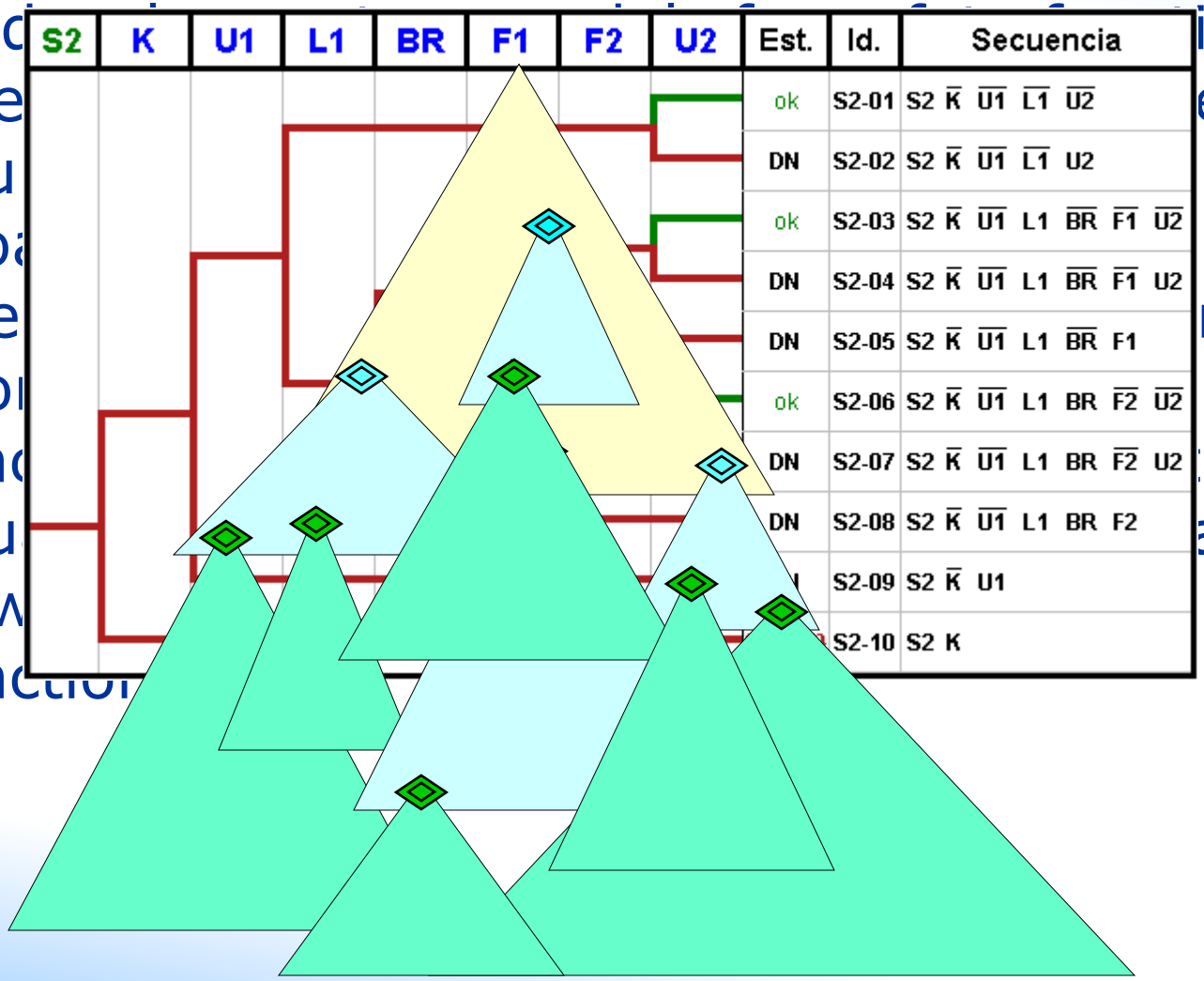
Analysis to Support Success Criteria

- Analysis needs to be carried out to provide justification for the success criterion
  - Neutronics analysis – for reactor shutdown/ hold-down
  - Thermal-hydraulics analysis – for heat removal from the reactor core
- Best estimate success criteria
  - Aim should be to define success criteria using best estimate analysis and data where possible
- Conservative success criteria
  - Success criteria often defined based on conservative/ design basis analysis
  - Results should be reviewed to ensure that this does not dominate CDF
  - Sensitivity studies should be carried out where this has been done

System Analysis

Principal Objective of System analysis Task in a PSA of NPP

- To d… …ions inte… …ers.
- Fau… bro…
- Eve… …ms (nor… func… …tems usu… …as pow… …their functio…



System Analysis
Systems usually modelled in a PSA

Front line systems

PWR

- High pressure safety injection (and/or charging pumps)
- Low pressure safety injection (and/or RHR)
- Accumulators
- Primary and Secondary pressure control
- Isolation of steam generators.
- Containment spray

BWR

- Safety injection or spray to the vessel: HPCS, LPCI, LPCS, RHR
- Containment Spray
- Core isolation cooling (RCIC)
- Emergency boration (SBLC)
- Steam isolation
- Safety/relief valves, ADSL
- Reactor scram systems

Support systems

AC,DC power supplies, including Diesel Generators.
Component cooling water, Service water,
Ventilation,
Reactor protection system, etc.

Fault Trees

- A fault tree is a graphical representation of the logical relationship existing between and undesired event or a failure in a system (top event) and and the causes leading to it. These causes are recursively analysed until the undesired event is related to combinations of elementary events in the system, such as component failure or a human failure)

- A fault tree is Boolean reliability model, since all the elements in the fault tree, from the elementary or basic events to the top event (e.g. representing the system failure) have 2 only possible states: the event occurs (e.g. the component fails) or does not occur (the component fulfils its mission perfectly). A Boolean variable is assigned to each element of the fault tree

Boolean Algebra

- **George Boole,** British Mathematician (1815-1864)

- Boolean variables:

They can take only 2 different values. Several sets of value names can be used:

TRUE	/	FALSE
1	/	0

The negative logic used in fault trees, they correspond respectively to:

failure, event happens / success, event doesn’t happen

Boolean Operators and Laws

"OR" Disjunction: ($\vee$), frequently, the arithmetic addition symbol is used instead: **+**

"AND" Conjunction: ($\wedge$); frequently, the arithmetic multiplication symbols are used instead: **x, ·, ***

"NOT" Negation: Several symbols added to the Boolean variable are used, such as: "***/***", " **'** ": /A, A'

Boolean laws or properties: Commutative, Associative, Distributive, Idempotent, Absorption, Morgan's laws, ...

Boolean Laws

MATHEMATICAL NOT.	USUAL NOTATION	LAW NAME
$X \wedge Y = Y \wedge X$	$X \bullet Y = Y \bullet X$	COMMUTATIVE LAW
$X \vee Y = Y \vee X$	$X + Y = Y + X$	
$X \wedge (Y \wedge Z) = (X \wedge Y) \wedge Z$	$X \bullet (Y \bullet Z) = (X \bullet Y) \bullet Z$	ASSOCIATIVE LAW
$X \vee (Y \vee Z) = (X \vee Y) \vee Z$	$X + (Y + Z) = (X + Y) + Z$	
$X \wedge (Y \vee Z) = (X \wedge Y) \vee (X \wedge Z)$	$X \bullet (Y + Z) = X \bullet Y + X \bullet Z$	DISTRIBUTIVE LAW
$X \wedge X = X$	$X \bullet X = X$	IDEMPOTENT LAW
$X \vee (X \wedge Y) = X$	$X + (X \bullet Y) = X$	ABSORPTION LAW
$X \wedge X' = 0$	$X \bullet X' = 0$	COMPLEMENTATION LAW
$X \vee X' = 1$	$X + X' = 1$	
$(X')' = X$	$(X')' = X$	
$(X \wedge Y)' = X' \vee Y'$	$(X \bullet Y)' = X' + Y'$	MORGAN'S LAWS
$(X \vee Y)' = X' \wedge Y'$	$(X + Y)' = X' \bullet Y'$	
$0 \wedge X = 0$	$0 \bullet X = 0$	
$1 \wedge X = X$	$1 \bullet X = X$	
$1 \vee X = 1$	$1 + X = 1$	
$0 \vee X = 0$	$0 + X = 0$	

Structure function of the system

- The structure function relates the state of the system to the state of the components or basic events.
- It is a Boolean function (time dependent) containing therefore Boolean variables and Boolean operators:

$$S(t) = \varphi(\underline{X}(t))$$

- The gates of a fault tree represent Boolean operators. The structure function is defined by the fault tree logic.
- The fault tree itself is a model of the system and contains valuable information. However, the structure function is the basis for the estimation of system failure probability.

Phases of System Analysis

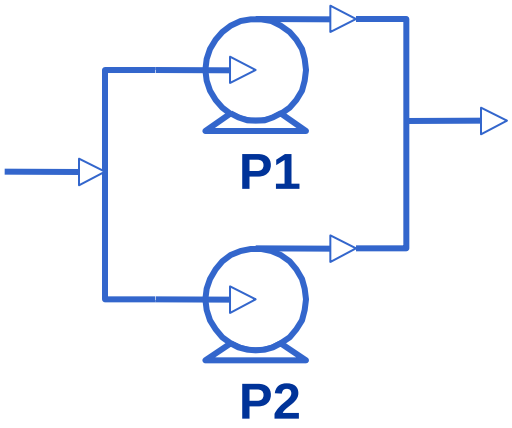
A V VM

- Acquisition of deep knowledge of system design and operation
- Obtaining modelling requirements, success criteria and boundary conditions
- Definition of system boundaries and interfaces
- Constructing simplified diagrams. Support simplification assumptions.
- Document the study and define needs for other models and reliability data.

- Document modelling assumptions
- **DEVELOP FAULT TREE MODEL. Check model validity.**

System example

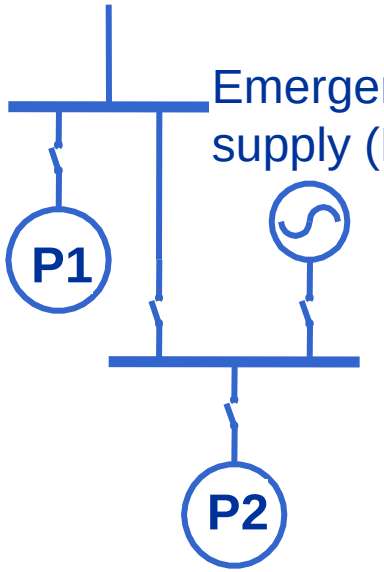
Running pump



Standby pump

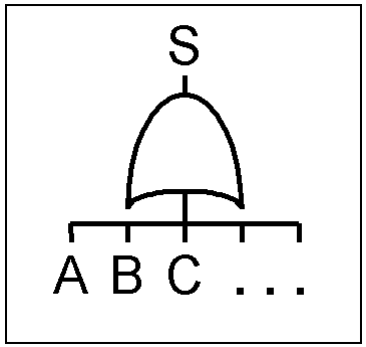
Normal power supply

Emergency power supply (DG)

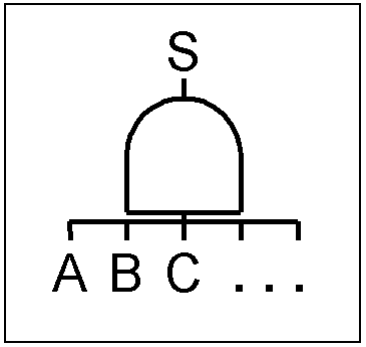


Fault Tree Symbols

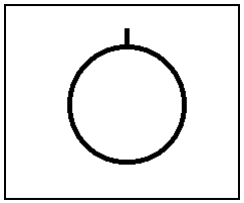
TW



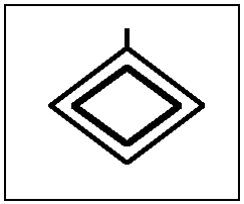
OR gate “O”
S=A+B+C+…
represents
disjunction



AND gate “Y”
S=A·B·C·…
represents
conjunction

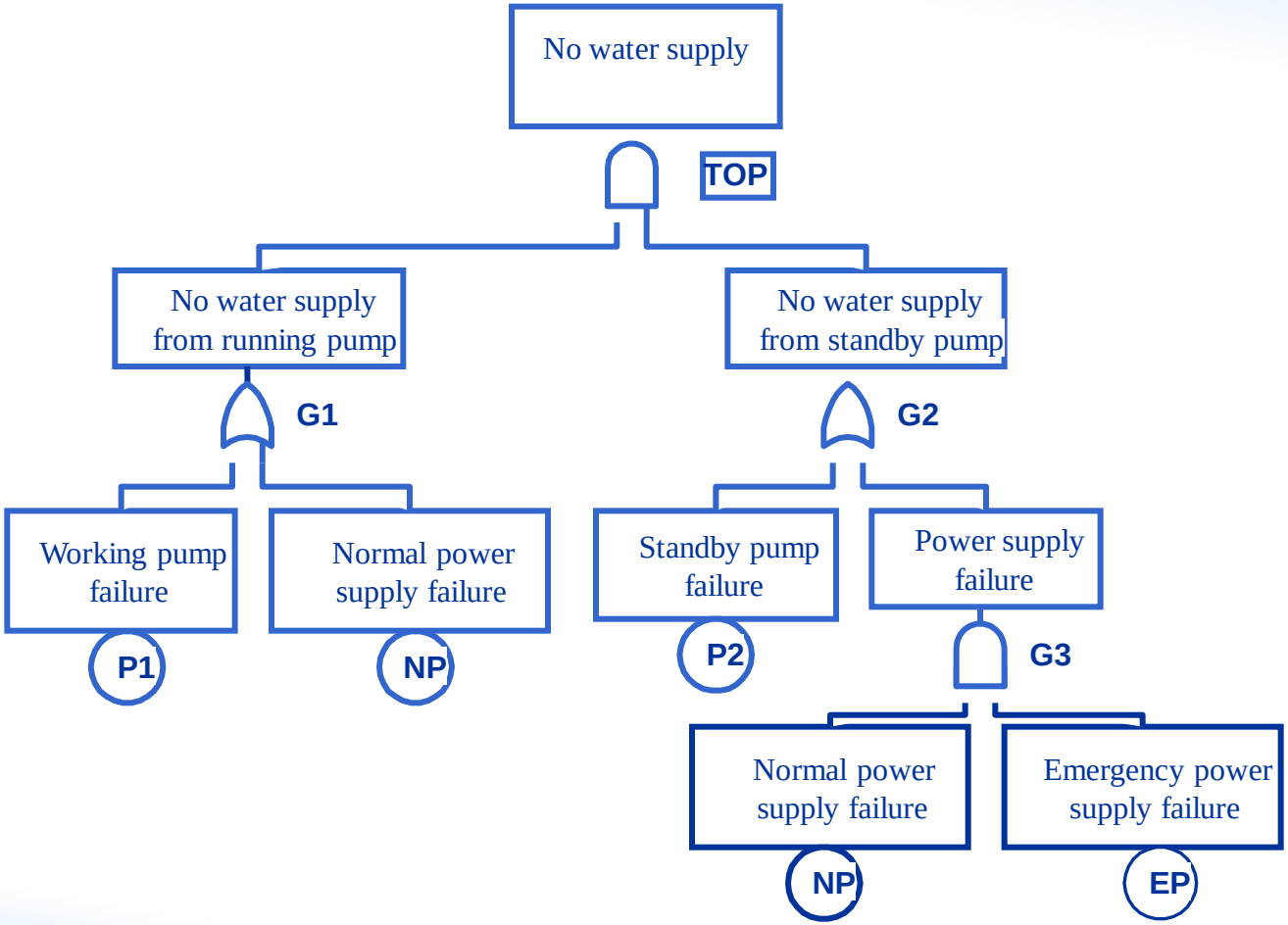


Basic
Event



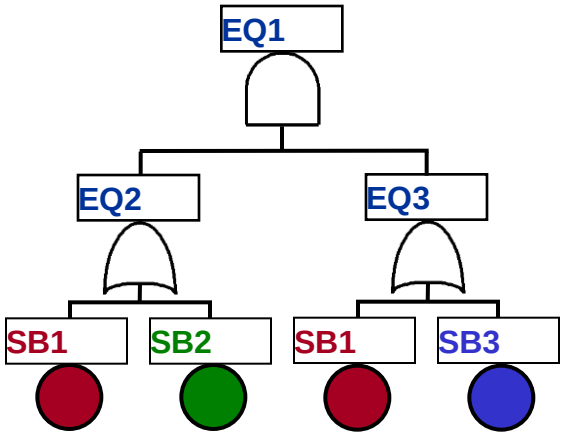
Event to be
developed in
other fault tree

Fault tree example



Fault Tree solution

Minimal cut sets



$EQ1 = EQ2 \cdot EQ3$

$EQ2 = SB1 + SB2$

$EQ3 = SB1 + SB3$

$EQ1 = (SB1+SB2)\cdot(SB1+SB3)$

(original structure function)

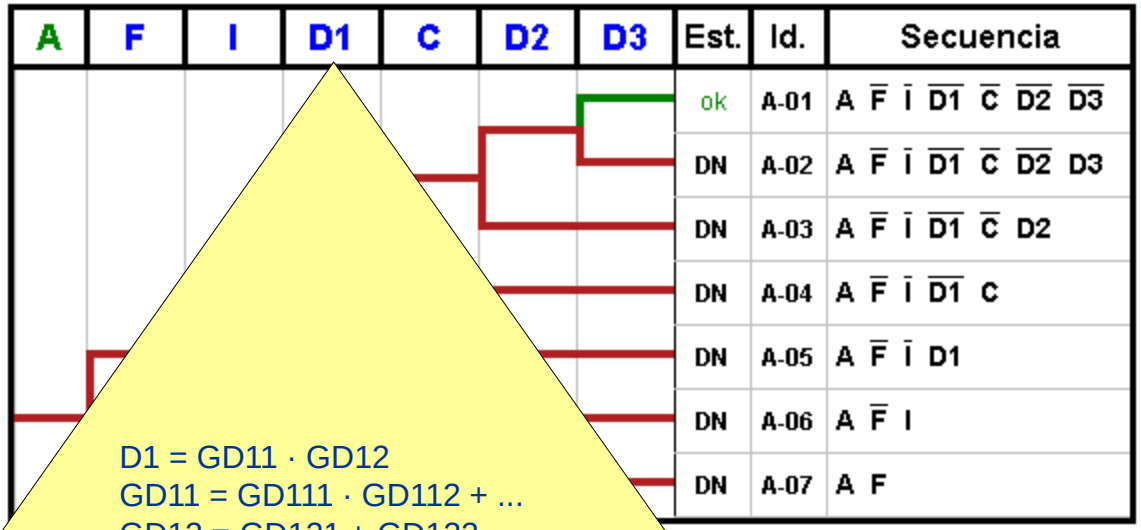
$EQ1 = SB1\cdot SB1 + SB1\cdot SB3 + SB2\cdot SB1 + SB2\cdot SB3$

$EQ1 = SB1 + SB1\cdot SB3 + SB2\cdot SB1 + SB2\cdot SB3$

$EQ1 = SB1 + SB2\cdot SB3$

(Disjunctive normal form, suitable for quantification)

Accident sequence equations



D1 = GD11 · GD12
GD11 = GD111 · GD112 + ...
GD12 = GD121 + GD122 · ...
...
...
GDxxx= Basic1 +Basic2 + ... + ...

Dependent Boolean variable

$$A\text{-}05 = A \cdot /F \cdot /I \cdot D1$$

Human Reliability Analysis

Human Reliability Analysis

- A structured Approach to Identify potential human failure events (HFEs) and to systematically estimate the probability of those errors using data, models or expert judgment.
- HRA produces:
  - Qualitative evaluation of the factors impacting the quantitative human error probability (HEP)
    - Includes identification of success paths
  - Quantitative human error probability

Categories (types) of Human Errors

- Pre-Initiators (type A):
  - Input to System Models (Fault Trees)
- Initiators (Type B):
  - Input to the Initiating Event Analysis
- Post-Initiators (Type C)
  - Input into Event Tree Analysis

- Other Categorization of Human Errors common (types 1-5, etc).

Pre-Initiators (Latent, Type A).

- Latent human interactions occur during routine maintenance, testing or calibration activities (before an initiating event) where equipment is rendered unavailable.
  - During maintenance, testing or calibration activities, plant personnel may need to disable, isolate, tag out or adjust equipment, which may render the safety function unavailable.
  - Upon completion of the activity, these safety functions need to be restored by realigning the equipment into desired, normal configurations.

Initiators (Type B)

- Human Actions Causing and initiating event. Types include:
  - Transients: Historical data typically includes human interactions in the initiating event frequency.
  - LOCAs: Mostly pipe breaks, so no human interactions.
  - PIEs originated by support system Initiators:
    - May model with initiating event fault trees
    - Support system initiator fault trees may contain human interactions.
    - Development and quantification would be the same as latent dynamic HRA modeling techniques.

Post-Initiators (Dynamic, Type C)

- Dynamic human interactions occurring after an initiator (typically, the most important In a PSA):
  - Consists of cognitive and executive elements
  - Cognitive elements includes:
    - Detection, diagnosis and decision-making
    - Occur in response to some cue: the cue may be the initiating event itself, an alarm, a procedural step or an observation.
    - Execution elements consists of:
      - Manipulation Tasks to implement the action
      - Typically a step in a procedure
    - Subject to time constraints and performance shaping factors.
    - Analyzed in a cue-response time framework.

Pre-Initiators: General Process

- **Identify** routine activities and practices, which if not performed correctly, may adversely impact the availability of mitigating systems.
- **Screen** out activities for which sufficient compensating factors can be identified that would limit the likelihood or consequences of errors in those activities.
- **Define** an HFE for each activity that cannot be screened out, and incorporate these HFEs in the appropriate PRA logic models.
- **Assess** the probability of each HFE with due considerations to dependencies

Pre-Initiators: Quantification Methods

- Accident Sequence Evaluation Program (ASEP) analysis procedure
  - Simplified version of THERP, NUREG/CR-4772
  - Constant HEP
    - Fixed combinations of recovery factors and dependency factors
- Handbook of HRA with Emphasis on Nuclear Power Plant Applications
  - NUREG/CR-1278, Swain
  - Detailed Modeling
  - Applicable to pre-and post initiators

Post Initiators: General Process

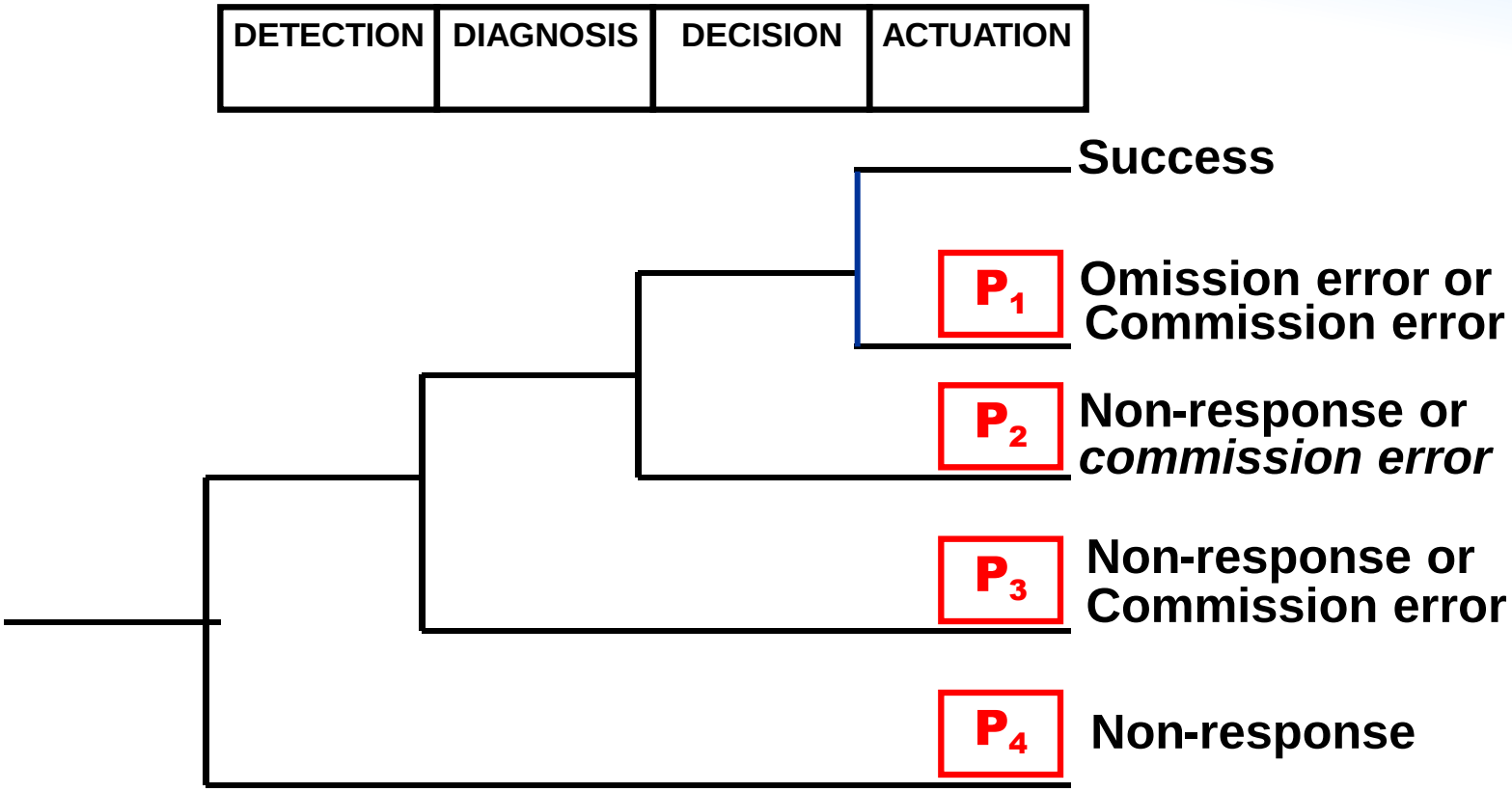
- **Identify** through a systematic review of the relevant procedures the set of operator responses required for each of the accident sequences.
- **Define** human failure events that represent the impact of not properly performing the required responses, consistent with the structure and level of detail of the accident sequences.
- **Assess** the probability of each HFE, addressing specific influences on human performance and potential dependencies among HFEs.
- **Review** the definition of HFEs and their assessments with the PSA team and representatives of the operations staff to ensure that they accurately reflect the plant features, procedures and operating practices.

Post Initiators: Quantification Methods

- THERP:
  - Annunciator Response model
  - Execution Analysis model
- HCR/ORE (EPRI Method TR-100259)
- Cause Based Decision Tree Method
- SPAR-H (NRC NUREG/CR-6883)

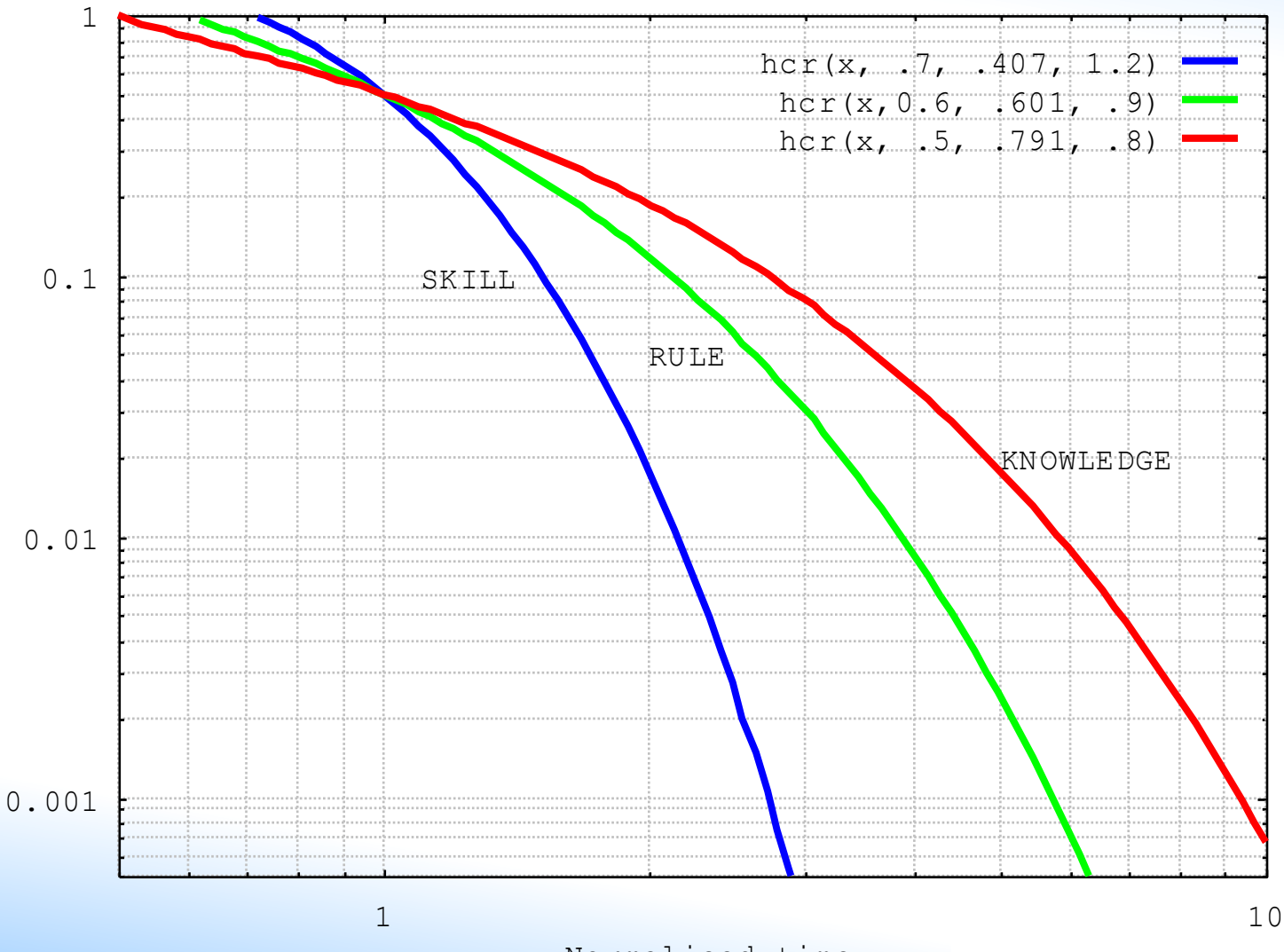
- All of these methods are included in the new EPRI HRA calculator:
  - See WWW.EPRI.COM/HRA/INDEX.HTML

CONTRIBUTIONS TO HUMAN ERROR PROBABILITY (HUMAN ERRORS DURING ACCIDENTAL SITUATIONS)

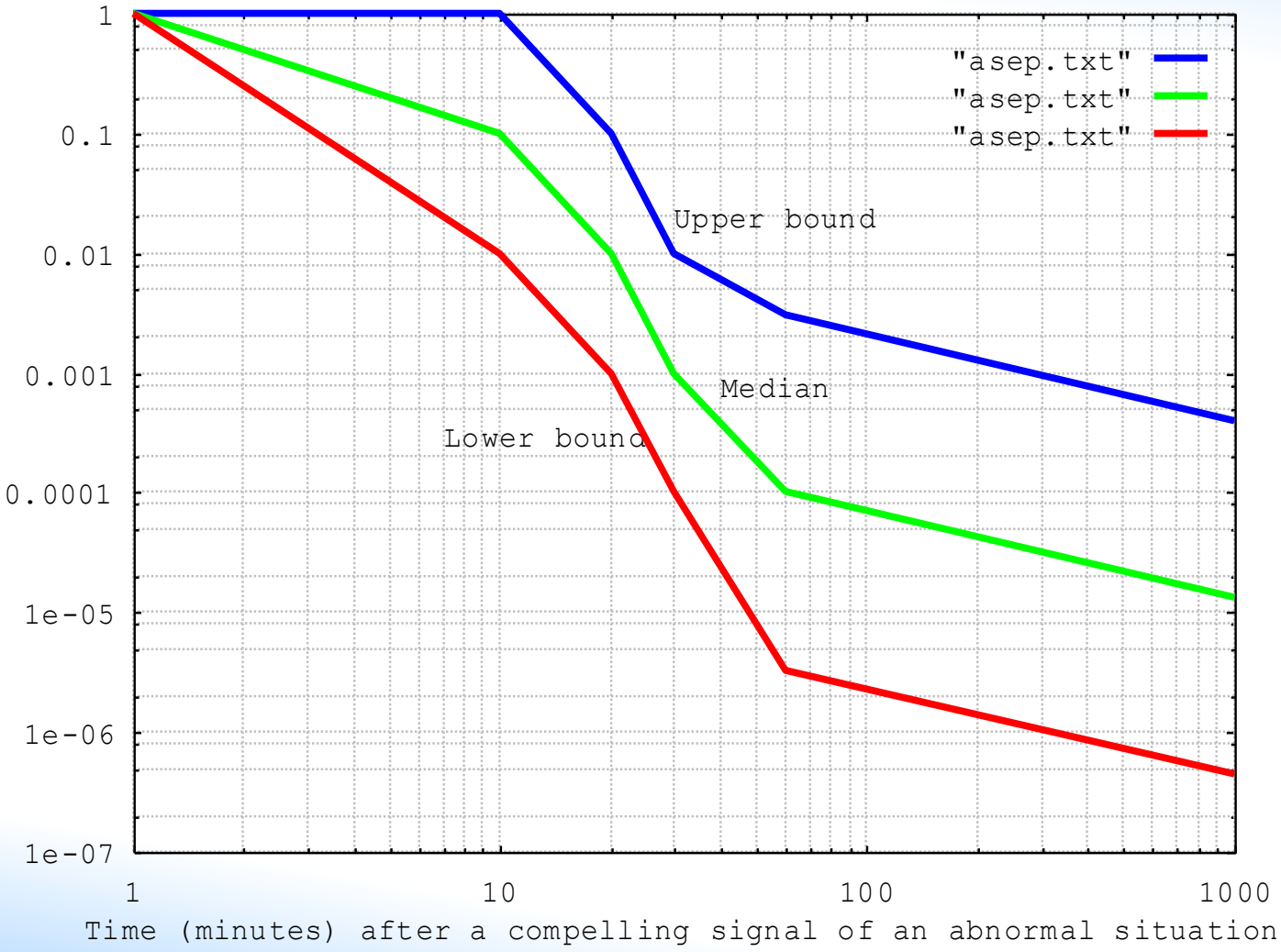


HEP ~ $P_1 + P_2 + P_3 + P_4$
+ the consequences of the commission errors

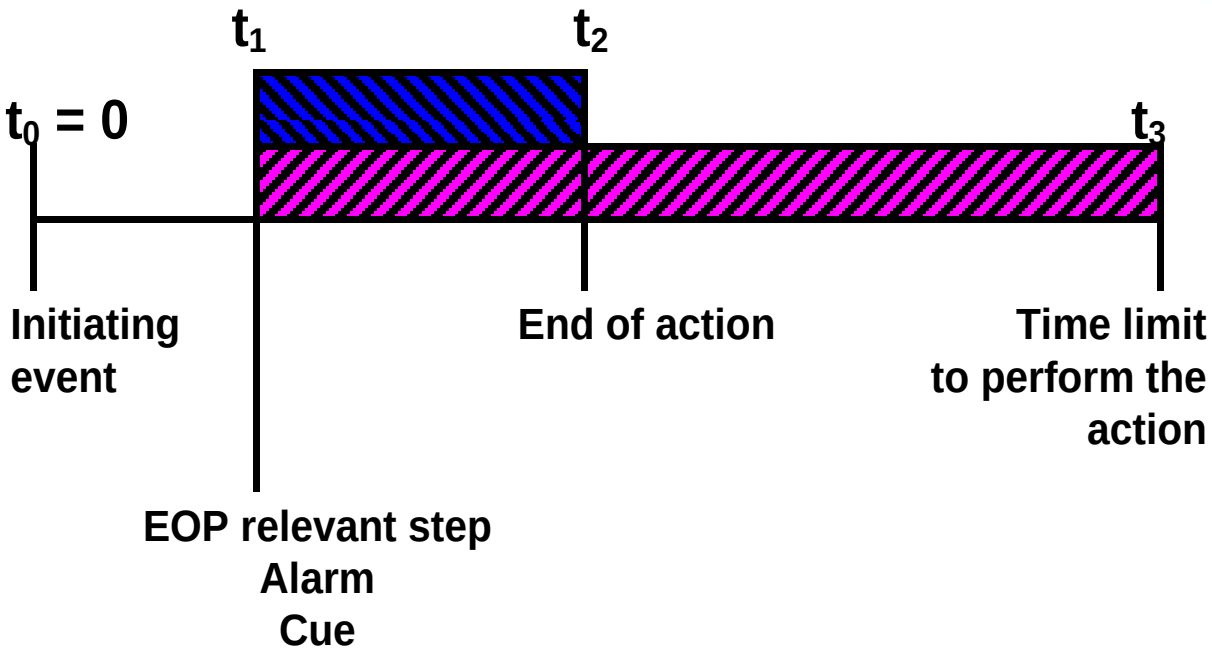
IMPACT OF AVAILABLE TIME AND EVALUATION OF TIME WINDOWS IN HRA HCR (Hannaman & Spurgin, 1984a)



IMPACT OF AVAILABLE TIME AND EVALUATION OF TIME WINDOWS IN HRA(ASEP: Swain, 1987)



IMPACT OF AVAILABLE TIME AND EVALUATION OF TIME WINDOWS IN HRA
HUMAN ACTION OF SHORT EXECUTION TIME



$t_{(A)}$ = Available time = $t_3 - t_1$

$T_{1/2\,(A)}$ = Median time for action = $t_2 - t_1$

GENERAL

- Dependency between two tasks refers to the situation in which the probability of failure of one task is influenced by whether a success or failure occurred on the other task.
- Failure to consider dependencies between human errors can cause a significant underestimation of the Core Damage Frequency.

HUMAN DEPENDENCIES
EXAMPLES OF COUPLING MECHANISMS

- Same person
- Same crew
- Same procedure
- Same procedure step
- Similar action
- Close in time

LEVELS OF DEPENDENCY(*)

- Complete: If action A fails, action B will fail
- High dependency
- Moderate dependency
- Low dependency
- Zero dependency: Probability of failure of action B is the same regardless the failure of or success of task A

(*) NUREG/CR-1278 (THERP), Chapter 10

EXAMPLES OF DEPENDENCIES TO BE CONSIDERED IN HRA

- Between pre-initiating event human actions
- Between post-initiating event human actions
- Between sub-tasks involved in the same action
- Between errors and recoveries
- Between pre and post initiating event human actions

DEPENDENCIES BETWEEN PRE-INITIATING EVENT HUMAN ACTIONS

- Common Cause calibration error events explicitly modelled in the fault trees
- Common Cause misalignments explicitly modelled in the fault trees
- Identification: Analysis of testing and maintenance procedures and schedules

DEPENDENCIES BETWEEN POST-INITIATING EVENT HUMAN ACTIONS

- Actions that appear multiplied in the same accident sequence:
  - Depending on the analysis method used, this may be difficult to determine for low probability cutsets.
  - Many PSAs have developed multi-step solution processes where Human Error Combinations are set to screening (high) probabilities, prior to performing dependency reviews.
- Substitution of the second probability by its dependent value, at cutset level

Failure Data Analysis

Objectives and needs of Reliability Data analyis

The reliability data in a PSA is needed to quantify the PSA and obtain risk estimates. Other wise only qualitative information, such as minimal cut sets or single failures, can be obtained. Reliability data is needed for:

- **Initiating event frequencies**
- **Component failure probabilities**
- **Component outage probabilities**
- Common cause failures (not addressed here)
- Human error probabilities (not addressed here)
- Probability of special basic events (case specific)

PSA results depend exclusively on the model logic and the data. Therefore, an adequate acquisition of reliability data is essential since the data will strongly influence the PSA results.

Type of Reliability Data sources

- Expert judgement
- Generic data sources:
  - National data banks
  - International experience of NPPs of same or different types
  - Wide industry experience
  - Generic data based on expert judgement
- Plant specific experience

Initiating event data

- **For frequent initiating events :**
  - Data can be mainly based on plant specific data. Data can be collected from the incident reporting system. If not enough specific data is available, use generic data. Analyse generic data to account for applicability of generic experience. Use Bayesian analysis if necessary to combine generic experience with plan specific analysis.
  - Always check applicability and quality of generic data sources.
- **For infrequent initiating events:**
  - Perform system analysis to derive system failure frequency, e.g. failure of support systems
  - Perform structural integrity analysis for structural failure rates
  - Otherwise use the generic plant experience that best fits to your needs, or use engineering judgement

Component Failure probabilities
Reliability models used for components in a PSA

1 Components failing to run or fulfilling its function during a given mission time, e.g 24 hours. An exponential distribution of life times is assumed. Failure rates (λ) are to be obtained. Failure probabilities are calculated as:

$$U(t) = 1 - \exp(-\lambda t), \quad t = \text{mission time.}$$

2 Standby components failing to fulfil its mission when they are required. An exponential distribution of life times is assumed. Failure rates (λ) are to be obtained. Mean unavailability between consecutive test is calculated as:

$$\underline{U}(\tau) \sim 1/2\ \lambda\tau\ , \qquad \tau : \text{test interval}$$

3 Components with a constant failure probability per demand. This probability needs to be estimated.

Use of Component Reliability Models

- For components running under normal conditions and during the accident, the failure to run model (1) is used
- For standby components, the standby model (2) is used. If the component needs to work during the accident, the failure to run (1) has to be modelled in addition. Example: A valve of a safety system needs to open (standby model). A pump of the same system needs to start (standby model) and to run during a certain time (failure to run model)
- For components which failure probability is mostly challenged by the number of demands, rather than the idle time, a failure on demand is used. Example: Breakers demanded to close or to open.

1. $U(t) = 1 - \exp(-\lambda t)$, t = mission time.
2. $\underline{U}(\tau) \sim 1/2\ \lambda \tau$, τ : test interval
3. $U = p$, constant probability

Selection of Component Reliability Data

- To the extent possible use plant specific experience, taking into account the resources available.
- Plant data is the most appropriate, but often not available in a usable form.
- If plant experience is small to allow direct confident estimates, a Bayesian update of generic data is recommended
- When necessary, generic data should be carefully selected, taking into account:
  - plant characteristics and similarity of equipment
  - component boundaries, level of detail and failure definitions used in the PSA. The should match with the definitions of the generic sources.
  - Use relatively new data sources professionally developed, and independently reviewed

Gathering plant information to obtain Specific Reliability Data

A typical maximum likelihood estimate for a failure rate (λ) is:

λ = **No. of failures** / **(No. of items x Reference time)**

Therefore, 3 elements of information are needed:

- **An adequate inventory of components**. A large amount of components provides a more confident estimate. However, grouping together components that exhibit some design differences can distort the results.
- **Reference time**, e.g. calendar time or running time, should be adequately selected and estimated. The later can be estimated based on plant computer, counters, etc. For failures on demand, the **number of demands** is to be estimated.
- **Number of failures:** From maintenance records, other plant information
  - More statistical evidence exist for running components than for standby components.
  - Component boundaries in the model need to be taken into account
  - Plant records should be complete, retrievable, well documented.
  - Plant Management support is essential
  - A PSA specialist should do the analysis.Craftsmen do the maintenance and testing, but they may not be the most appropriate person to decide whether a a defect is safety significant or not.

Component Outage probabilities

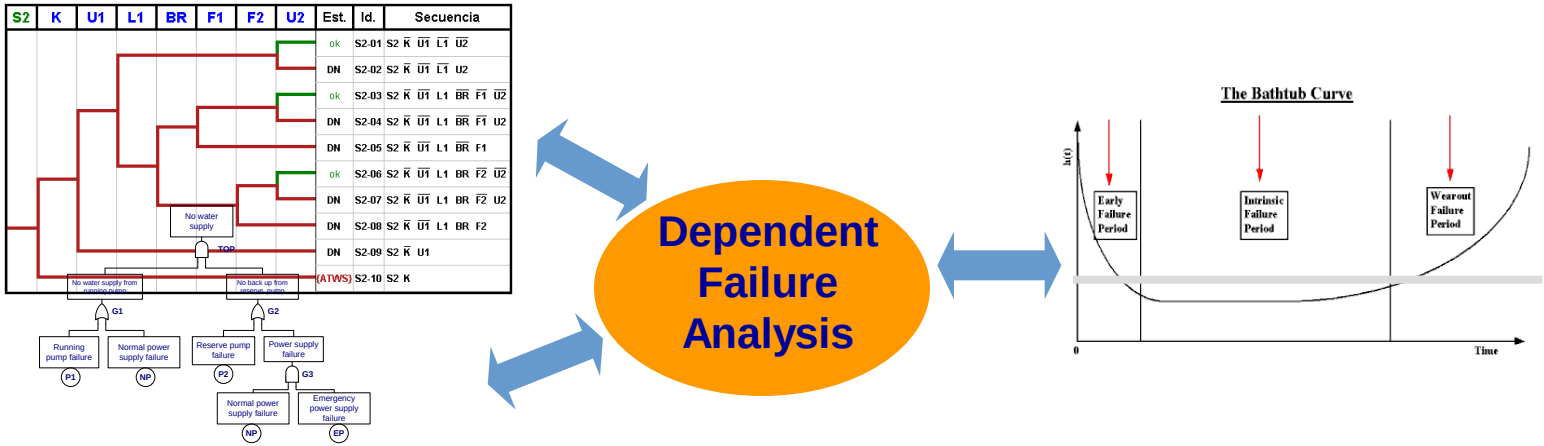
- Component and system outages due to maintenance or testing are analysed and grouped in a number of basic events based on the similar impact on the system functionality due to the realignments required
- Estimates are necessary of the frequency and duration of such outages. These estimates can be derived from maintenance records, periodic test procedures or other plant documentation, or from engineering judgement.
- The average outage time probability is the ratio of the sum of outage times to the total time at power operation.

$$\underline{U} = t_{out} / t_{total}$$

Dependent Failure Analysis

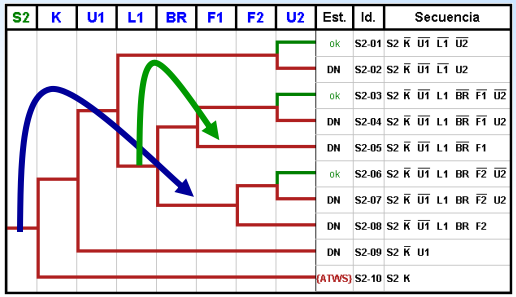
Analysis of Dependent Failures Objectives

- Ensure that dependencies between postulated event are properly treated to avoid underestimation of risk in the PSA.
- Dependency analysis needs to be reflected in the PSA models: Accident sequence analysis (event trees) and system analysis (fault tree). Quantification of common cause failures requires knowledge of component reliability parameters. Coordination of these tasks is essential.



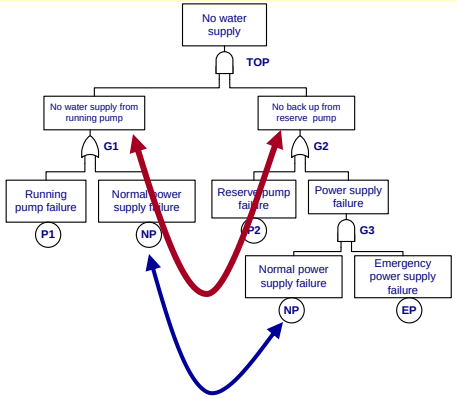
Type of dependencies

Dependencies between initiating event and mitigating system functions
Dependencies of mitigating system functions on failure/success of previous system actuations or human actions:



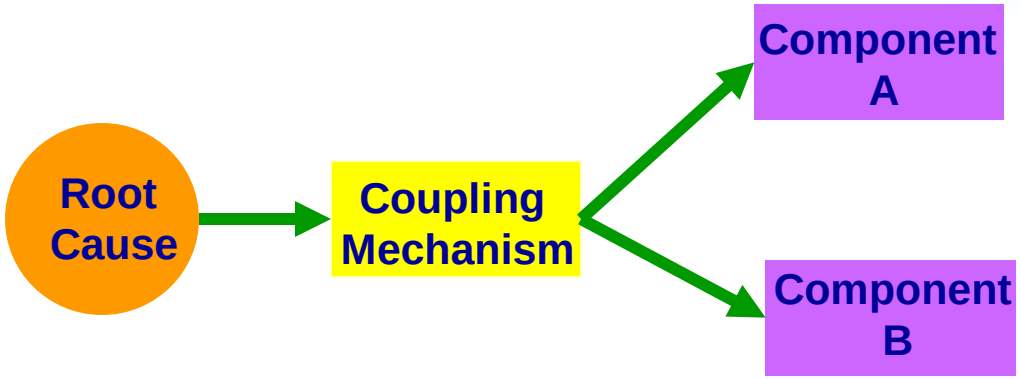
Solution: Adequate treatment in the Event Tree models and documentation

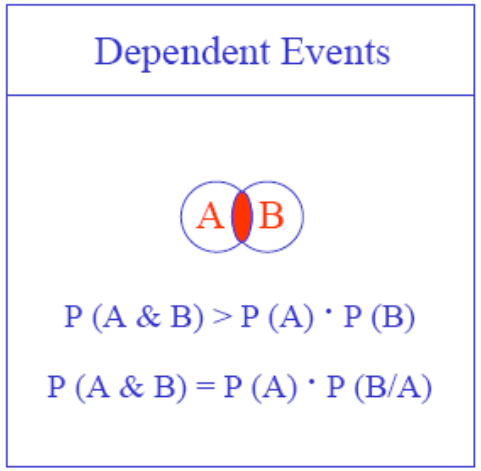
Intersystem dependencies: Functional, spatial, human, etc.
Intrasystem (intercomponent) dependencies: Functional, spatial, human, etc.



Solution: Adequate level of detail in the analysis and explicit postulation of events that affect several systems or redundant components within the system and through support systems

What to do when root causes of common cause failures cannot be model explicitly ?





Solution:

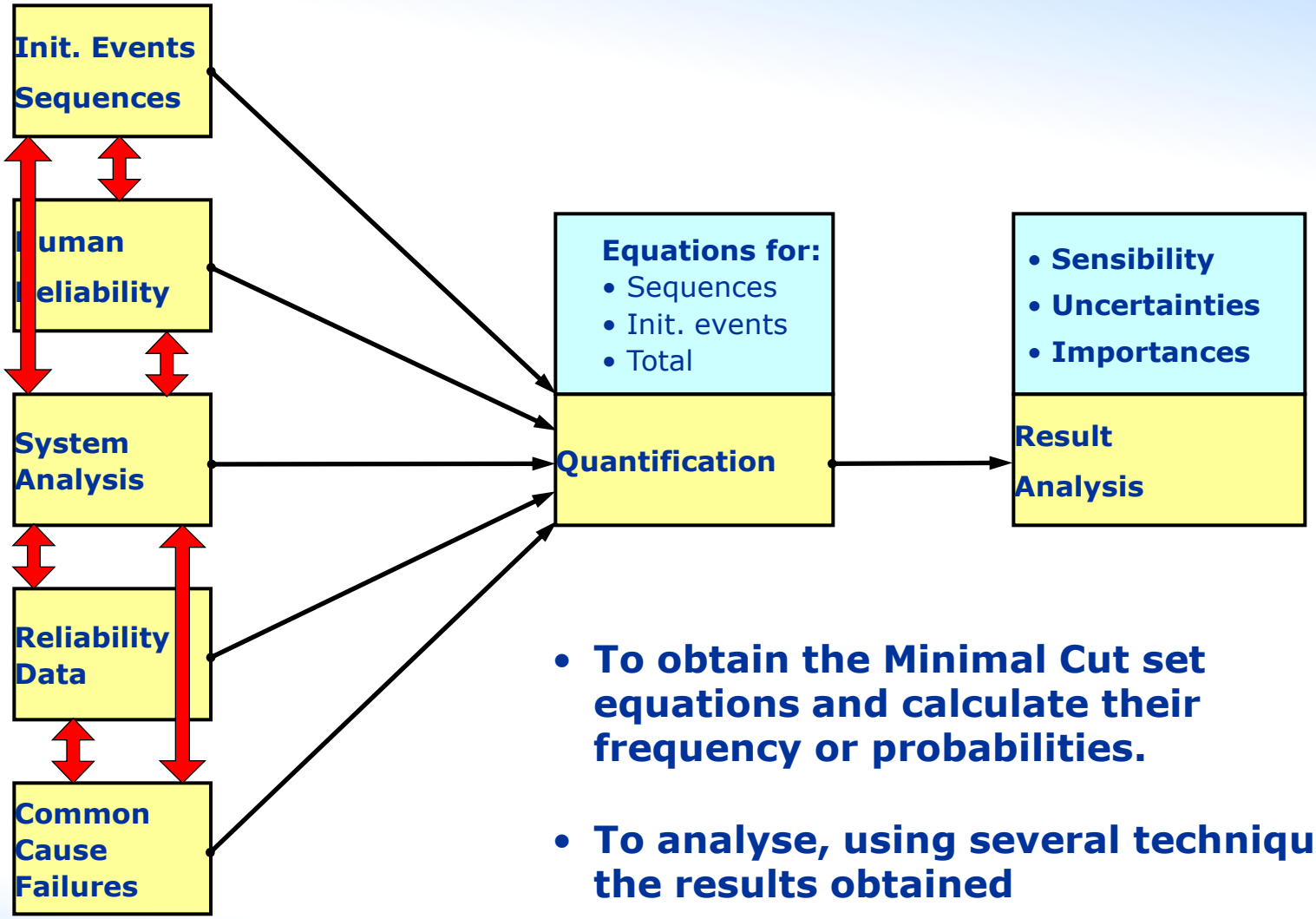
Postulation of common cause failures for dependent components that lump together all common mode failure mechanism that cannot be addressed specifically. Relevant only for redundant equipment, significant if not diverse.

Example: $P(A \& B) = P(A) \cdot P(B) + P(AB_{CCF})$

Probabilistic estimation of common cause failure events (AB_{CCF}) by parametric models: (α Factor, β Factor, MGL, etc.)

PSA Quantification and Analysis of Results

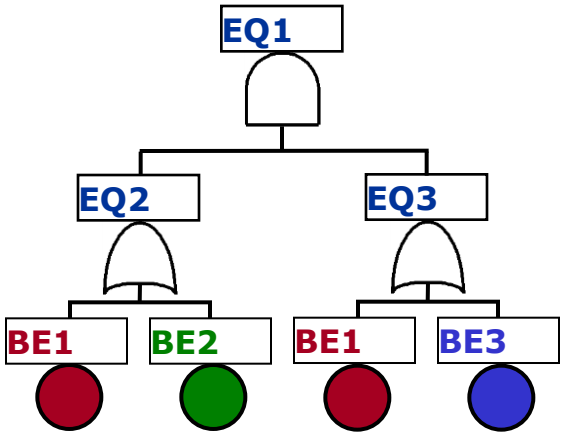
Relations between PSA tasks



- **To obtain the Minimal Cut set equations and calculate their frequency or probabilities.**
- **To analyse, using several techniques, the results obtained**

Fault Tree solution

Minimal cut sets



$EQ1 = EQ2 \cdot EQ3$

$EQ2 = BE1 + BE2$

$EQ3 = BE1 + BE3$

$EQ1 = (BE1+BE2)\cdot(BE1+BE3)$

(original structure function)

$EQ1 = BE1\cdot BE1 + BE1\cdot BE3 + BE2\cdot BE1 + BE2\cdot BE3$

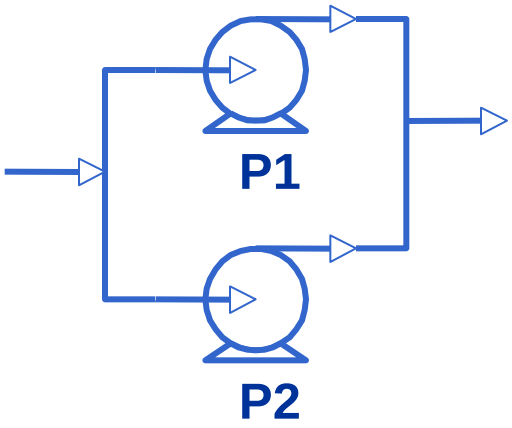
$EQ1 = BE1 + BE1\cdot BE3 + BE2\cdot BE1 + BE2\cdot BE3$

$EQ1 = BE1 + BE2\cdot BE3$

(Disjunctive normal form, suitable for quantification)

System example

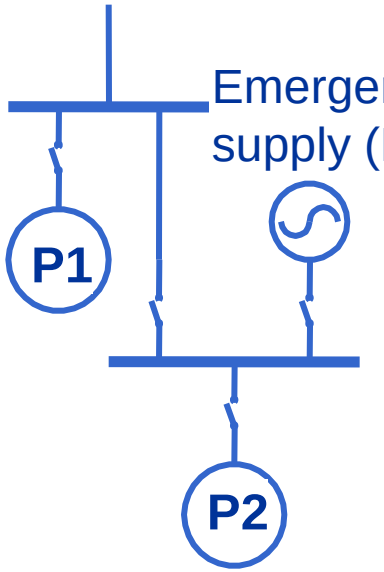
Running pump



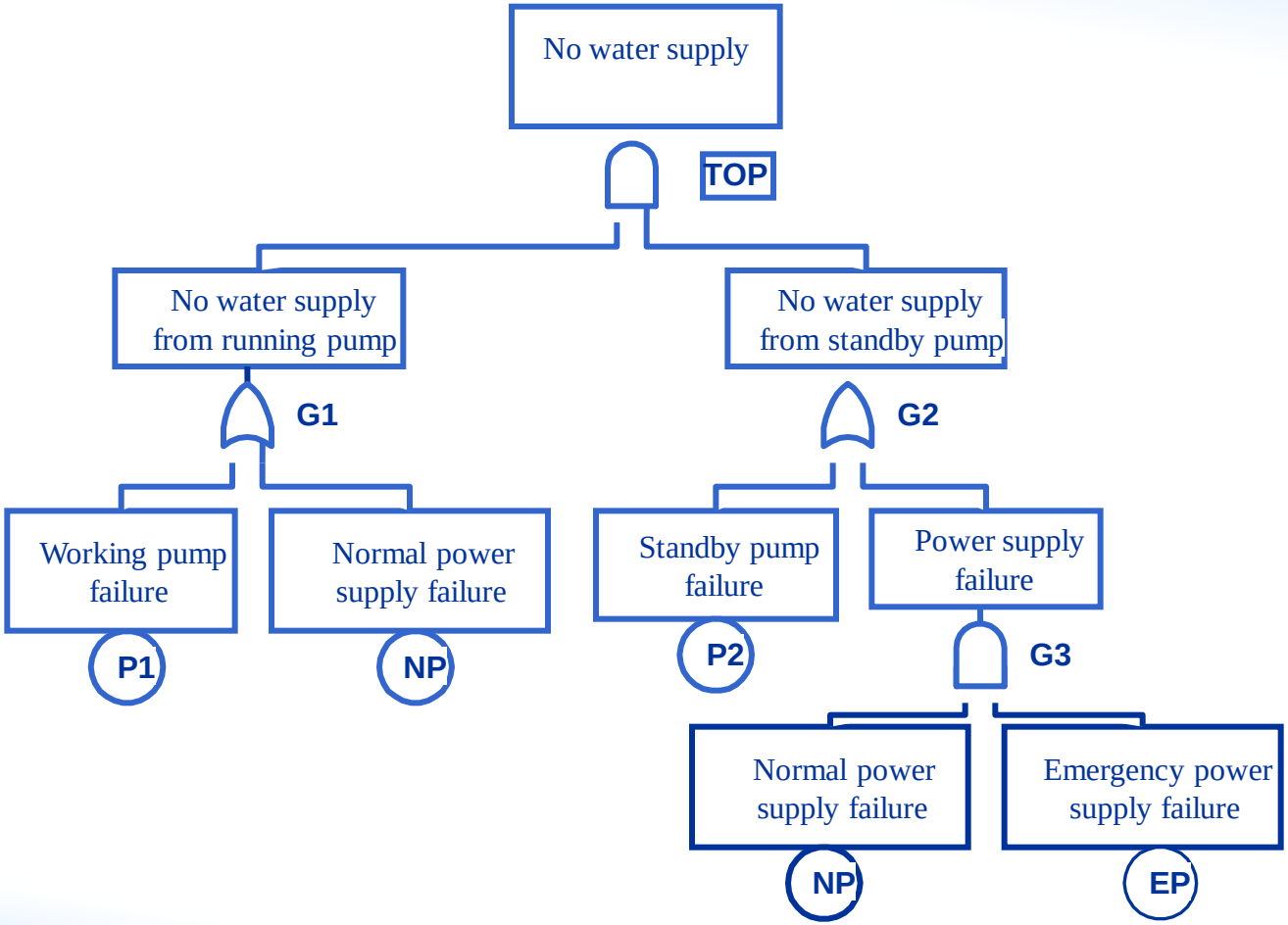
Standby pump

Normal power supply

Emergency power supply (DG)



Fault tree example

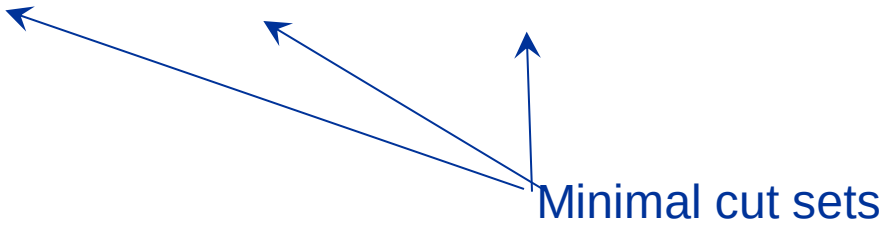


Minimal cut set identification

TOP = G1*G2
G1 = P1+NP
G2 = P2+ G3
G3 = NP*EP

TOP = (P1+NP)*(P2+NP*EP) = P1*P2 + P1*NP*EP + NP*P2 + NP*EP =

P1*P2 + NP*P2 + NP*EP



Global Quantification process

- Obtain the equation for every event tree header, H_i

$Ec(H_i) = f$(Basic events)

- Obtain the equation for each sequence Seq_i, combining those of the headers in failed (H_f) and success states (H_S).

$$Eq(Seqi) = Eq(H_{f1}) \cdot Eq(H_{f2}) \cdot \ldots \cdot /Eq(H_{s1}) \cdot /Eq(H_{s2}) \cdot \ldots$$

- Obtain the equation for the whole event tree of the initiating event IEi, adding the equations of all accident sequences

$$Eq(IEi) = Eq(Seq_1) + Eq(Seq_2) + \ldots$$

- Obtain the total Core damage frequency adding the equations for all the event trees.

$$Eq(Total) = Eq(IE_1) + Eq(IE_2) + \ldots$$

Probability Calculations

- For any pair of events E_1, E_2

$P(E1 \cdot E2) = P(E1) \cdot P(E2|E1)$

$P(E2|E1) = P(E2)$ iff E1 y E2 are independent events, e.g. the basic events of PSA models

- Probability of a Minimal Cut Set C_i with basic events $Be_{1,2,\ldots,n}$

$P(Be1 \cdot Be2 \cdot \ldots \cdot Ben) = P(Be1) \cdot P(Be2) \cdot \ldots \cdot P(Ben)$

- Probability of the sum of any type of events, e.g (minimal cut sets)

$P_E(C1+C2) = P(C1) + P(C2) - P(C1 \cdot C2)$

$P_E(C1+C2) = P(C1) + P(C2) - (P(C1) \cdot P(C2))$ iff $\cap$ C2 = $\varnothing$

$P_E(C1+C2+C3) = P(C1) + P(C2) + P(C3) - P(C1 \cdot C2) - P(C1 \cdot C3) - P(C2 \cdot C3) + P(C1 \cdot C2 \cdot C3)$

(Inclusion-exclusion principle or Poincaré equation)

Reliability upper bounds for Minimal cut set equations

Exact calculations are only affordable for very small systems. Upper bounds are used

- **Rare event upper bound**

  If the basic event probabilities, P(Ci), are low $\Rightarrow$ P(Ci·Cj·...) << P(Ci)

  $$P_{REUB}(C1+C2+...+Cn) \approx P(C1) + P(C2) + ... + P(Cn)$$

  $$P_{REUB} \geq P_E$$

- ***Minimal Cut Set Upper Bound" (only applicable for coherent systems)***

  $$P_{MCUB}(C1+C2+...+Cn) \approx 1 - \prod_{i=1}^{n} (1 - P(Ci))$$

  $$P_{REUB} \geq P_{MCUB} \geq P_E$$

Conditional Core Damage probability, P_{CD}, and Core Damage Frequency, F_{CD}

The former P(Ci) are conditional damage probabilities $P_{CD}(Ci)$ provided that an initiating event has occurred. To obtain the Core Damage Frequency, $F_{CD}(Ci)$, these probabilities have to be multiplied by the initiating event frequency , $F_o(SI)$, assuming they are independent.

$$F_{CD}(Ci) = F_o(SI) \cdot P_{CD}(Ci)$$

Equation for the sequences of an Initiating Event

IE ·Be1 ·Be2 +
IE ·Be3 +
IE ·Be1 ·Be4 ·Be5 +
IE ·Be2 ·Be6 +
⋮ ⋮ ⋮
IE · . . .

$F_{CD}(Ec.) \approx F_o(IE) \cdot \Sigma P_{CD}(Ci)$

Total Core Damage Equation

IE1 ·Be1 ·Be2 +
IE2 ·Be1 ·Be2 +
IE1 ·Be3 +
IE3 ·Be1 ·Be7 ·Be9 +
⋮ ⋮ ⋮
IEn · . . .

$F_{CD}(Ec.) \approx \Sigma (F_o(IEi) \cdot P_{CD}(Ci))$

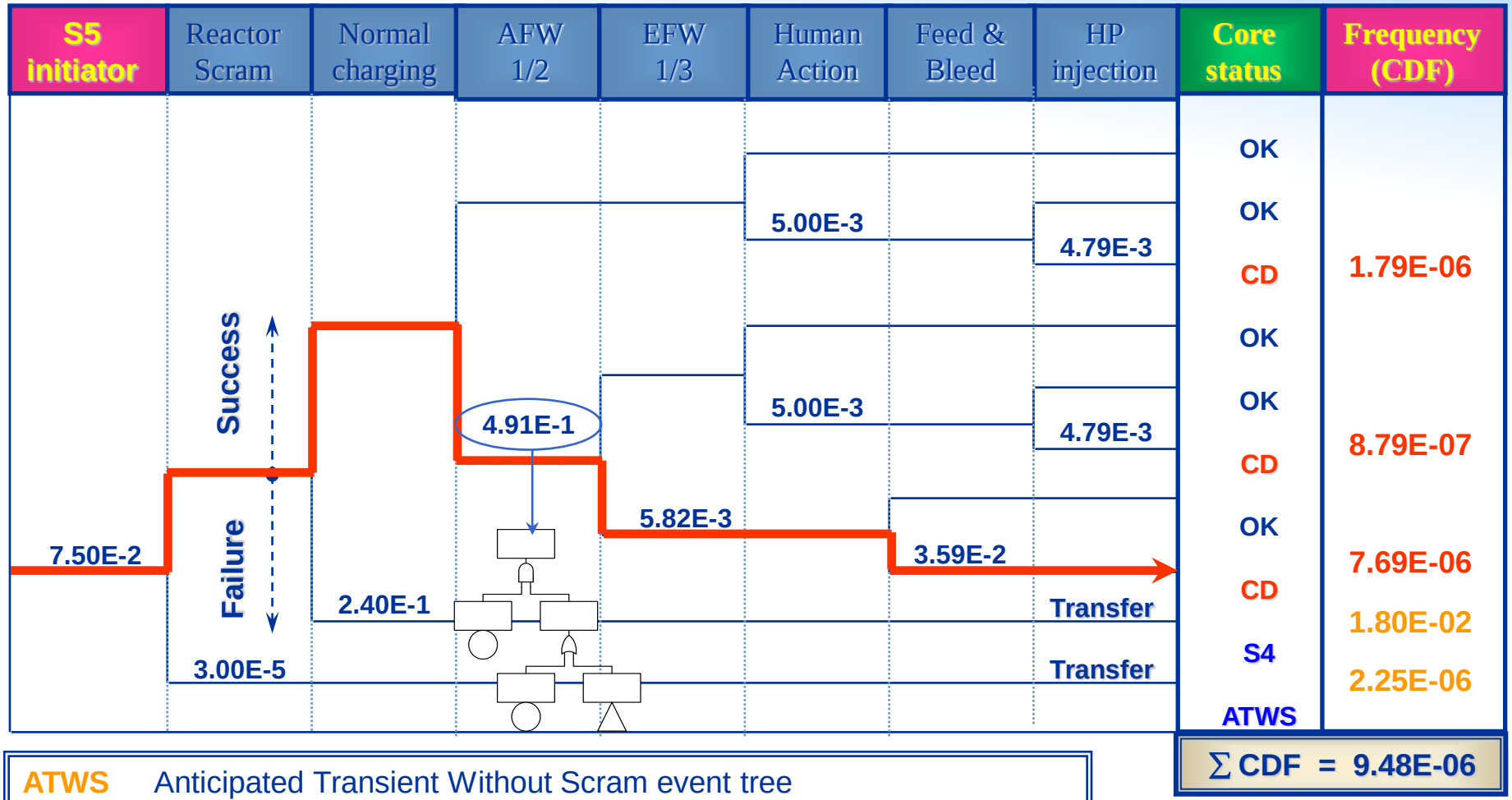
Truncation (cut off)

- The Boolean equations have astronomical numbers of minimal cut sets. Therefore, it is necessary to eliminate those minimal cut sets that make a negligible contribution to risk estimates. For this purpose, a truncation threshold is established to eliminate negligible parts of the equation during the development of the equations.

- Usual truncation values with respect to the core damage frequency range from

$$10^{-8}/\text{year} \quad \text{to} \quad 10^{-10}/\text{year}$$

Example of Event Tree - Very Small LOCA



ATWS	Anticipated Transient Without Scram event tree
S4	Small LOCA initiator group event tree
S5	Initiating event (Very Small LOCA)

CD = Core Damage State

OK = Core Safe State

Final Objective: Core damage equation >> Core damage frequency and dominant risk contributors

- Initiating event
- Basic events

  Different codes for:

  - Human errors
  - Hardware failures
  - Component outages

They are independent Boolean variables

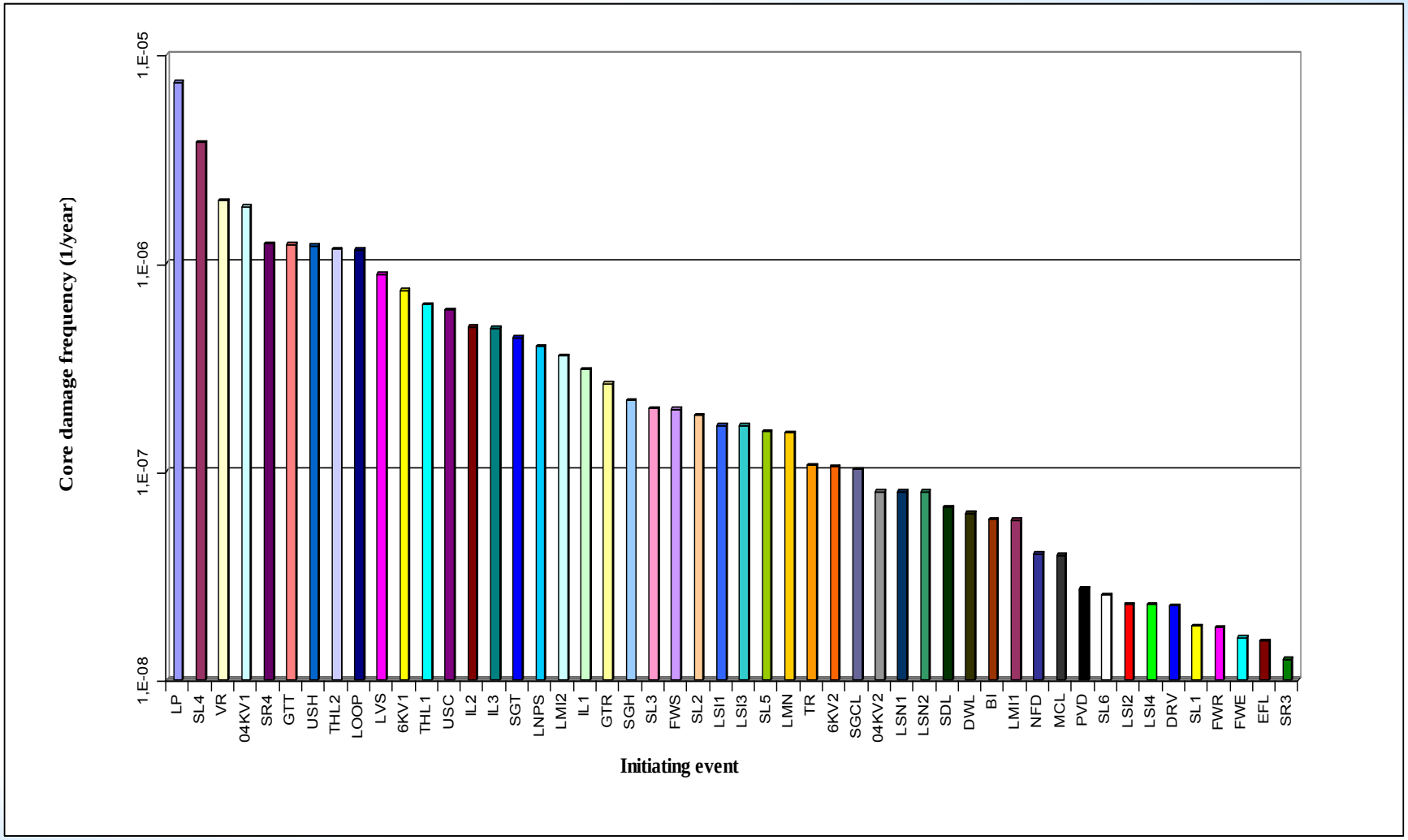
Sucesos		
S1	· 1FOIHRECAH	
T2	· 1FD1EDYBLH	· 1FOAACONTH
T9A	· 1ONBVEGCDF	
S2	· 1F1IHRECAH	
RT	· 1FORRMANUH	
RT	· 1F1AISPREH	· 1FDREFDESH
T4	· 1FD1EDYBLH	· 1FOAACONTH
S2	· 1BM14001AL	
T2	· 1ONBVEGCAF	· 1P1PKTRNBP
T2	· 1ONBVEGCDF	· 1P1PKTRNAP
T3	· 1FD1EDYBLH	· 1FOAACONTH
T9A	· 1FORSAPOYH	· 1ONBVEGCDF
T9A	· 1FOIHAPOYH	· 1ONBVEGCDF
T8	· 1FD3EDYBLH	· 1FOAACONTH
V		
A	· 1VM140005A	· 1VM1453REK2
T2	· 1ONBVEGCAF	· 1ONBVEGCDF
RV		
S2	· 1VM161214K	· 1VM161214L
S2	· 1VM1115BDK	· 1VM1115BDL

Total Core Damage Equation

Núm.	FDN (/año)	FDN acum.	Sucesos
1	4.87e-6	8.5 %	S1 · 1FOIHRECAH
2	4.04e-6	15.6 %	T2 · 1FD1EDYBLH · 1FOAACONTH
3	3.86e-6	22.4 %	T9A · 1ONBVEGCDF
4	2.77e-6	27.3 %	S2 · 1F1IHRECAH
5	1.37e-6	29.7 %	RT · 1FORRMANUH
6	8.92e-7	31.2 %	RT · 1F1AISPREH · 1FDREFDESH
7	8.22e-7	32.7 %	T4 · 1FD1EDYBLH · 1FOAACONTH
8	7.65e-7	34.0 %	S2 · 1BM14001AL
9	6.79e-7	35.2 %	T2 · 1ONBVEGCAF · 1P1PKTRNBP
10	6.79e-7	36.4 %	T2 · 1ONBVEGCDF · 1P1PKTRNAP
⋮	⋮	⋮	⋮ ⋮ ⋮
302	2.91e-8	82.2 %	A · 1TU10LRF1B · 1VM15008BO
303	2.90e-8	82.3 %	T1 · 1NECALMO · 1SQSQYK02F · 1VA100037C
304	2.90e-8	82.3 %	T9A · 1F1FEDYBLH · 1ONBVEGCDF
305	2.89e-8	82.4 %	T1 · 1CF360001I · 1GDGD000BR · 1TB360001S
306	2.82e-8	82.4 %	RT · 1FOILREP3H · 1FOVPPORVH
307	2.82e-8	82.5 %	T2 · 1FDOEDYBLH · 1FOAACONTH · 1FODISBRRH
308	2.82e-8	82.5 %	RT · 1CBBVA402F · 1F1AISPREH
309	2.82e-8	82.6 %	RT · 1CBBVA103F · 1F1AISPREH
310	2.79e-8	82.6 %	T1 · 1BM430003L · 1M2AA00B2M
311	2.78e-8	82.7 %	T2 · 1F1FEDYBLH · 1M2AA00B2M · 1VK360018L
⋮	⋮	⋮	⋮ ⋮ ⋮

5.70E-5 /año

Example of risk profile for different initiating events



Importance Measures for Basic Events

P_R **P**robability of **R**eference Equation

P_0 **P**robability of the Equation given that P(BE)=**0** => never fails

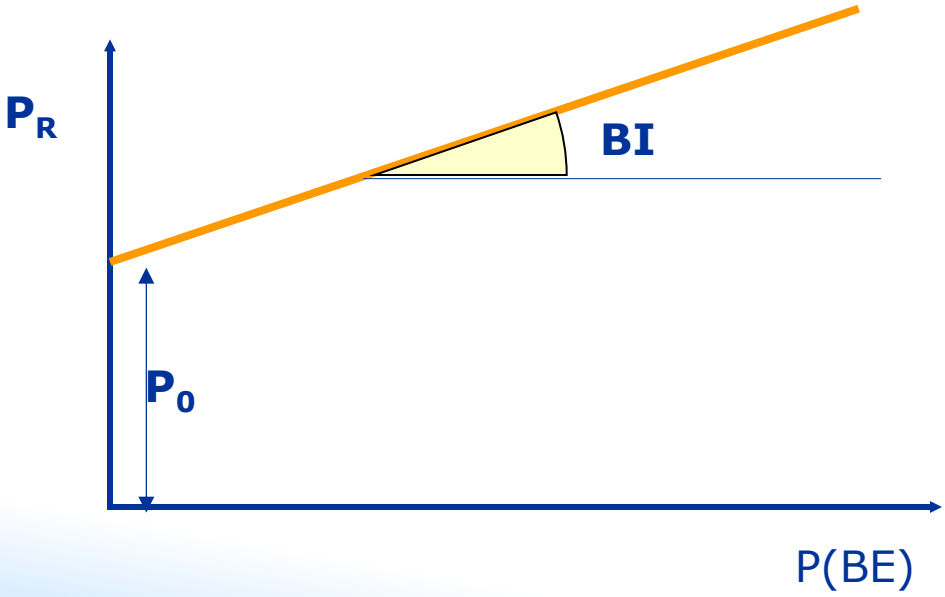
P_1 **P**robability of the Equation given that P(BE)=**1** ≈> has failed

- **Birnbaum, BI**

$$\mathbf{BI}(BE) = \frac{P_1 - P_0}{P_R}$$

$$\mathbf{0} \le \mathbf{BI} \le \infty$$

Fractional contribution of the Basic event to the equation probability; It is partial derivative of the equation with respect to the basic event probability.



Sensitivity analysis with respect to a single basic event probability

equivalent

to Birnbaum importance

Other Common Importance Measures

P_R **P**robability of **R**eference Equation

P_0 **P**robability of the Equation given that P(BE)=**0** => never fails

P_1 **P**robability of the Equation given that P(BE)=**1** ≈> has failed

- **Fussell-Vesely, FV**

$$\mathbf{BI}(BE) = \frac{P_R - P_0}{P_R}$$

$\mathbf{0 \le FV \le 1}$ $0\% \le FV \le 100\%$

Basic event contribution to the equation probability; It is the relative reduction of the Equation probability in case that the basic event would never happen.

- **Risk Reduction Worth, RRW**

$$\mathbf{RRW}(BE) = \frac{P_R}{P_0}$$

$\mathbf{1 \le RRW \le} \infty$

It is the reduction factor in the equation probability that would be achieved if the event would never occur (the component would never fail)

- **Risk Achievement Worth, RAW**

$$\mathbf{RAW}(BE) = \frac{P_1}{P_R}$$

$\mathbf{1 \le RAW}$

It is the incremental factor in the equation probability that would be obtained if the event happens for sure (≈).

Use of importance measures

- To appreciate the significance of risk contributors, that may be diluted in a large amount of cut sets
- To rank safety significance of plant features
- To estimate the risk impact of removing equipment from service (risk achievement worth)
- To bound the risk benefits from proposed component improvements (risk reduction worth)
- To evaluate the impact of some precursor events

- The effect of multiple changes cannot be evaluated on the basis of single importance measures.

Sensitivity Analysis

- **How would the PSA results change if …?**
  - Modelling assumptions or success criteria are changed
  - The reliability data of a certain type of equipment is changed
  - Some components are more or less frequently tested
  - The fuel cycle duration is enlarged
  - No maintenance is carried out for some equipment
  - If the operators would be infallible?
  -
  -
  -

- In some cases the Sensitivity Analysis just affects the data or parameter involved in the basic event probability calculations and a reassessment of the already obtained core damage equation would be enough. When the changes introduce significant distortion of the data or the models, such as changes of success criteria or modelling assumptions, it would be necessary to modify the models and recalculate again the whole PSA.

Uncertainty Analysis

- Sources of uncertainty:
  - Reliability Data and other data
  - Model limitations
  - Modeling assumptions
  - Knowledge of physical phenomena
  - Truncation
  - Other
- How to account for the impact of uncertainties on PSA results. Limited tools:
  - Sensitivity analysis for single or combined factors
  - Propagation of uncertainty of input data
  - Expert judgment, ??

Uncertainty Analysis

- The component reliability data and other probabilities of basic events used in the calculations are not exactly known. There is a certain degree of uncertainty in their estimations. These uncertainties can be characterised by a distribution function (normal, lognormal, gamma...) of the parameters used in the model instead of the mean fixed value used.

- Los calculations formerly done with the **mean values** of the distributions provided a result known as a **"Point Estimate Value".**

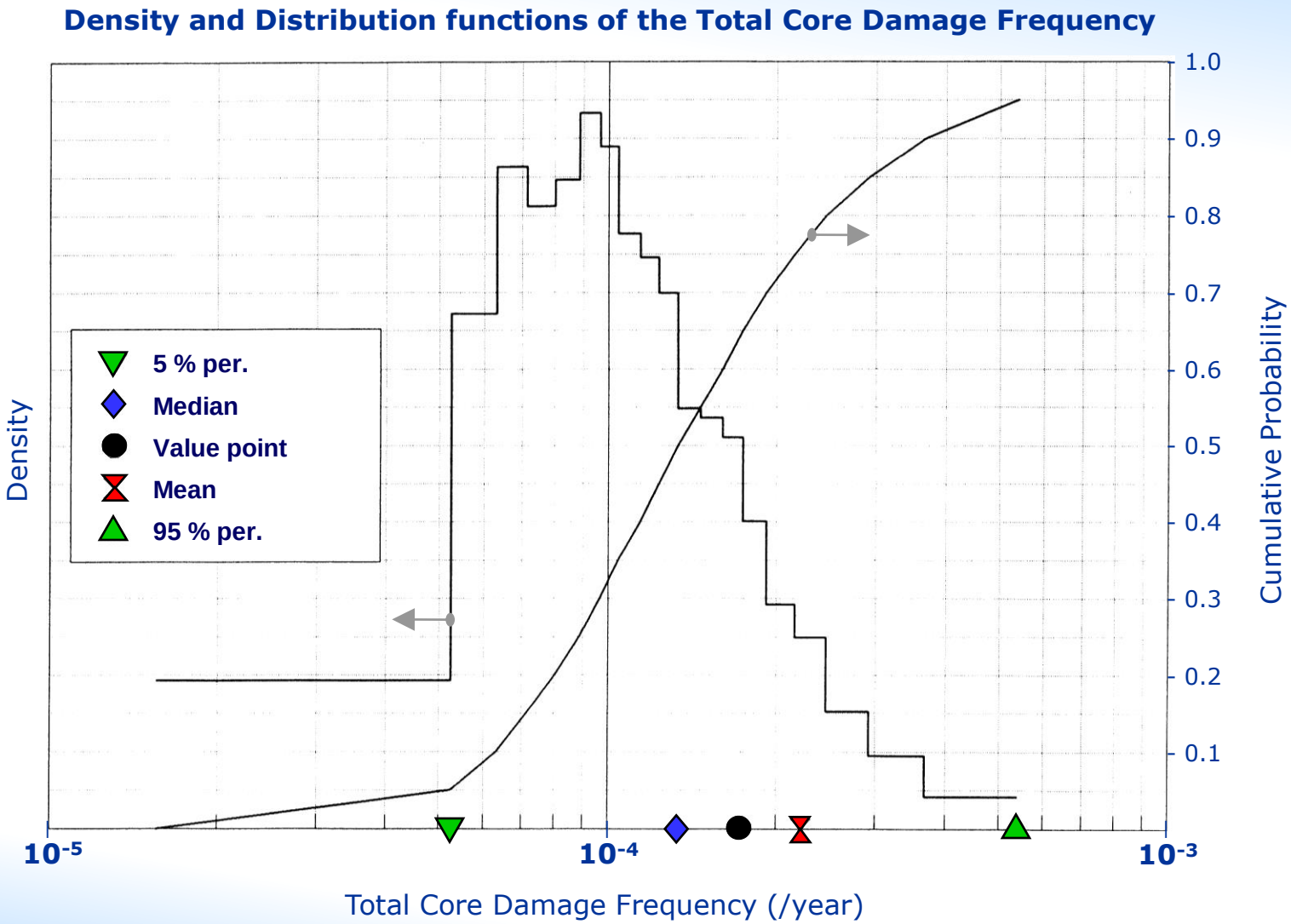
- The uncertainty of the input parameters can be propagated through the model to obtain a distribution of the core damage frequency. The **mean value** of the core damage frequency distribution is not the same than its **Point Estimate Value.**

- The propagation of the uncertainty of basic event reliability estimates to the PSA results can very hardly be done analytically in some simple cases. Therefore, Monte Carlo simulation with several sampling techniques are used to obtain an uncertainty distribution of the core damage frequency. After a sufficient amount of simulation trials a table distribution or histogram of the PSA results can be obtained. From it, the mean and median values and percentiles can be derived.

Propagation of uncertainty in reliability data

- Origin of data uncertainties:
  - Interpretation and classification of failure events
  - Determination of demands, running or exposure time, applicable population, etc.
  - Size of data sample (statistical uncertainty)
  - Mathematical models
- Propagation methods:
  - Analytical methods: Limited application
  - Simulation methods: Broadly use for different distributions and sampling techniques.
- Correlation of data uncertainties:
  - Common sampling for components sharing the same data. Sensitivity analysis for single or combined factors
  - Adequate use of sampling methods and random number generation.
- Remarks:
  - Mean value of the CDF distribution is different from the point estimate CDF
  - Redundant design reduces the uncertainty. Series design increases it.

Example of Uncertainty Analysis Results



Summary

- In the PSA Quantification Task, all the models and products of previous PSA tasks (Accident sequence Analysis, System Analysis, Data Analysis, …) are used and linked together. The Boolean models are transformed into a logical equivalent form (containing minimal cut sets) that allows to estimate probabilities or frequencies for parts of the models or the whole PSA.

- The size and complexity of the models for a NPP PSA is such that simplifications or approximations must be done to be able to quantify the models with an acceptable effort. Such approximations are well known and reasonable, and don't question the validity of the PSA results.

- Once the PSA results and the Boolean equations in terms of Minimal Cut Sets are known, several techniques are used to analyse the PSA results. Especially useful for that purpose are the Importance Measures of the Basic Events, since they reveal the basic events that mostly contribute to the plant risk and how sensible are the PSA results to changes in their probabilities.

IAEA 60 Years
Atoms for Peace and Development

Thank you!