IAEA
International Atomic Energy Agency
Atoms for Peace and Development

Workshop on the Application of Level 1 Probabilistic Safety Assessment, 5 - 9 September 2022, Bangkok, Thailand

P1. Overview of Level 1 PSA

Gurgen KANETSYAN
Head of Risk Assessment Group
Nuclear and Radiation Safety Centre
E-mail: g.kanetsyan@nrsc.am

Outline

- Background of Level 1 PSA
- General methodology of Level 1 PSA
  - Main tasks (IE, ET, FT, HRA, etc.)
  - General aspects of operational modes
  - General aspects of internal and external hazard PSA
  - Interpretation of PSA results
- Level 1 PSA project organization

Background

- Risk is the possibility of suffering damage. It is inseparably associated with human existence.
- In engineering the objective of risk assessment is to:
  - identify sources of risk,
  - quantify the risk resulting from them,
  - develop and implement measures to reduce it.
- Final goal of risk assessment is to create appropriate base for safety-related decision-making process

Background

- Risk assessment answers three basic questions:
  1. **What** can go wrong?
  2. **How frequently** does it happen?
  3. What are the **consequences**?

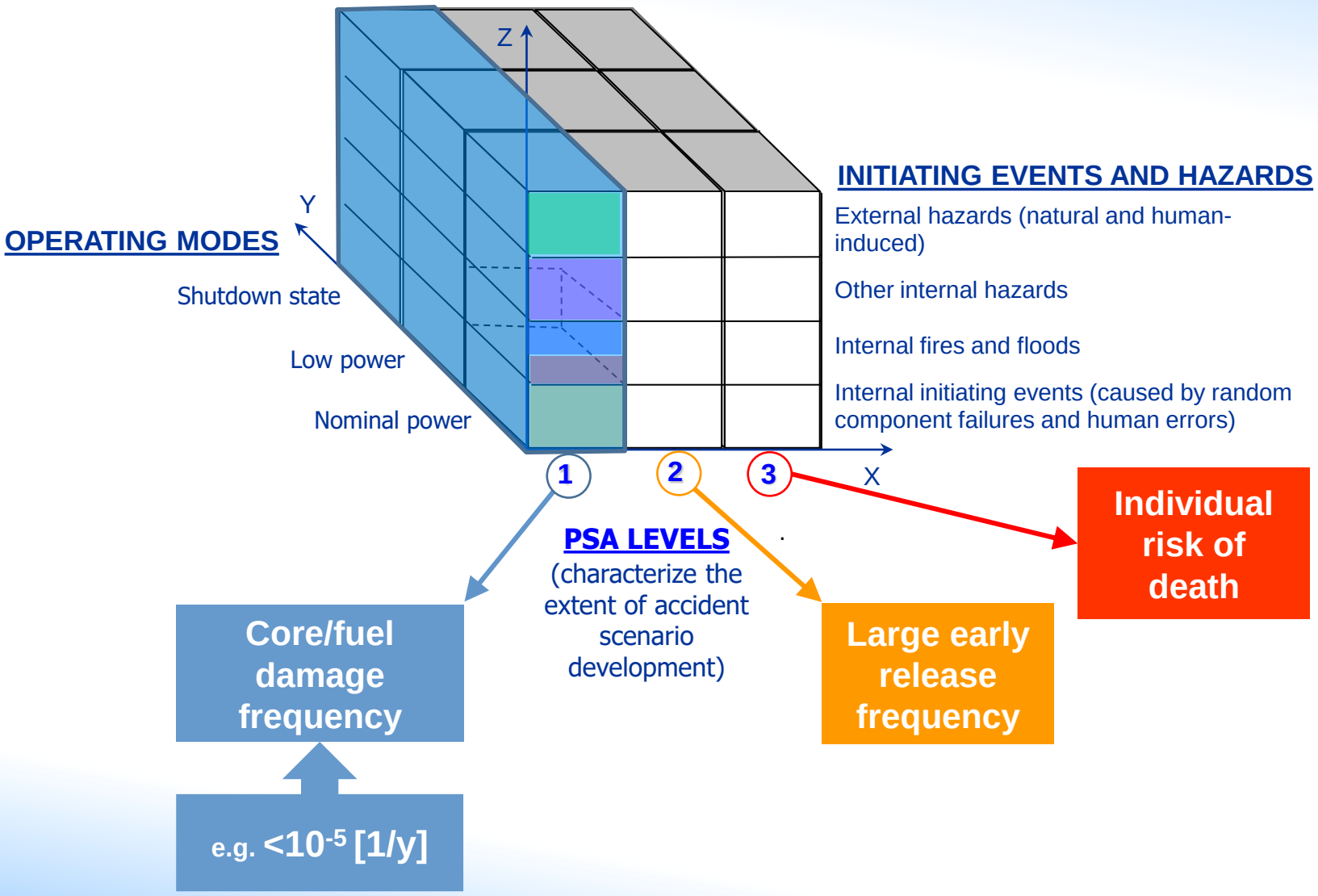
- The most famous risk assessment technique is probabilistic safety assessment (PSA)
  - Concentrate mainly on BDBA risk
  - Allow to analyze entire spectrum of possible accident scenarios
  - Allow to obtain risk profile for NPP

- PSA is used in different industries: Aviation, Oil&Gas, Transport, etc.

Background

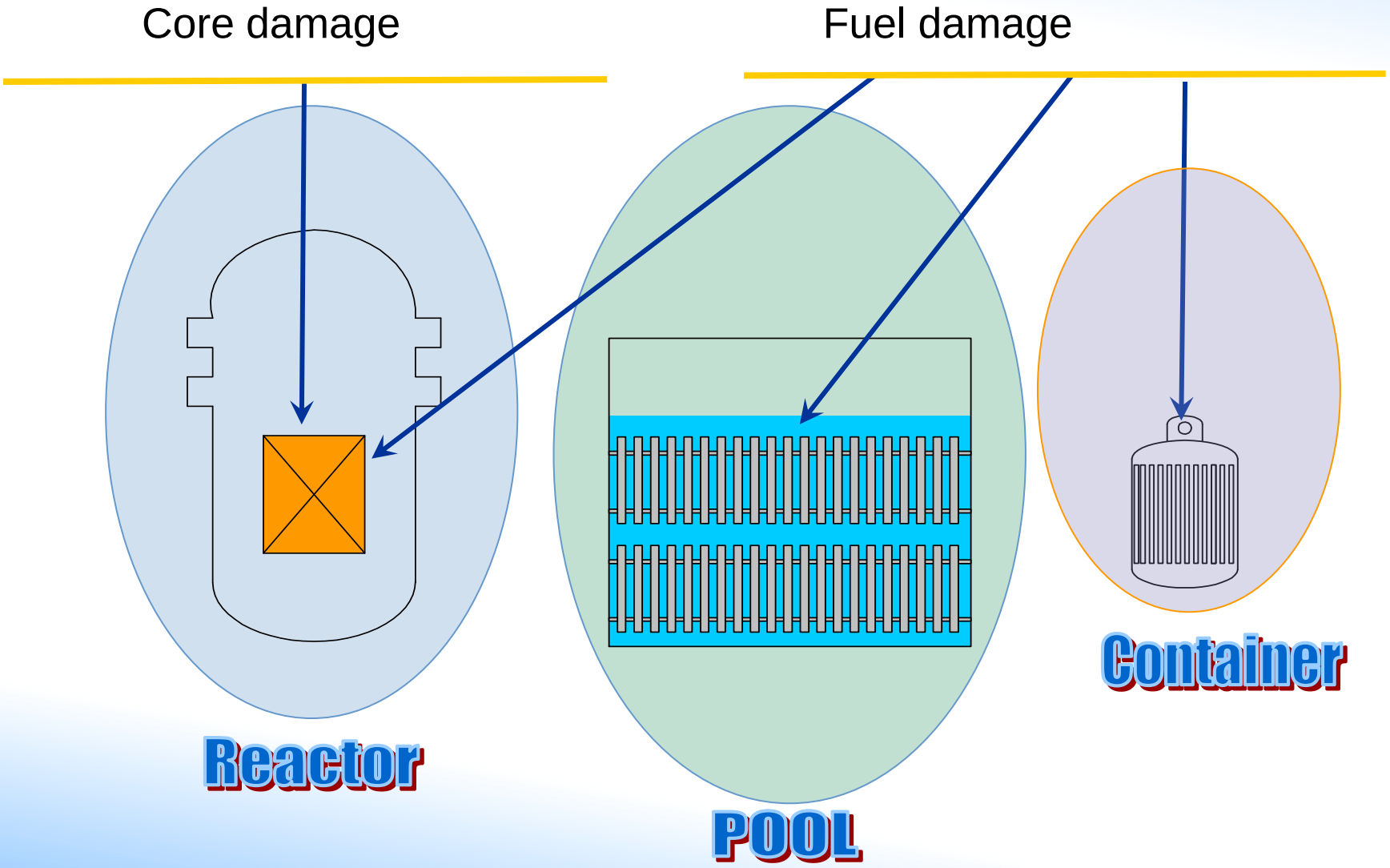
- Objectives of PSA are:
  - Estimation of the frequency for undesirable event
  - Identification of the initiating events and dominant accident sequences with the highest contribution to the undesirable event frequency (risk profile)
  - Identification of weaknesses or vulnerabilities in plant systems design and operation
  - Preparing input for safety-related decision making

Background

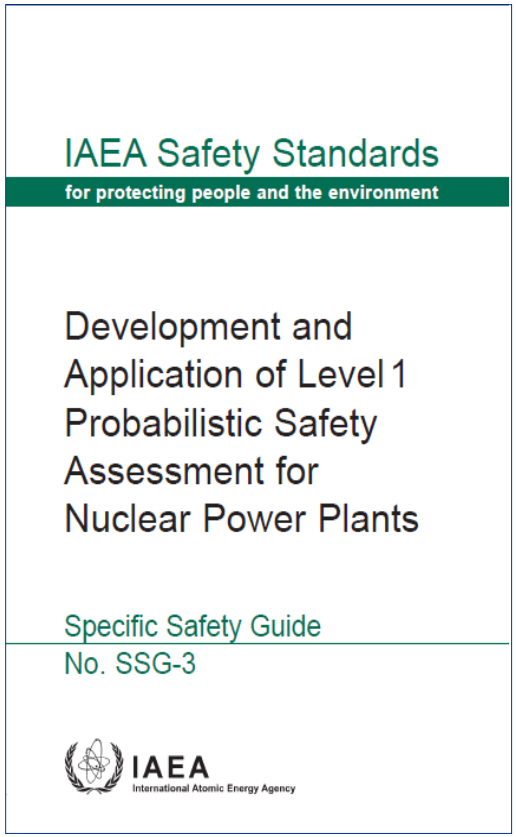

Z
Y
X
OPERATING MODES
Shutdown state
Low power
Nominal power
INITIATING EVENTS AND HAZARDS
External hazards (natural and human-induced)
Other internal hazards
Internal fires and floods
Internal initiating events (caused by random component failures and human errors)
1
2
3
PSA LEVELS
(characterize the extent of accident scenario development)
Core/fuel damage frequency
Large early release frequency
Individual risk of death
e.g. <10-5 [1/y]

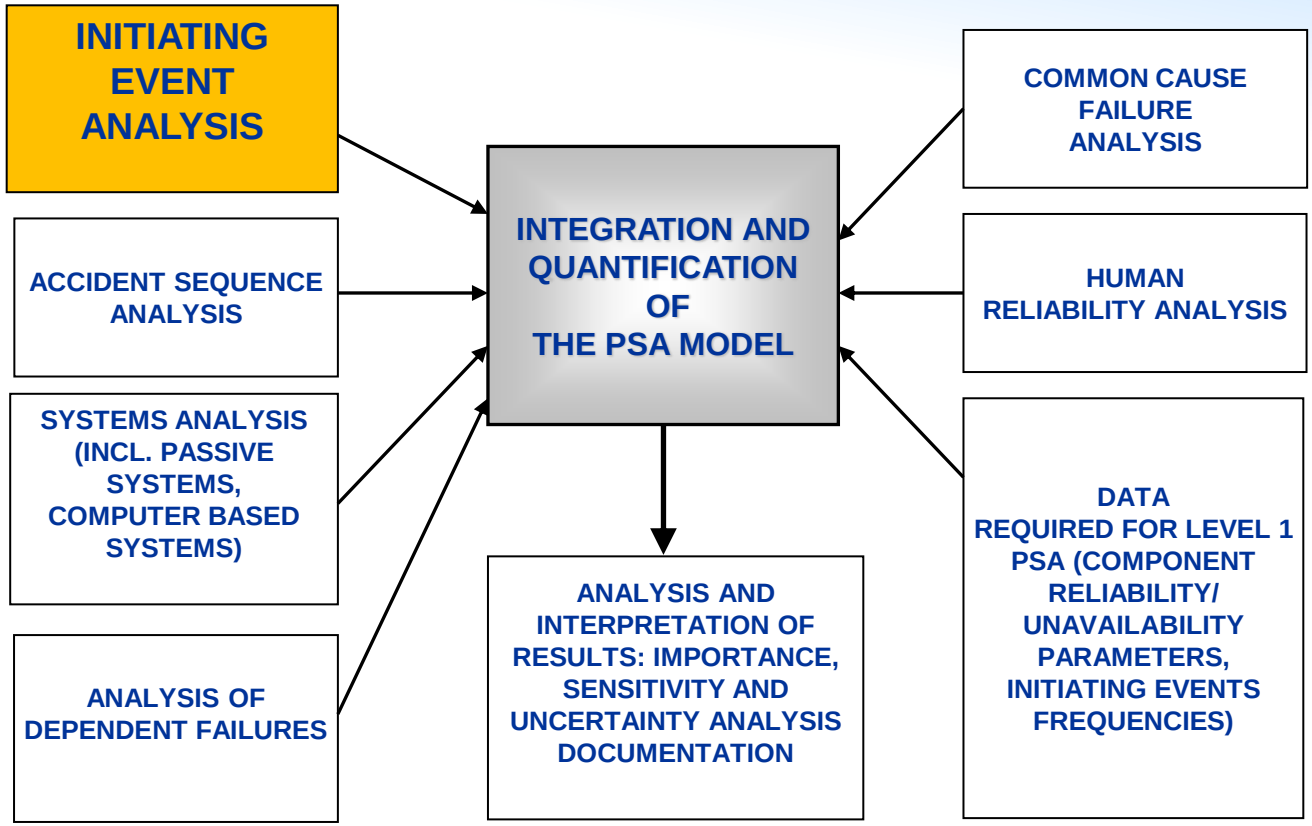
Background

LOCATION OF IRRADIATED FUEL

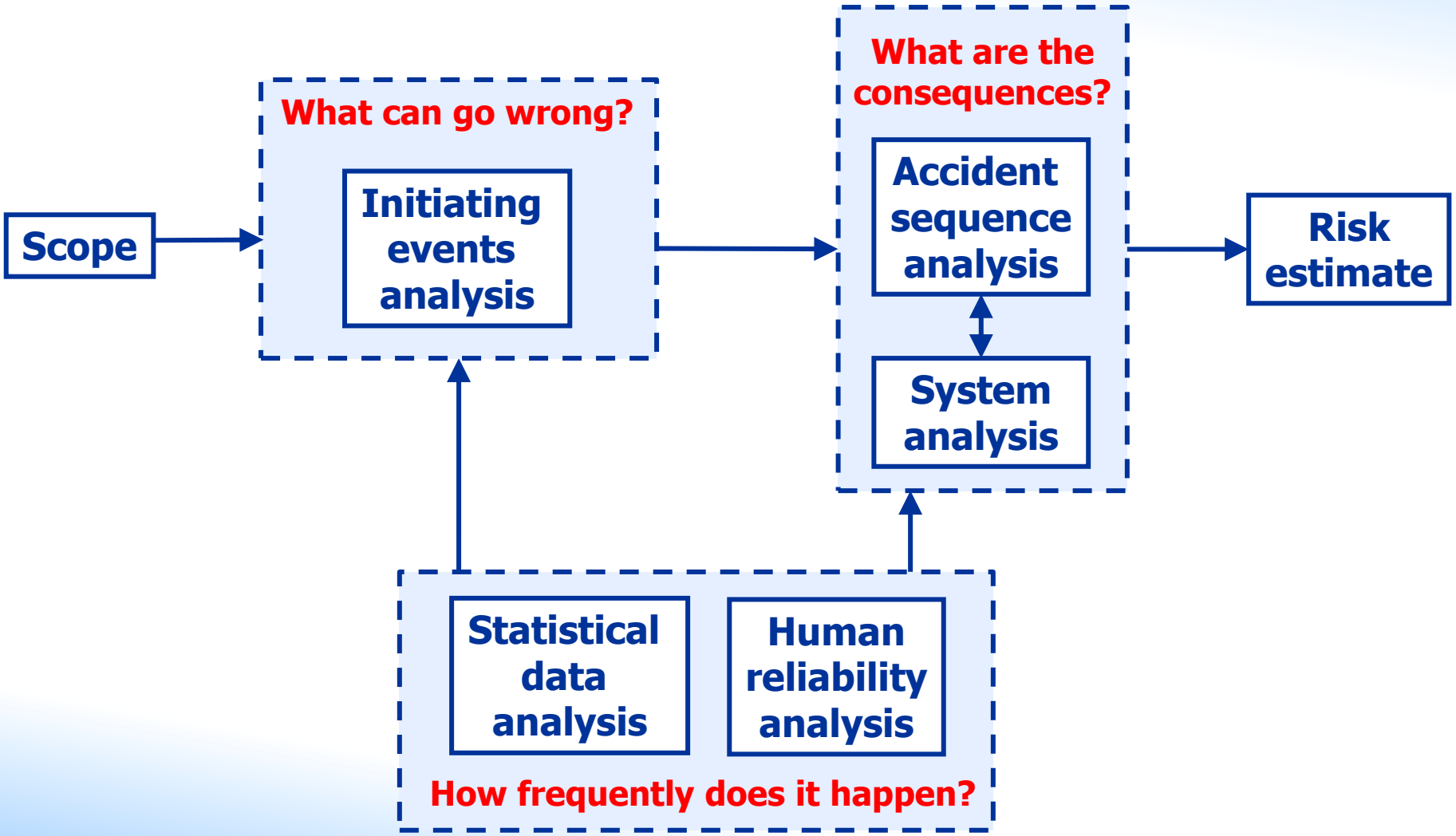


General methodology of L1 PSA

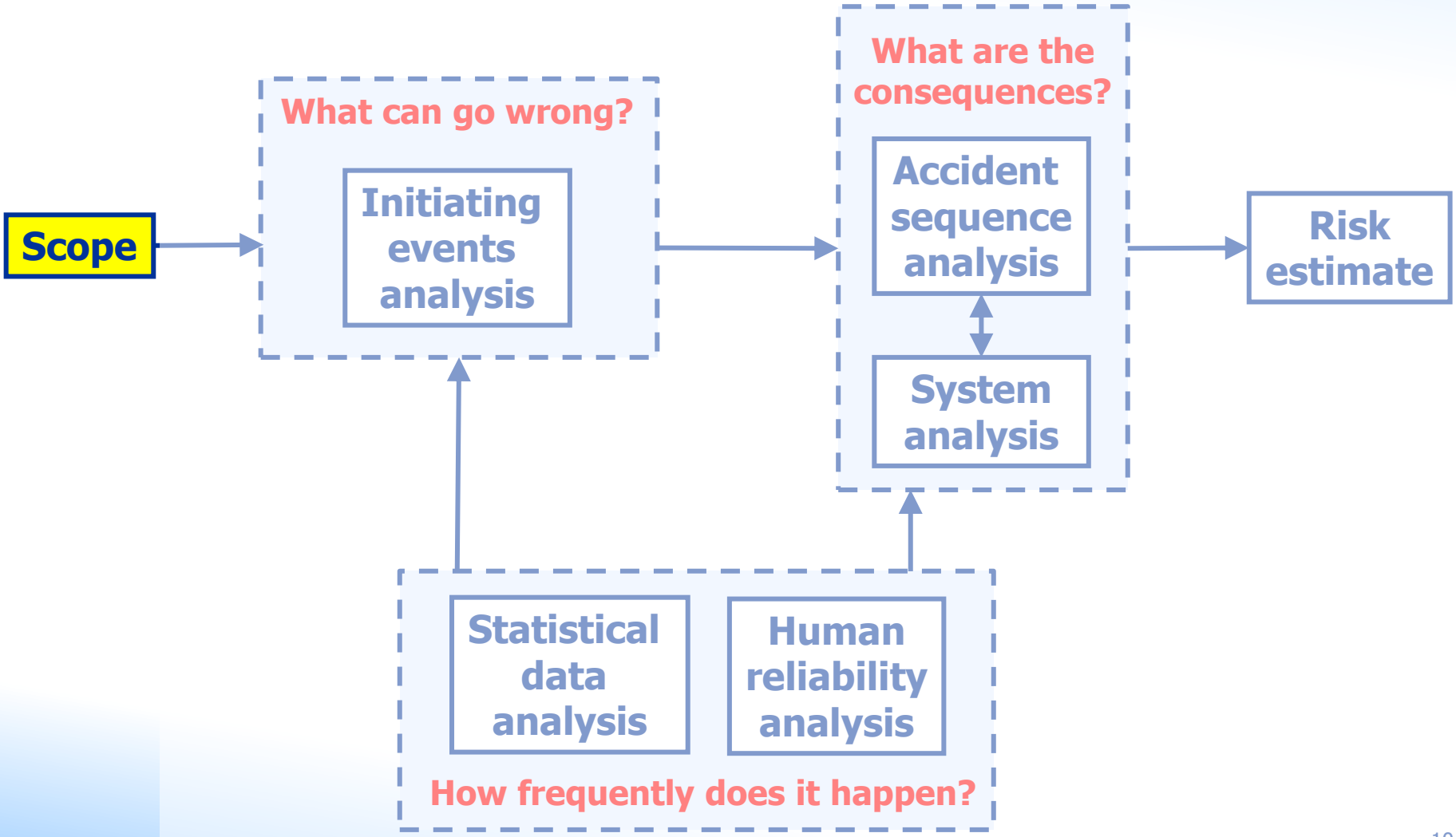




General methodology of L1 PSA



Scope & plant familiarization



Scope & plant familiarization

- First step is definition of PSA scope

- For nuclear power plants PSA scope is defined by following 3 aspects:

1. **Undesirable event to be analyzed?**
   - Reactor core damage, spent fuel pool damage, radioactive release, etc.
   - even financial losses could be analyzed
   - Clear definition of undesirable event should be done (e.g. for CDF – 1200^{O}C, etc.)

2. **Regimes to be analysed?**
   - Full power operation, low power operation, shutdown, etc

3. **Initiating events to be analysed?**
   - Internal events, fires, floods, seismic events, winds, etc.

Scope & plant familiarization

- Plant familirization provides the basis for accurate representation of the plant in the PSA model
- A lot of efforts should be taken to obtain and clarify all the necessary information, mainly received from the NPP and design organizations:
  - **Plant Safety Case/Technical Safety Justification Report**
  - Technical Specification/ operational procedures
  - Piping and Instrumentation Diagrams
  - Thermal-hydraulics analysis reports
  - List of interlocks
  - Accident mitigation procedures
  - Staff training manuals and programmes
  - Control room logs
  - Maintenance records
  - **Statistical data on components failures and incident data, and component exposure times**
  - Generic information sources etc.

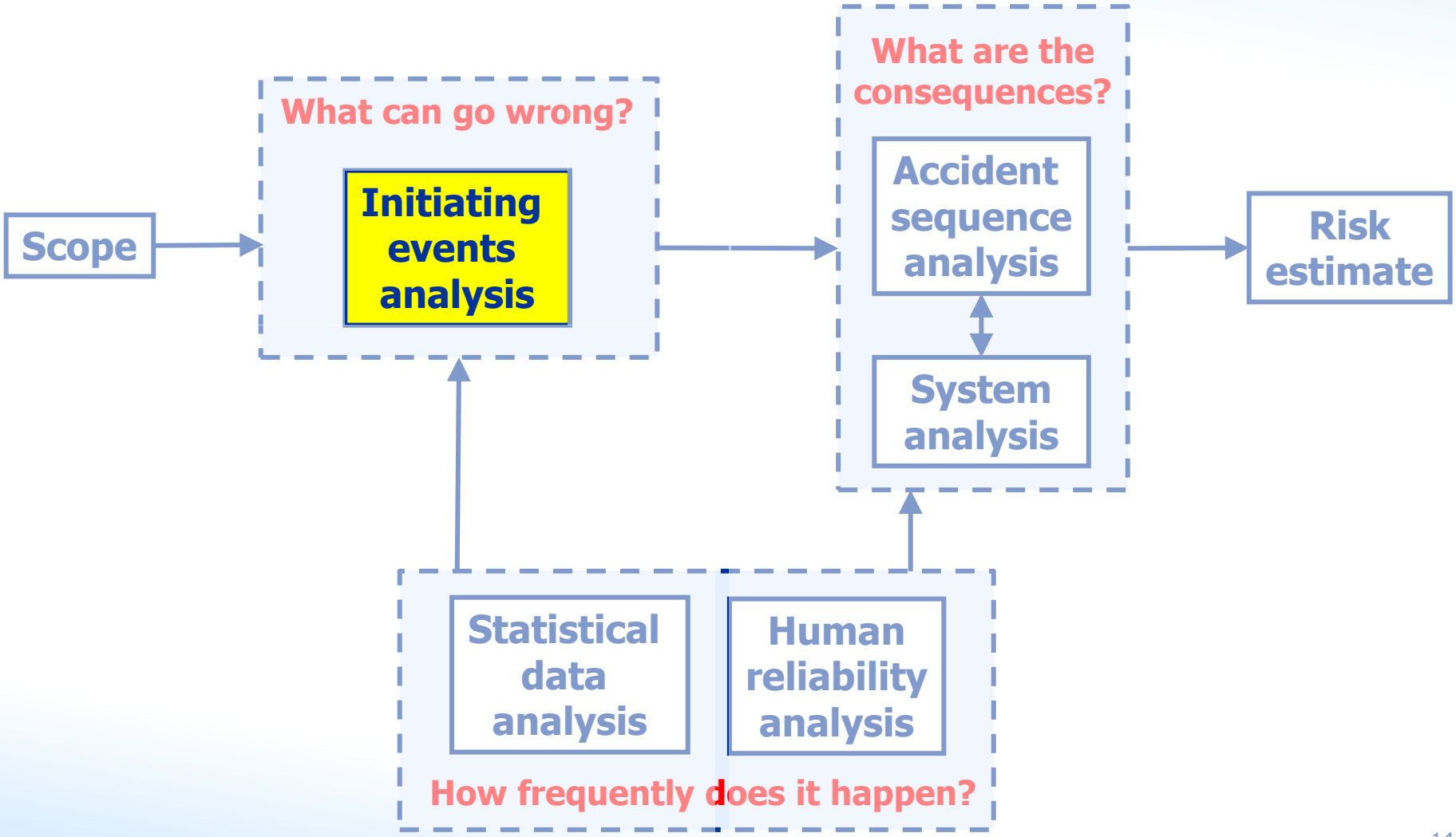
For newly designed plant the information from prototype plants should also be used

Scope & plant familiarization

- The plant documentation, SAR and EOP provide the basic information of the plant responses to the accidents
- This information is supplemented with discussions / interviews with safety analysts and the utility staff
- **All members of the PSA team should be involved in plant familiarization** initially by the documentation review, then by plant visits

- **Regular contact with utility personnel is maintained throughout the course of the study**
- **Several confirmatory plant visits during the analysis should be conducted.**

Initiating events analysis



Initiating events analysis

- IE analysis is one of the key PSA tasks which plays significant role for PSA quality

- The main objective of IE analysis are
  - to identify a (reasonably) **complete** set of the events that interrupt normal plant operation and that require successful mitigation to prevent core/fuel damage - all significant contributors to core/fuel damage must be identified
  - to group the identified initiating events so as to facilitate the efficient modeling of plant response and initiating events frequency assessment whilst providing sufficient resolution regarding modeling of accident sequences

Initiating events analysis

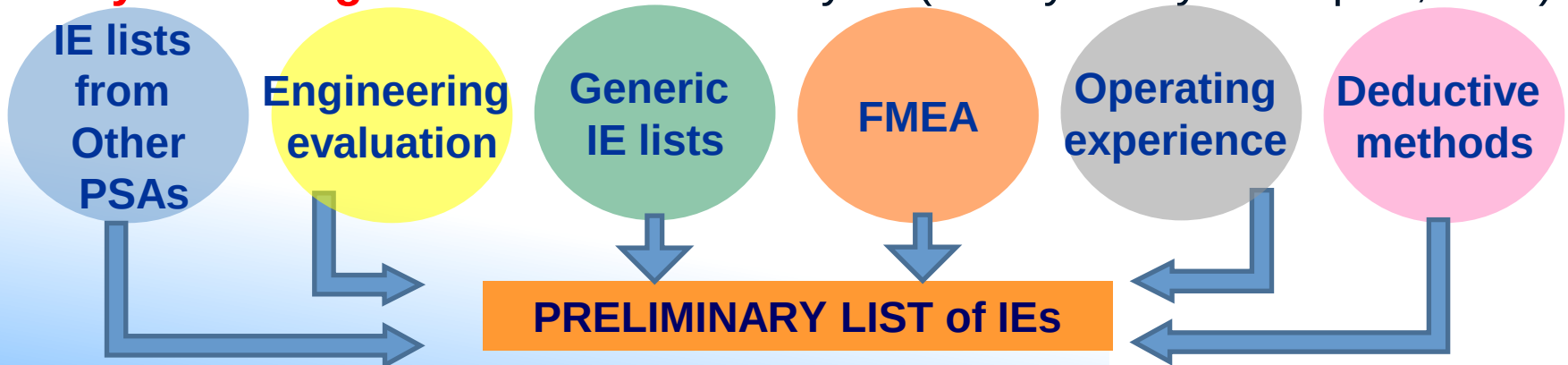
- The main steps of initiating events analysis are:
  - Definition of initiating event
  - Identification of initiating events
  - Initiating events grouping
  - Initiating events frequency assessment
  - Documentation aspects
- Prior to IE identification the definition of initiating event should be established
- Definition of initiating event by IAEA Safety Guide on Level-1 PSA, SSG-3, 2010

An initiating event is an event that could directly lead to core damage (e.g. reactor vessel rupture) or challenges normal operation and that requires successful mitigation using safety or non-safety systems to prevent core damage

Initiating events analysis

METHODS FOR IEs IDENTIFICATION

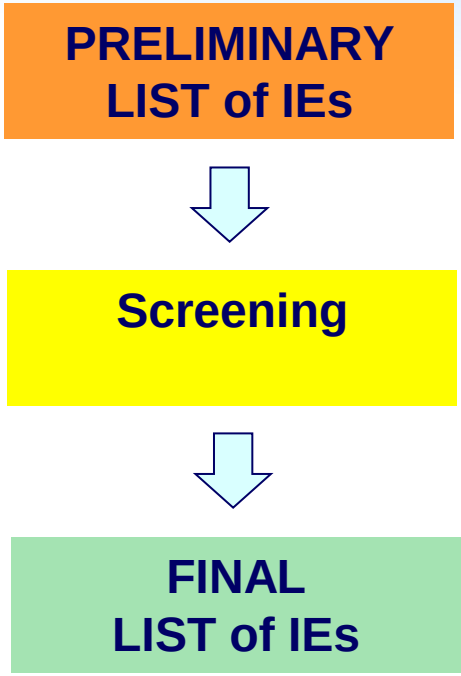
1. **Analytical engineering methods** such as hazard and operability studies (**HAZOPs**) or failure mode and effects analysis (**FMEA**) or other relevant methods to determine whether system/components failures, either partial or complete, could lead to an IE
2. **Deductive analyses** such as **master logic diagrams** to determine the elementary failures or combinations of elementary failures that would challenge normal operation and lead to an IE
3. **Comparison with the lists of IEs** developed for the Level 1 PSAs for similar plants and with existing safety standards and guidelines
4. **Identification** of IEs on the basis of the analysis of **operating experience** from the plant under investigation and from similar plants
5. **Review of the deterministic** design basis accident analysis and **beyond design basis** accident analysis (Safety Analysis Report, SAR)



Initiating events analysis

SCREENING OF INITIATING EVENTS

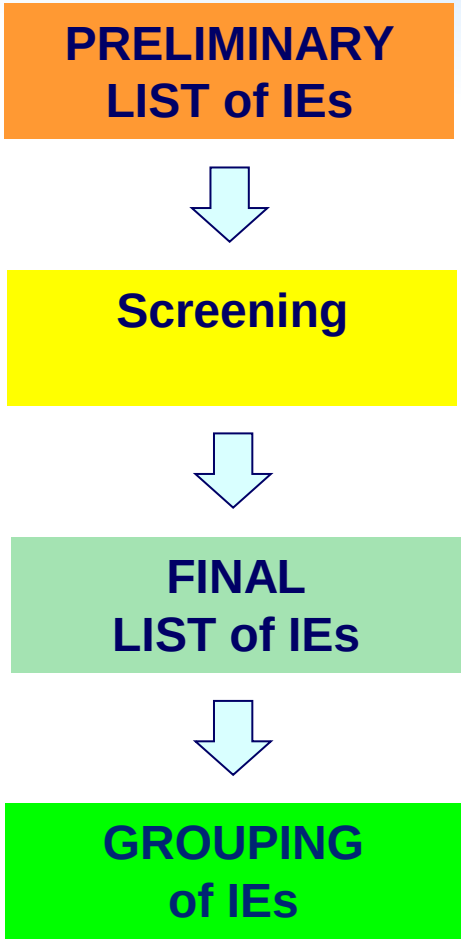
- **Objective: Identified candidates IEs are subjected to a screening analysis**
  - **To screen out events not applicable for the plant under consideration**
  - **To concentrate the analysis on the most risk-significant IEs**
  - **To compile a final list of IEs**
- **General screening criteria**
  - **The event does not correspond to the scope of the PSA**
  - **The frequency of the event is less than the truncation value related to the frequency of a significant accident sequence**
  - **If operator has sufficient time to prevent disturbance in plant operation**



Initiating events analysis

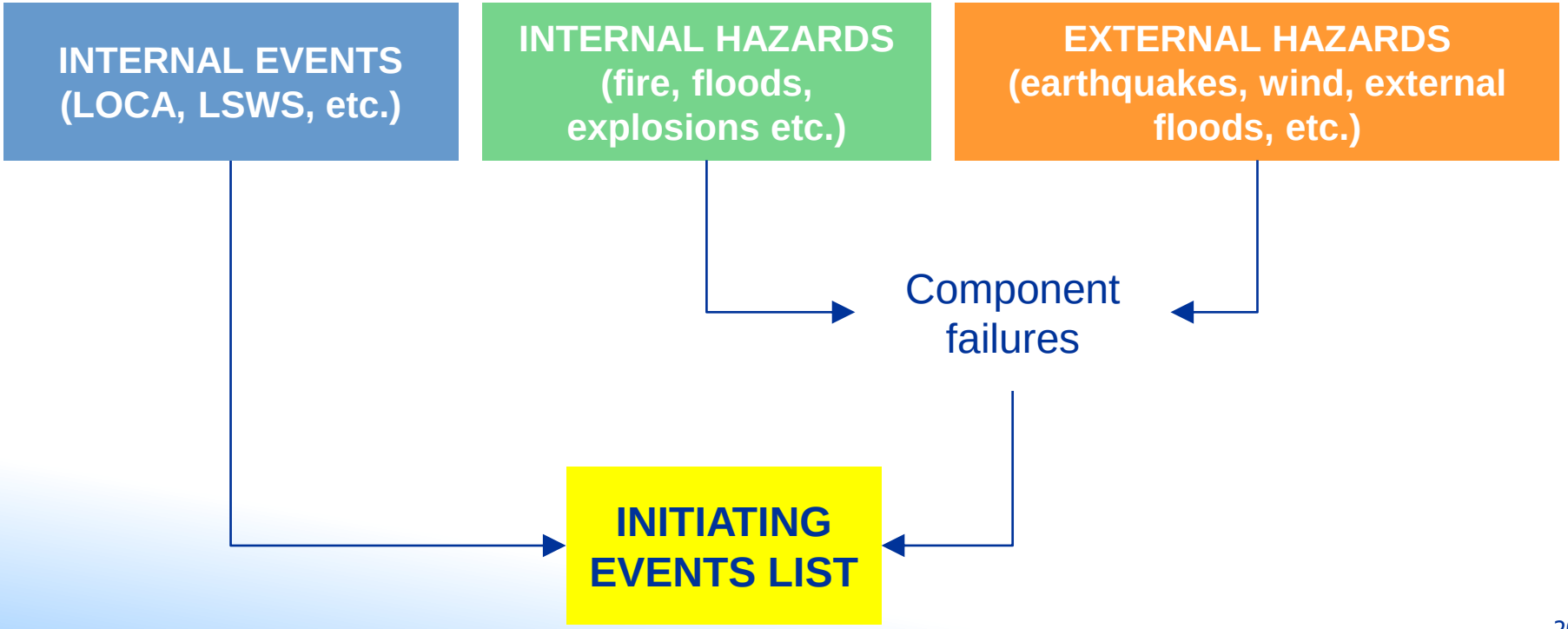
BASIS FOR IEs GROUPING

- **Initiating events should be arranged in groups in which all of the following properties of the initiating events are the same (or very similar):**
  - The accident progression following the initiating event
  - The success criteria for the mitigating systems
  - The effect of the initiating event on the availability and operation of safety systems and support systems
  - The response expected from plant operators
- **The results of thermal hydraulic calculations are used to confirm**
  - Accident progressions and timing
  - Success criteria
- **Objective: To facilitate an efficient, but realistic estimation of CDF**
  - ✓ Manageable number of accident sequence models
  - ✓ Sufficient information for frequency estimation



Initiating events analysis

- Initiating events at NPP are caused by components failures or human errors (internal events)
- Component failures also could be originated by different type of hazards: INTERNAL and EXTERNAL HAZARDS



Initiating events analysis

- Neglecting one or more initiating events leads to inadequate evaluation of CDF value

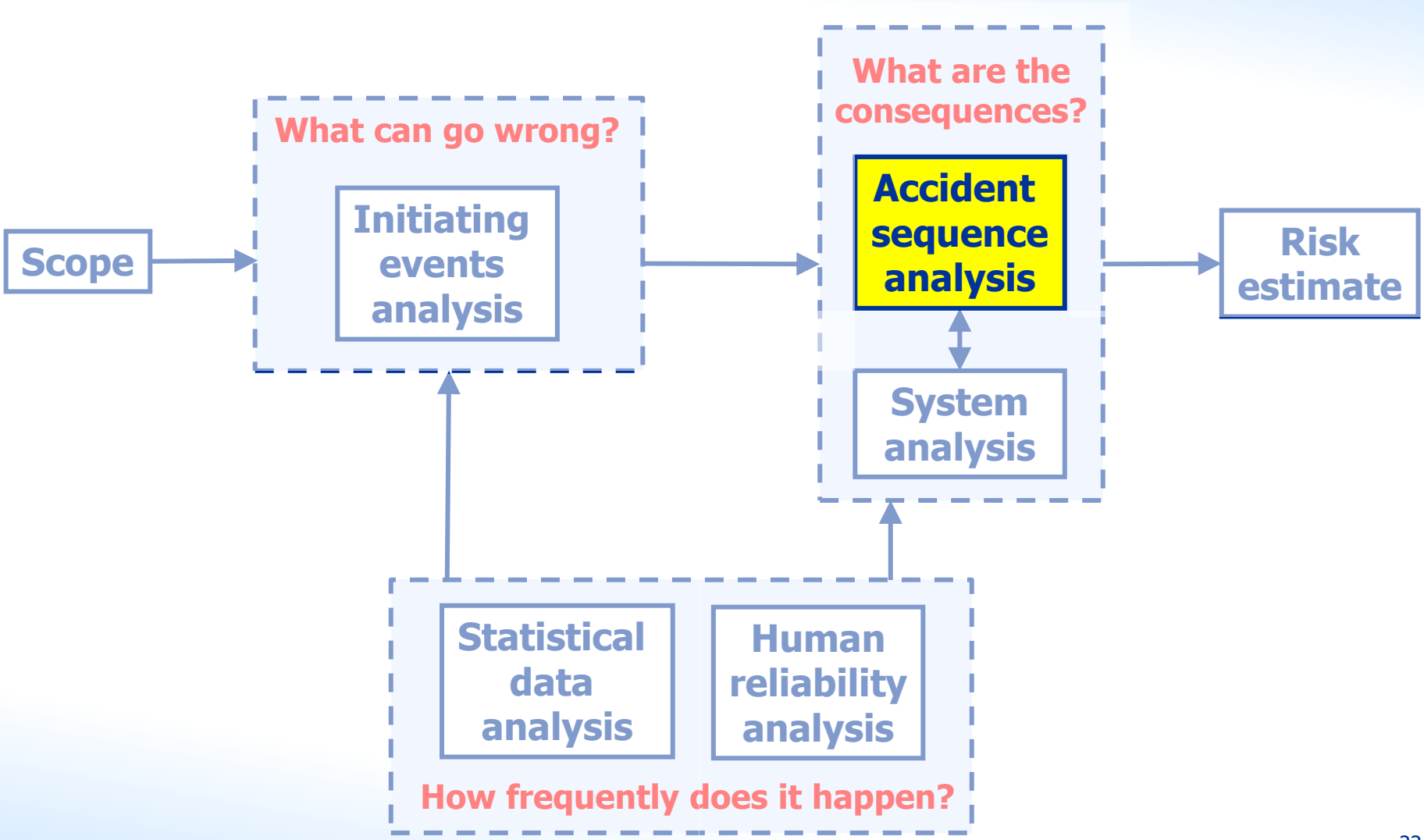
- Therefore IE selection process should be accurately carried out in order to assure completeness of final IE list

- Frequency of the reactor core damage equals

$$CDF = IEF_1 \times M_1 + IEF_2 \times M_2 + \cdots + IEF_N \times M_N$$

where IEF_i – initiating events frequency, M_i – the probability of mitigation failure

Accident sequence analysis

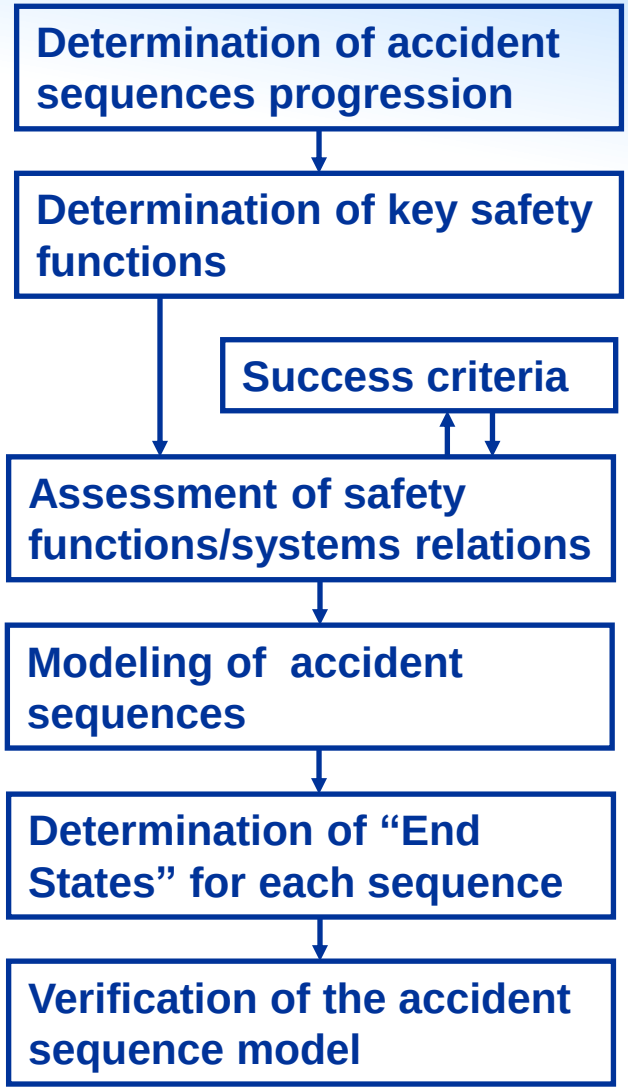


Accident sequence analysis

- Accident sequence is a chain of events that link initiator and consequences depending on the success or failure of the mitigating safety and safety related systems

- Consideration of all non-negligible accident sequences in the PSA model (Accident sequences leading to core damage in Level 1 PSA)

- One of the most used approaches for accident sequence modeling is **EVENT TREE METHOD**

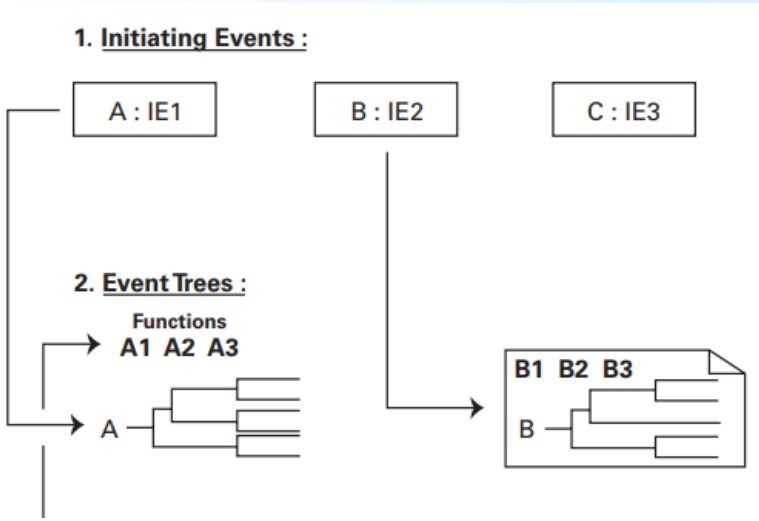


Accident sequence analysis

- **Event trees (ETs) are static logic models used to represent accident sequences**
  - ETs are developed to systematically identify accident sequences
  - ETs & Fault trees form the fundamental basis for the calculation of CDF
- **Purpose of Event Tree**
  - Display sequence progression
  - Display sequences end states
  - Display sequence-specific dependencies
    - Physical (systems)
    - Functional (success criteria)
    - Human actions
  - The event tree is the powerful tool to support understanding of various potential sequences that result in severe accident
  - Improve understanding of the PSA models
    - Analysts / users
    - Plant personnel
    - Reviewers

Accident sequence analysis

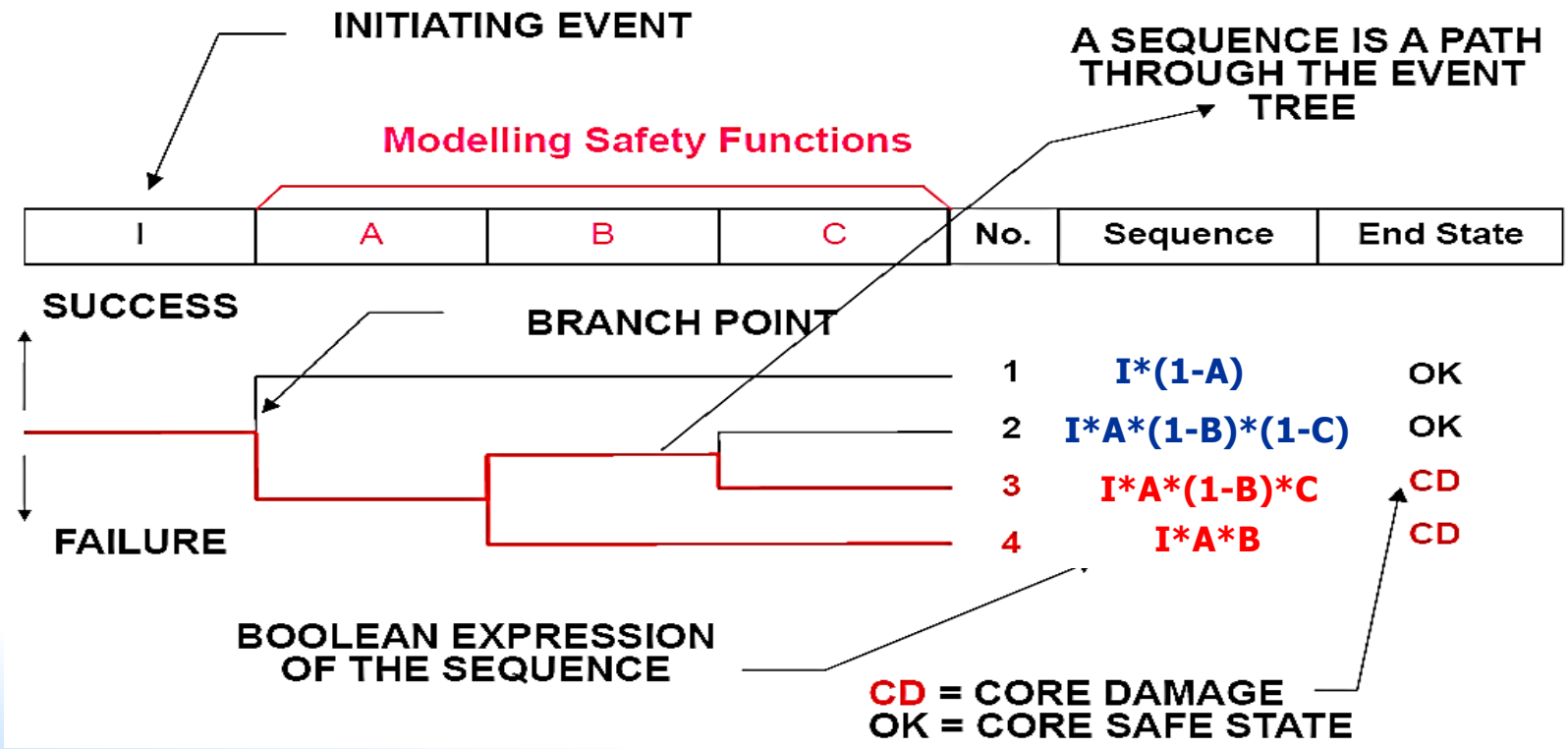
- Event trees are the logic models from which the accident sequences are derived
- In general, separate event trees are constructed for each initiating event group
- Each event tree had a different structure since the initiating events were grouped according to the mitigating requirements - different mitigating requirements result in the different tree structure



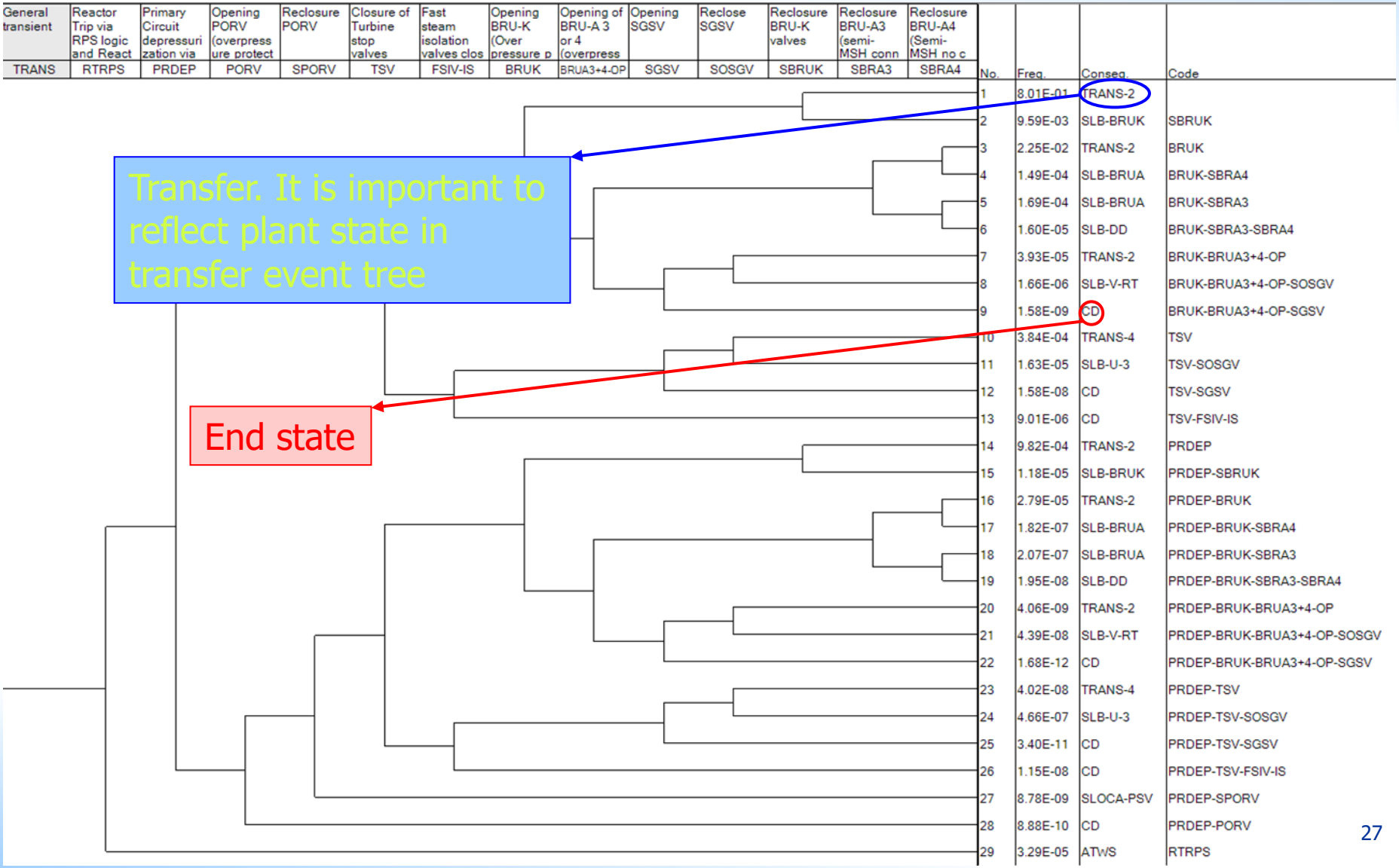
- Headings (function events) of the event trees correspond to the systems responding to the initiating event
- Normally only front line systems appear on the trees. System dependencies and dependencies arising from the phenomenological aspects of the accident are reflected in the tree structure
- Also critical human actions could appear as a functional event in the event tree (e.g. recovery of LOSP)

Accident sequence analysis

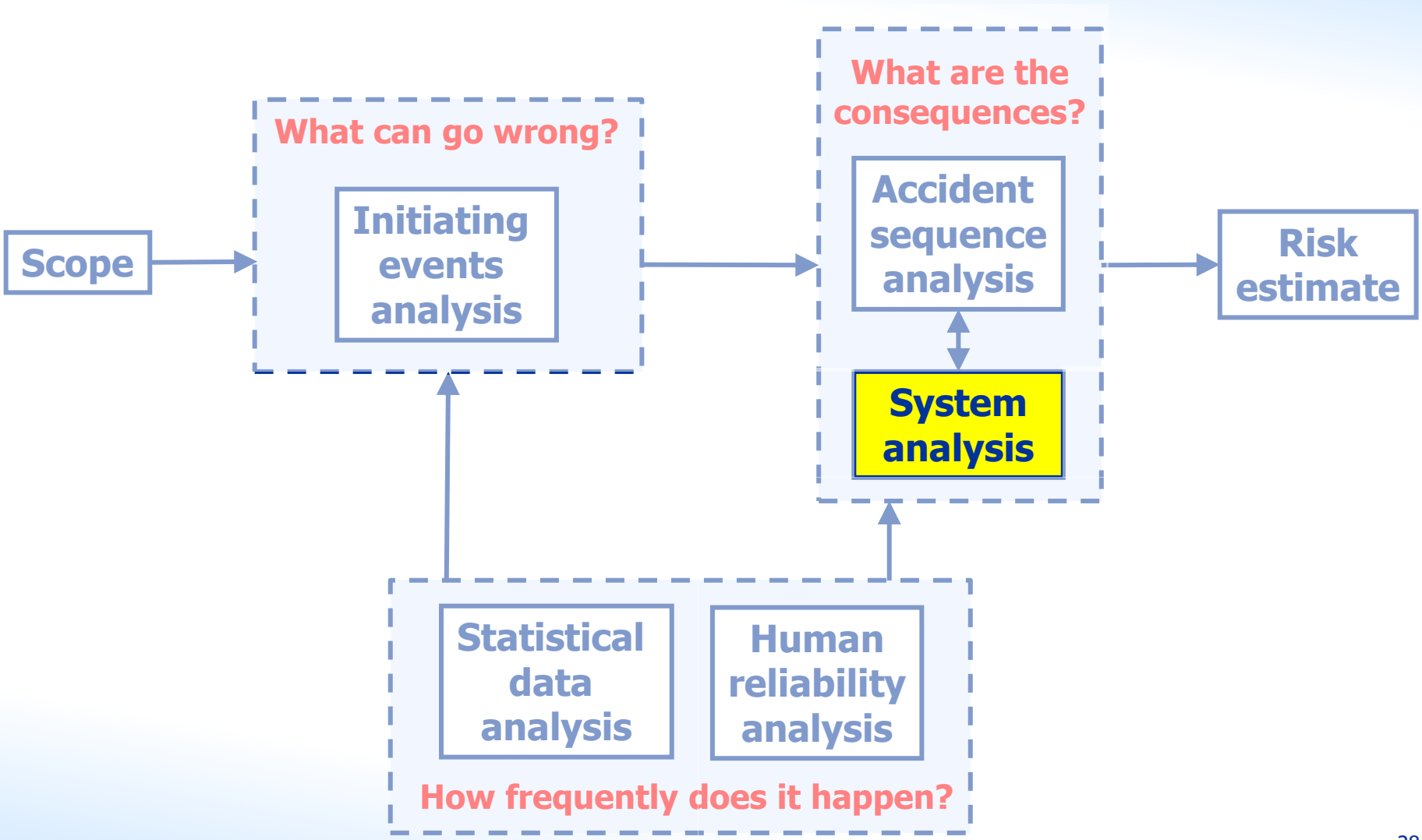
- Event tree is constructed based on success criteria identified for particular IE group.



Accident sequence analysis



System analysis



System analysis

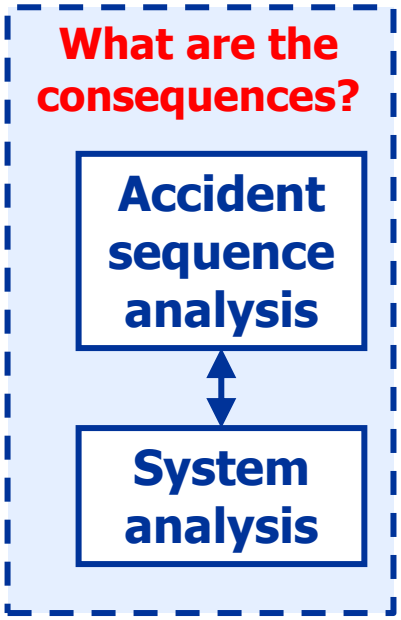
- The aim of system analysis is to develop logical model which reflects dependency of system successful operation from following factors:
  - Components condition
  - Support systems operation
  - Human actions, etc.

- There are different methods for system reliability model construction (fault tree method, GO-schemes, Markov chains, etc.)

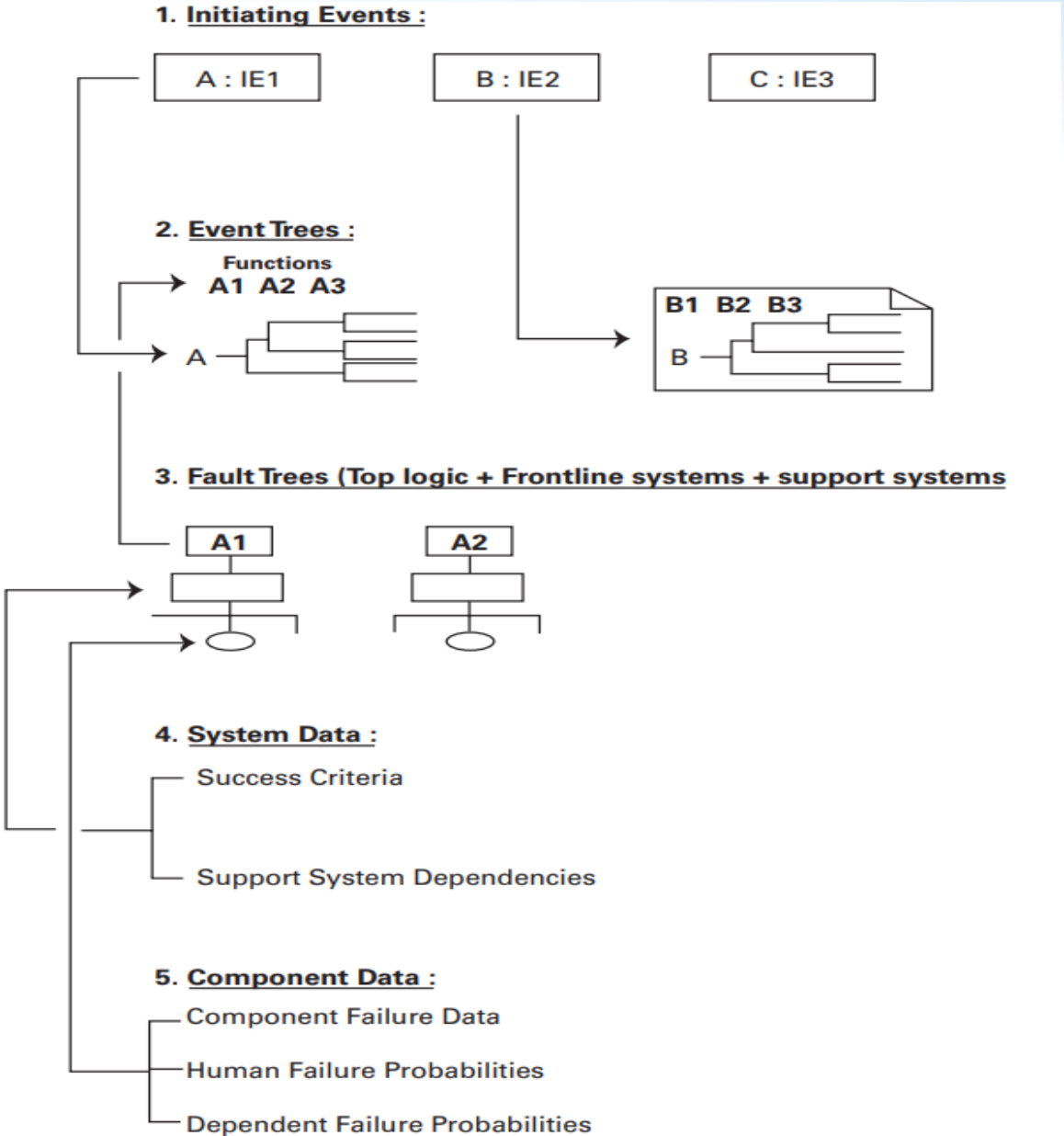
- The most popular and user-friendly one is **FAULT TREE METHOD**.

System analysis

- Fault trees (FT) are a graphical and analytical method whereby an undesired state of a system is specified, and the system is then analyzed in the context of its operation to find all possible ways in which the undesired event can occur
- FTs are used to model the failure of events in the event trees
- The combination of event trees and fault trees provides a comprehensive and detailed representation of the plant's safety logic
  - **Provide answer to the question "What are the consequences?"**



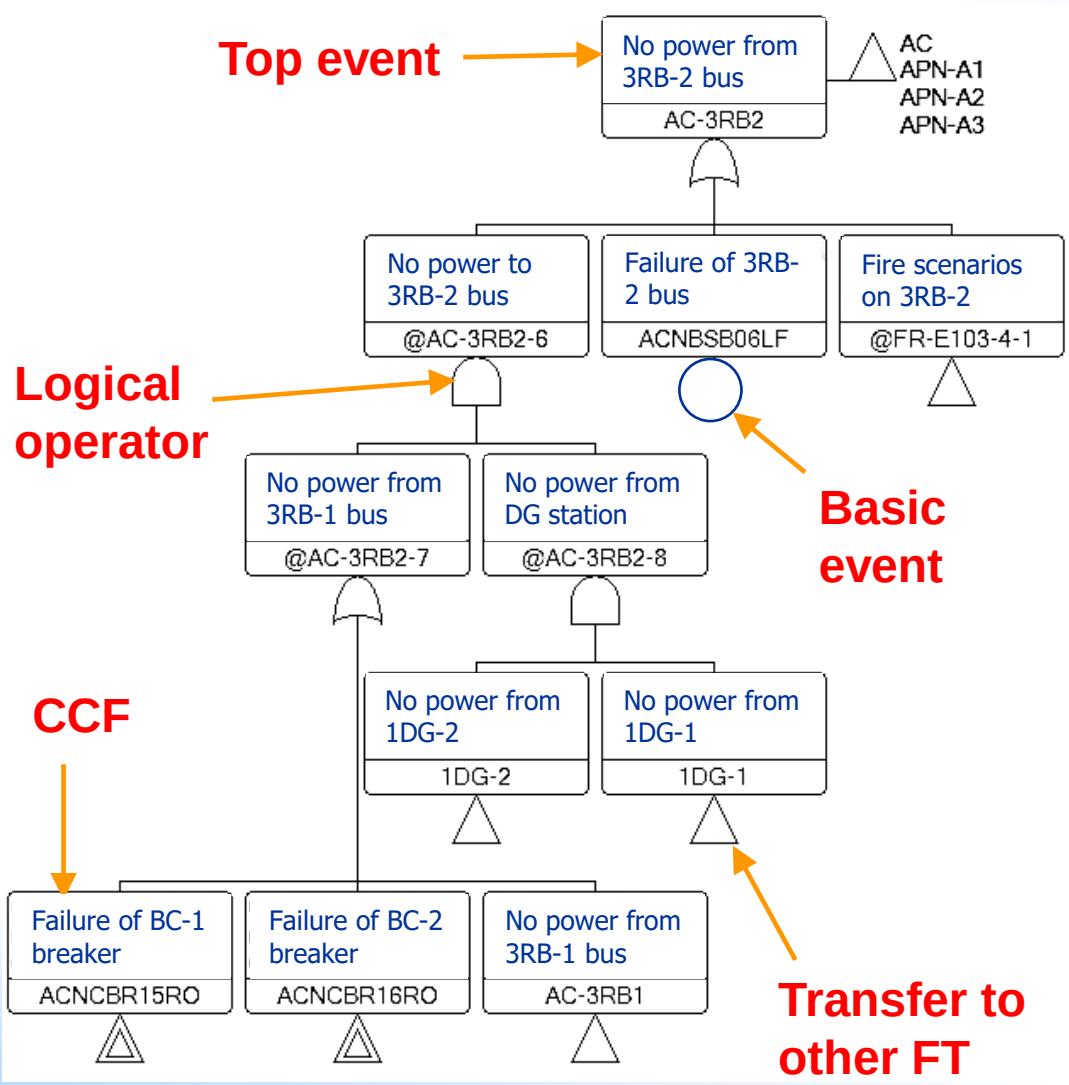
System analysis

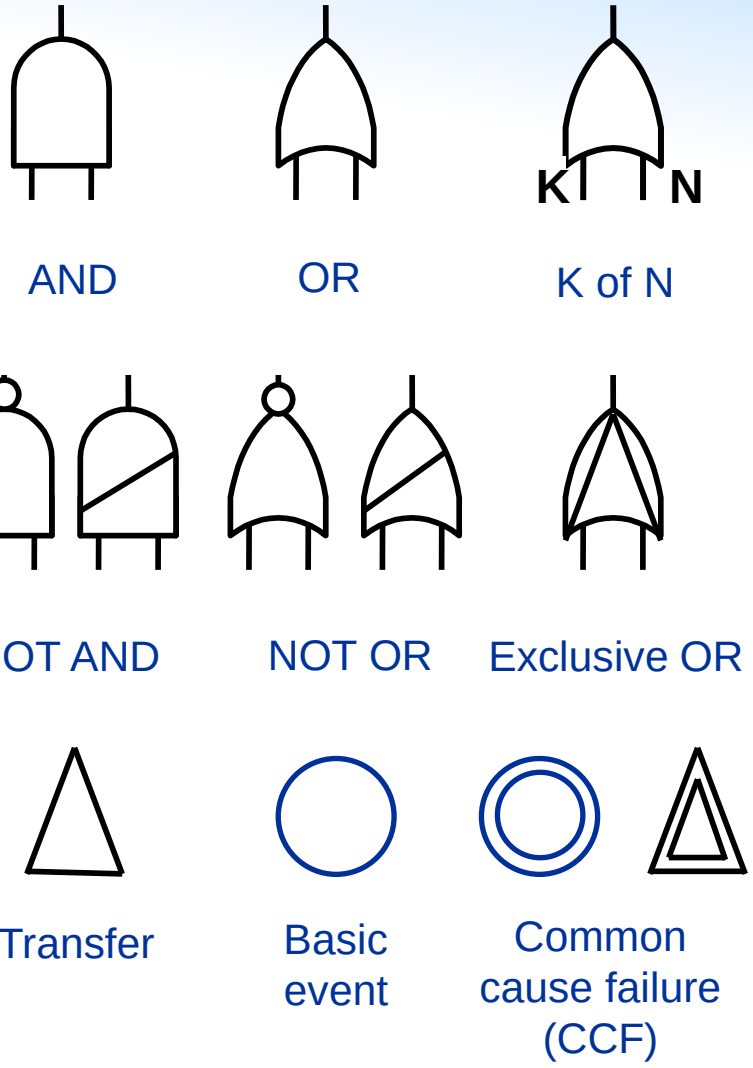


System analysis

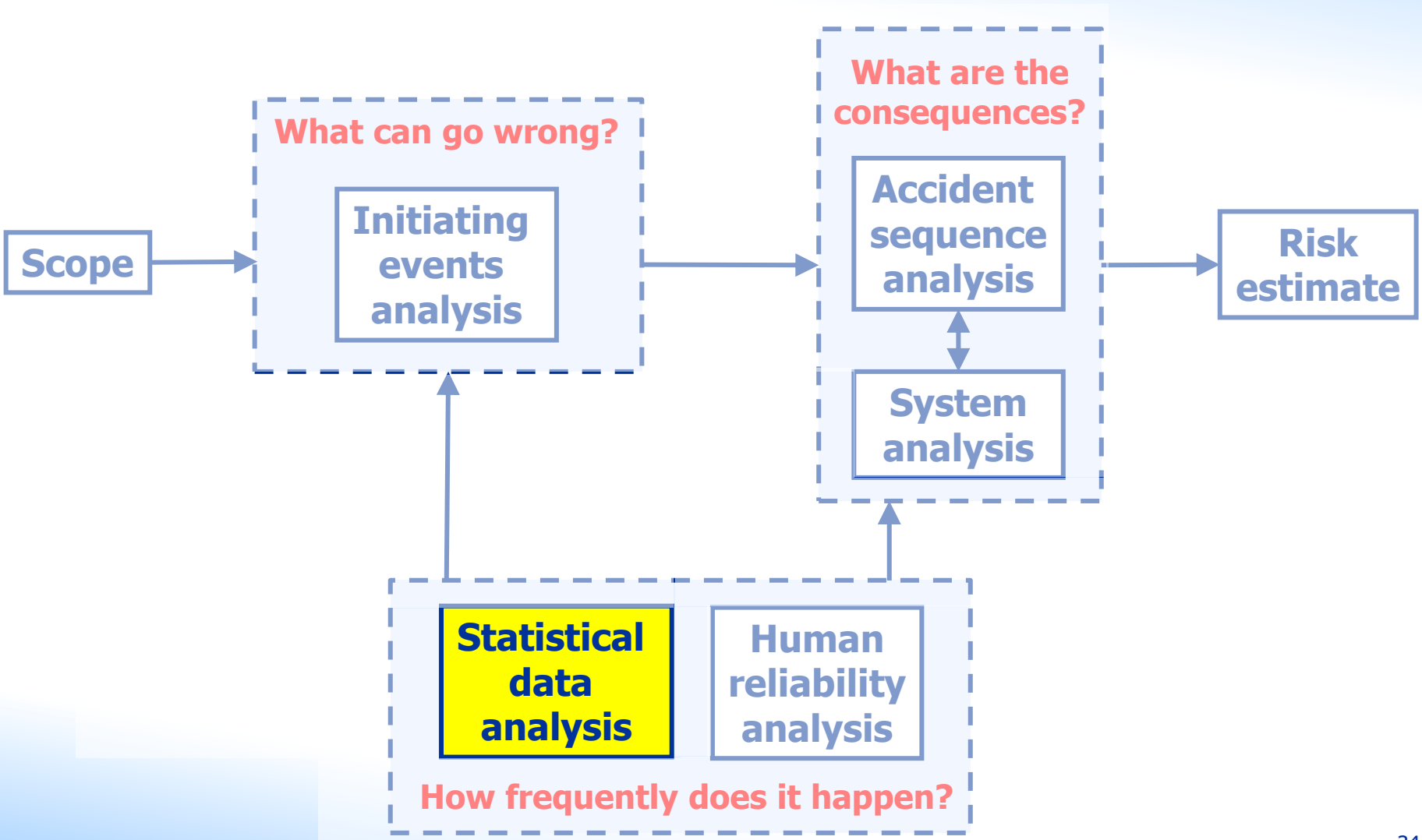
- The system fault tree should include all possible failure modes which contribute to the system unavailability:
  - Relevant component failures
  - Outages from testing, maintenance and repairs
  - Human errors including dependencies between human actions
  - Failures of supplies and supports (normally handled through transfers to the fault trees of supplies and supports)
  - Common Cause Failures (CCFs)
  - Failures induced by Initiating event (where applicable)

System analysis





Data analysis



Data analysis

- The objective of data analysis is to provide quantitative information needed to estimate the core damage frequency. Specifically, this activity includes the estimation of:
  - Initiating event frequencies
  - Component reliability (failure probability)
  - Component unavailability due to maintenance
  - Component unavailability due to testing
  - Common cause failure probability
  - Human error probability (next task HRA)

Data analysis

NUREG/CR-6823 Handbook of Parameter Estimation for PRA (table 2.1)

2.2 Initiating Events	2.3 Failures to Start or Change State (2 models)		2.4 Failures to Run or Maintain State	2.5 Durations	2.6 Unavailability
Typical Event					
Event occurs initiating an accident sequence	Standby system fails on demand		System in operation fails to run, or component changes state during mission	A condition persists for a random time period	System is unavail-able, intentionally out of service, when demanded
Parameter(s) to Estimate					
λ, event frequency	For failure on demand: p, probability of failure on demand	For standby failure: λ, rate of occurrence of standby failures	λ, rate of failure to run	Parameters of assumed probability distribution of duration time	q, fraction of time when system will be out of service
Data Required to Estimate Parameters[a]					
Number of events, x, in total time, t	Number of failures, x, in total number of demands, n	Number of failures, x, in total standby time, t	Number of failures, x, in total running time, t	Depends on model, but typically the lengths of the observed durations	Onset times and durations of observed out-of-service events; OR observed fractions of time when system was out of service

[a] The data here are the minimal requirements to estimate the parameter. More detailed data are needed to check the model assumptions.

Data analysis

- Initiating event frequencies:

  $IEF=N/T_E$ [1/h] (N- number of events, T- exposure time [h])

- Component failure probability
  - Probability to fail on demand

    $P= N/N_O$ (N-number of failures, N_O-number of demands)

  - Probability to fail to run

    $P=\lambda T_{MT}$ (λ-failure rate [1/h], T_{MT}- mission time [h])

  - Periodically tested component

    $P=\lambda T_I/2$

    (λ-failure rate [1/h],

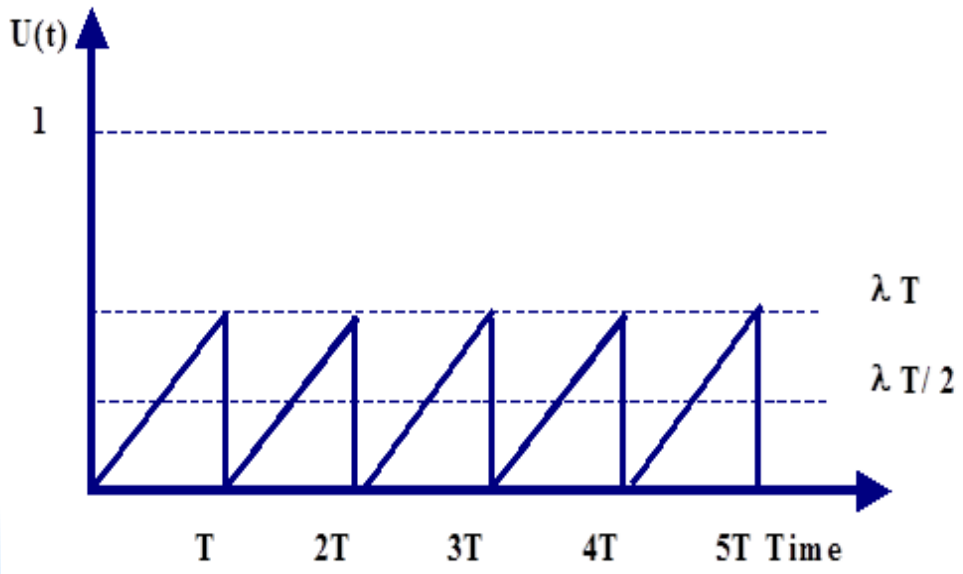
    T_I- test interval [h])

- Component unavailability due to maintenance/testing

  $P=T_O/T_E$

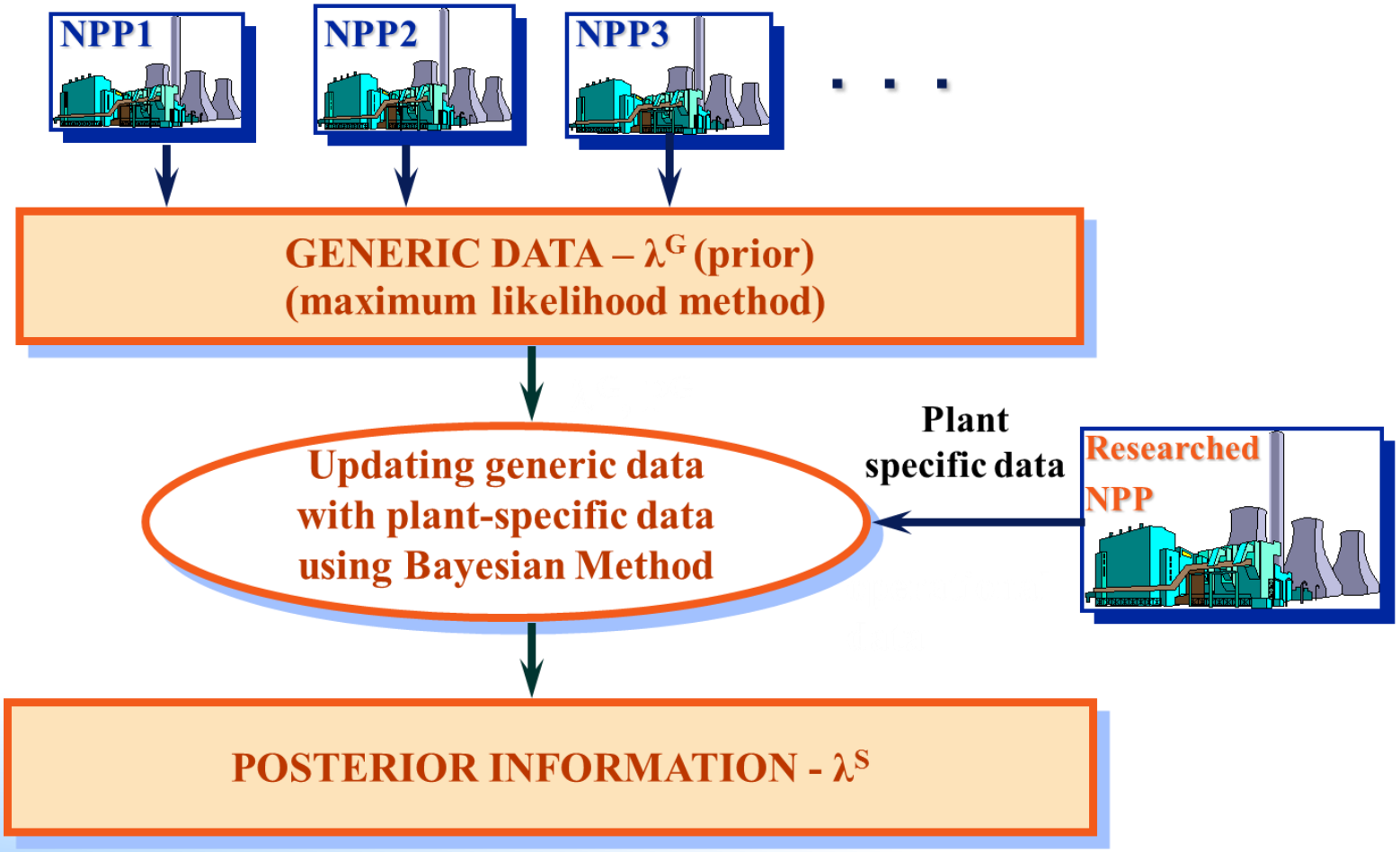
  (T_O- time in maintenance/test [h],

  T_E- exposure time [h])



Data analysis

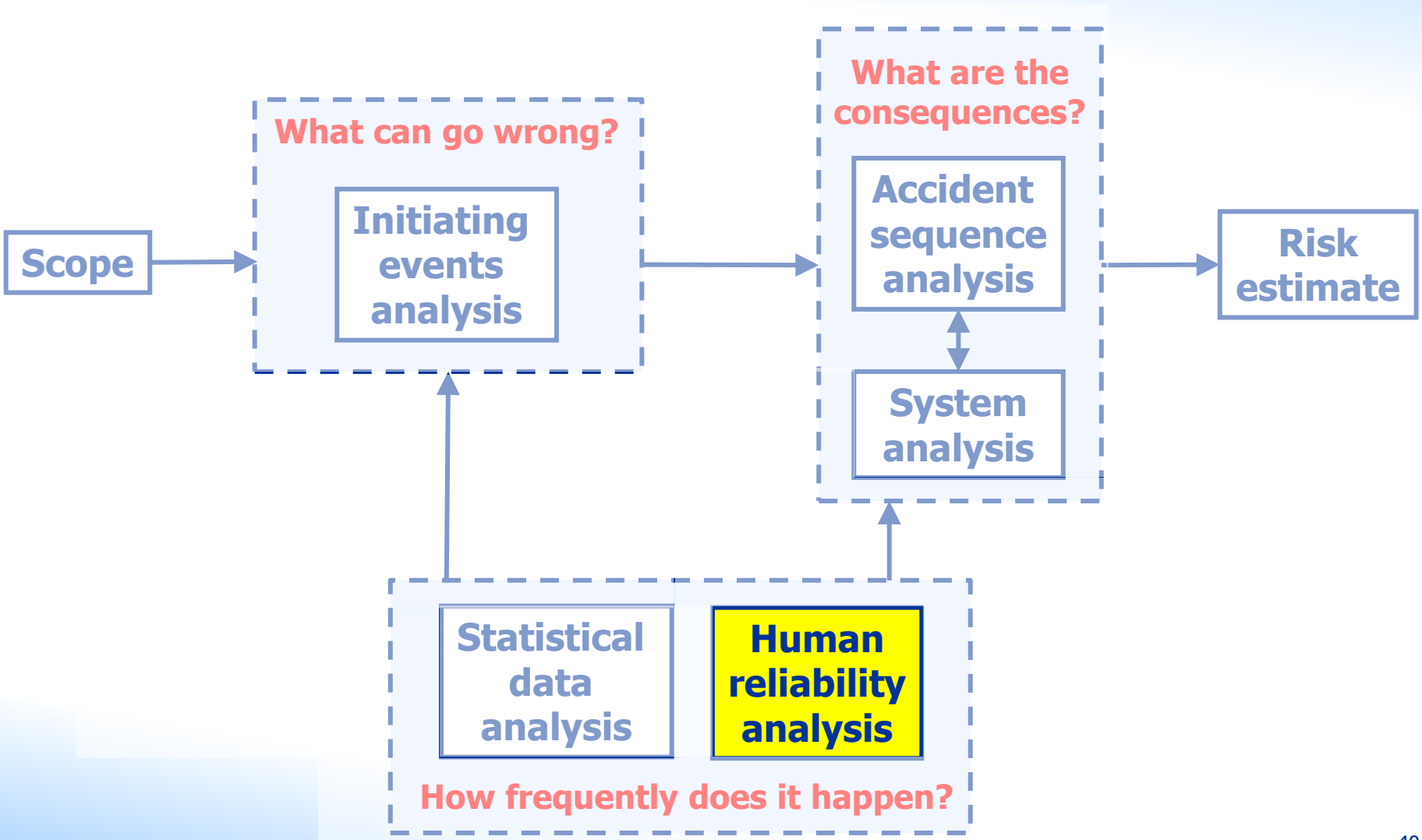
- Extensive statistical data collection process is necessary to find out all necessary parameters (λ, t, etc.)



Data analysis

- Common cause failure probability
  - Components could fail due to common cause which is arising from a single cause. CCF may occur simultaneously or consecutively in a number of associated components.
  - Common cause failure is driven by unknown root cause which could occur if components are:
    - of similar type
    - performing similar function
    - produced by the same manufacturer
    - operating under similar conditions
    - located in the same room
    - operating under similar procedures
  - Different methods are used to calculate CCF probability (α-factor, β-factor, MGL, etc.)

Human reliability analysis



Human reliability analysis

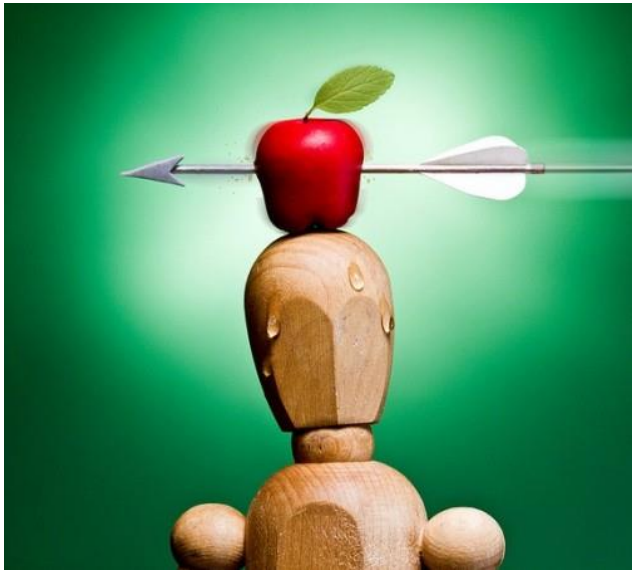
- Human reliability analysis (HRA) is the assessment of the risk associated with the plant personnel interactions, and in particular human errors

- Two types of human error modes have been defined:
  - Error of Omission (EOM)
  - Error of Commission (ECOM)

Human reliability analysis

- **Error of omission**
  - **The failure to initiate performance of a system required action (e.g., skipping a procedural step or an entire task)**

- **Error of commission**
  - **Carries out an action incorrectly (opening valves in system A rather than system B)**
  - **Carries out an additional, unrequired action (opening valves that are not required to be opened in the procedure being carried out)**



Human reliability analysis

- **CATEGORY A – PRE-INITIATORS**
  - Errors that cause equipment or systems to be unavailable when required post fault

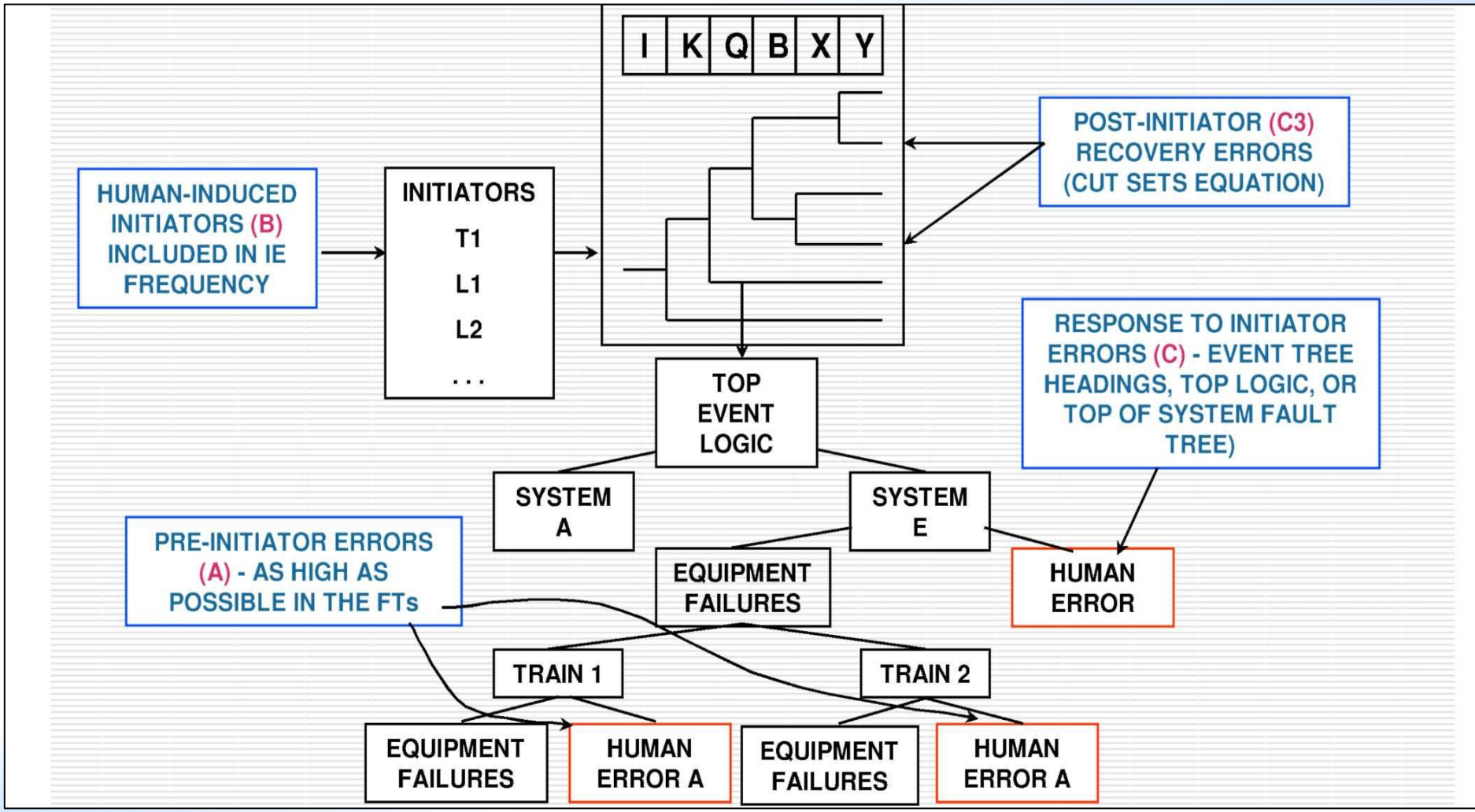
- **CATEGORY B – INITIATORS**
  - Errors that either by themselves or in combination with equipment failures lead to initiating events

- **CATEGORY C – POST-INITIATORS**
  - Errors occurring post-fault. These can occur while performing safety actions or can be actions that aggravate the fault sequence (Types C1, C2 & C3)

Human reliability analysis

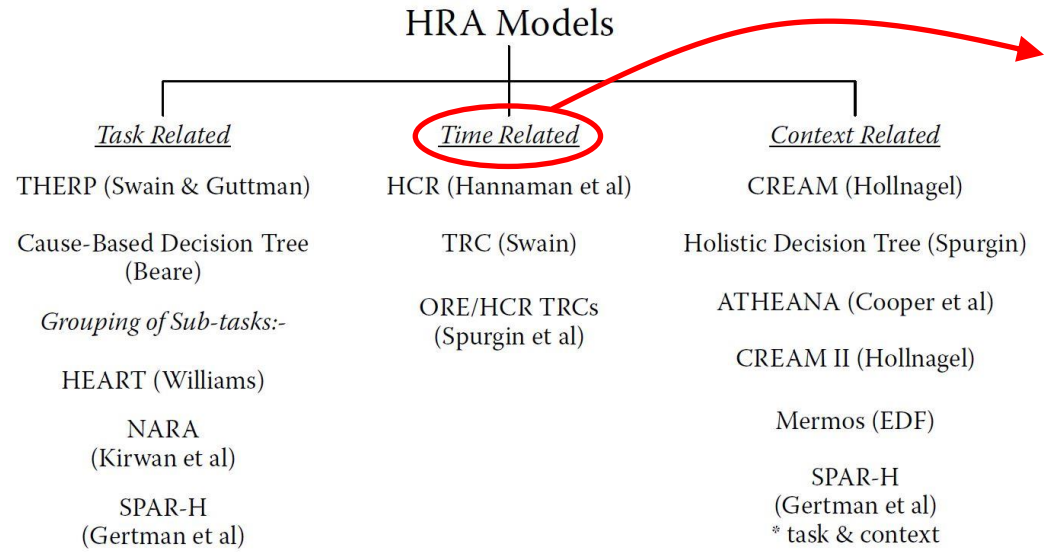
TYPE	DESCRIPTION	IMPACT ON PSA
A	Human actions before the initiating event during normal operation that degrade system availability	Miscalibrations, misalignments explicitly modeled in the PSA (system fault trees)
B	Human actions that contribute to initiating events	Not explicitly modeled in the PSA for full power mode (except when using fault trees to model initiating events). Treated at IE data level. Explicitly considered for Low Power and Shutdown PSA
C1	Human actions during the accident following the correct procedures	Human failure event (HFE) explicitly modeled in the PSA (event trees and fault trees)
C2	Human actions during the accident that due to the inadequate recognition of the situation or the selection of the wrong strategy, make it worse	Identified errors of commission explicitly modeled in the PSA (event trees and fault trees)
C3	Human actions during the accident, trying to recover the situation; for example repairs of equipment	Recovery actions explicitly modeled in the PSA (normally treated at sequence level)

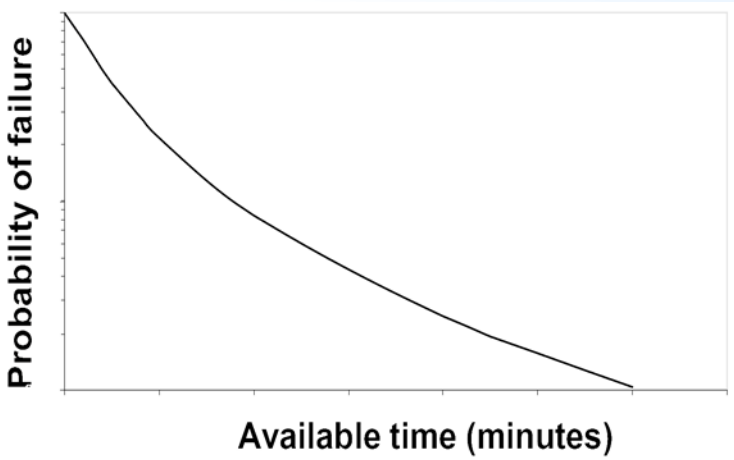
Human reliability analysis



Human reliability analysis

- Different models/methods could be used for calculation of HEP

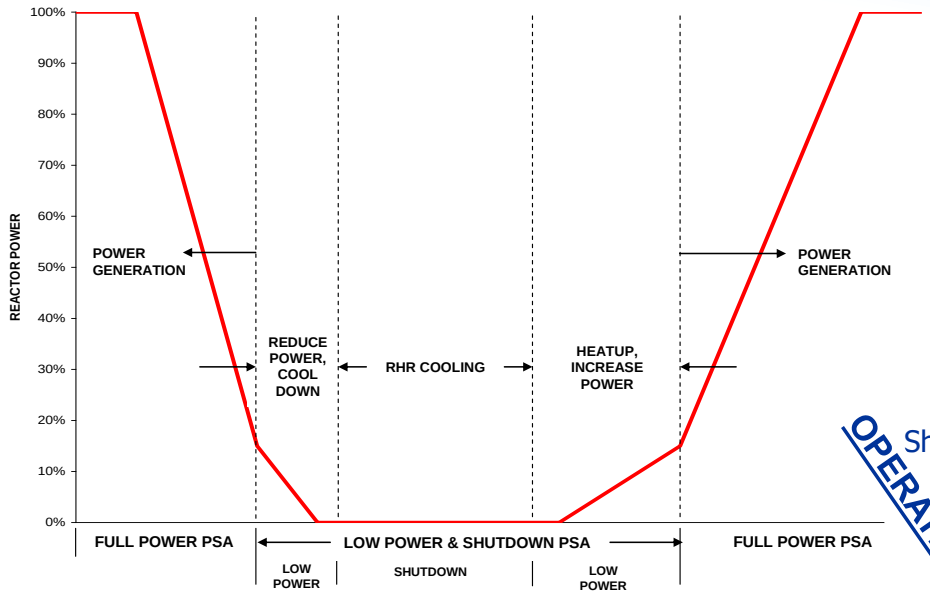


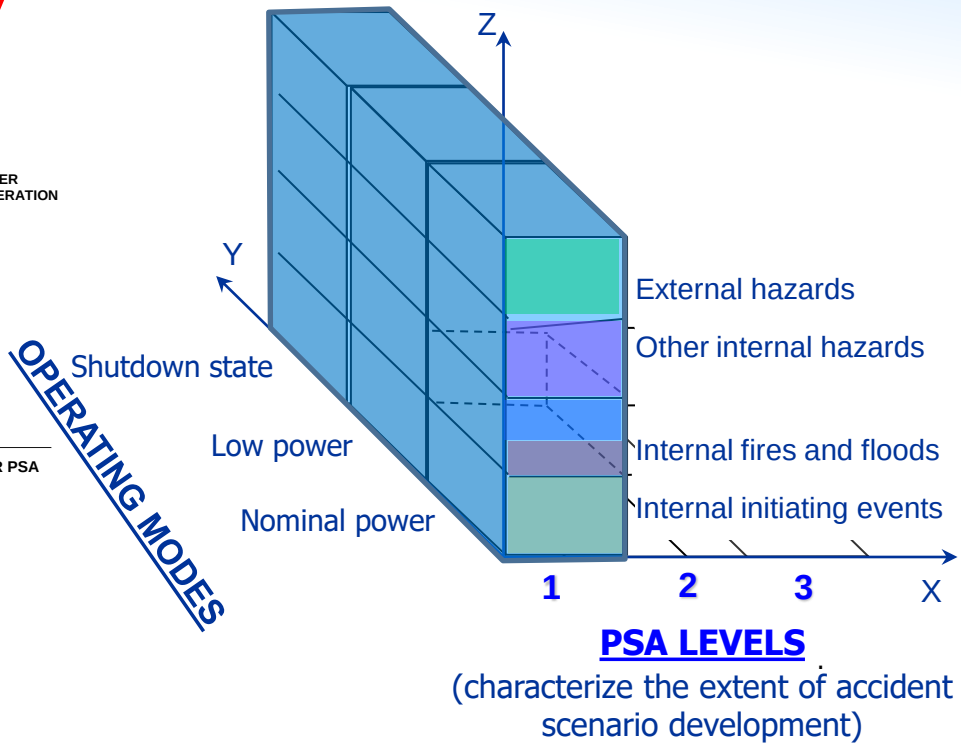


**** A. Spurgin, Human reliability assessment: theory and practice (fig.5.1)***

- In general any method used to determine HEPs should be:
  - self consistent
  - based on existing data and information
  - adjustable to take the operational environment and accident sequence context into consideration

Operational modes





Operating modes are as follows (WWER):

1. Full power operation
2. Reactor criticality
3. Hot shutdown
4. Semi-hot shutdown
5. Cold shutdown—reactor vessel is closed
6. Cold shutdown—reactor vessel is open and
7. Empty reactor vessel (the fuel is removed from the reactor vessel and located to the spent fuel pool).

Operational modes

Plant operational states (POSs) are define (because of extensive changes in plant configuration during a shutdown period), this is done to reflect the plant configuration during an outage evolution. Important characteristics describing a plant operating state are as follows:

- RCS temperature and pressure
- RCS water level (inventory)
- Decay heat removal
- Availability of safety and support systems
- Containment integrity
- System alignments and
- Reactivity margins

POS	Planned refuelling outages	Unplanned outages[a]	Planned and unplanned outages
Power 1	18.47	2.91	21.38
POS1	13.71	3.68	17.39
POS2	8.96	3.75	12.71
POS3	34.58	23.61	58.19
POS4	206.91	–	206.91
POS5S	224.66	–	224.66
POS5L	1,094.29	–	1,094.29
POS6	259.77	–	259.77
POS7	107.51	1.89	109.40
POS8	19.05	0.40	19.45
POS9	29.41	3.19	32.60
POS10	79.82	6.61	86.43
Power 2	123.88	7.69	131.57
POS1–10	Σ_j = 984.38/1,854.01*	Σ_j = 43.13	Σ_j = 1,027.51/1,897.14*
Power 1–2	Σ_j = 142.35	Σ_j = 10.60	Σ_j = 152.95

POS1 The reactor is subcritical. The RCS pressure is between the nominal pressure and 4 MPa. The RCS temperature is between nominal and 180 °C. All trains of the safety systems are available (exceptions are allowed by the limiting conditions of operation). All SGs are connected to the reactor vessel. The primary to secondary side heat removal operates in the steam-water regime using the auxiliary feedwater system and steam removal via the steam dump station to the condenser initially and via the technological condenser at the end of POS. In this POS, the containment is closed.

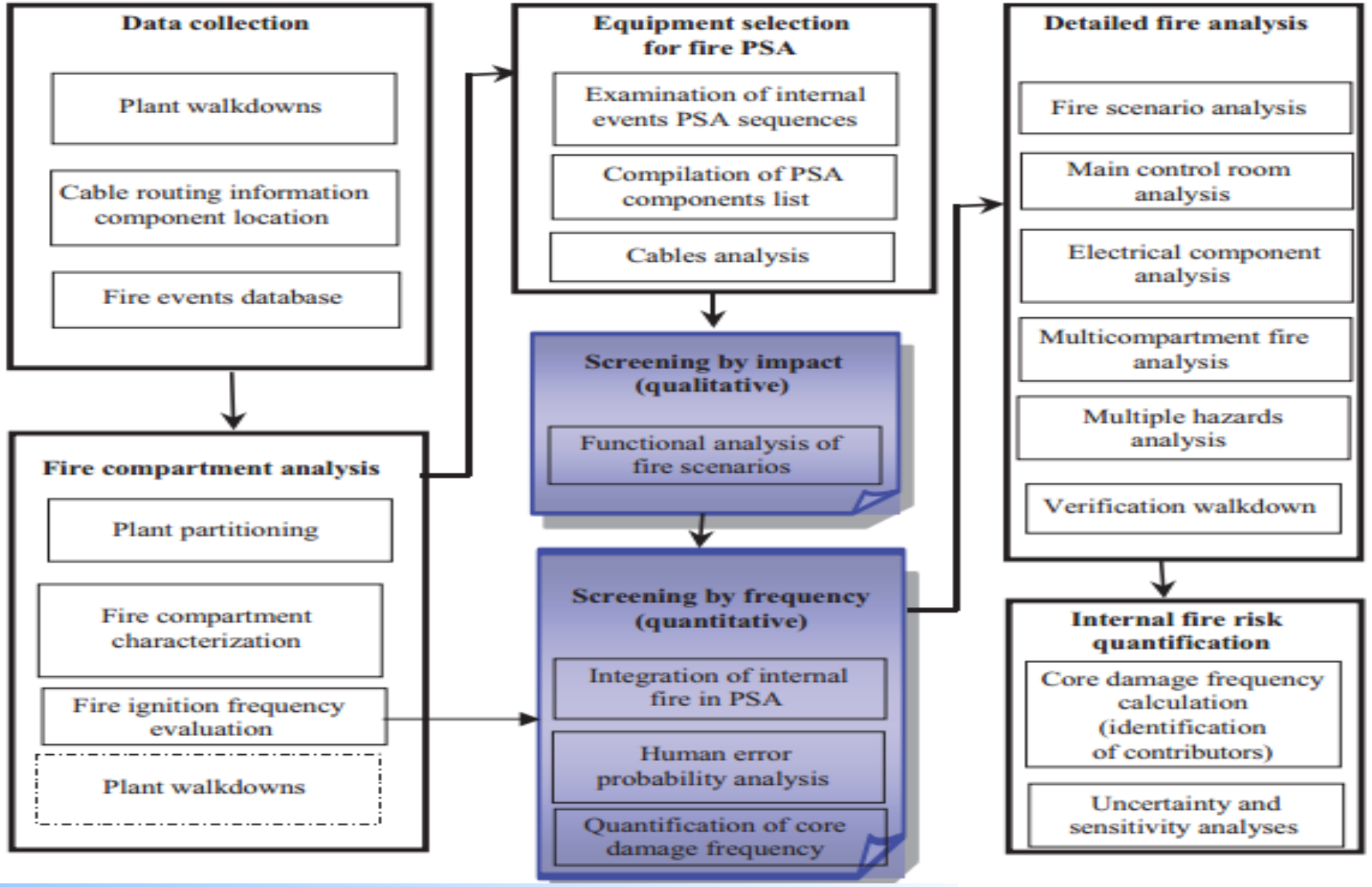
Internal & external hazards

- Apart from random component failures and human errors, fault sequences may be caused by the damage imposed by other hazards
  - **Internal hazards** originating from the sources located on the site of the NPP both inside and outside plant buildings (internal fires, internal floods, missiles, etc.)
  - **External hazards** originating from the sources located outside the site of the NPP (seismic, external fires, external flood, wind, etc.)

- Such hazards can damage plant components and potentially lead to CD. These hazards have the potential to affect several equipment and impact plant personnel simultaneously

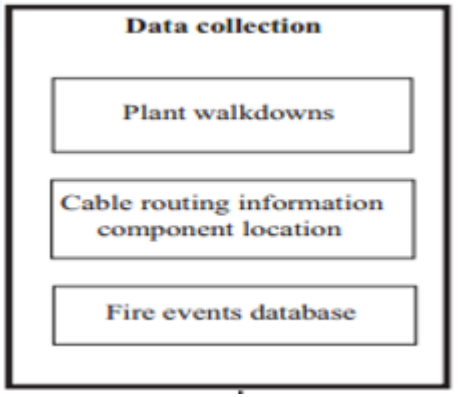
- Both internal and external hazards should be included in the Level 1 PSA.

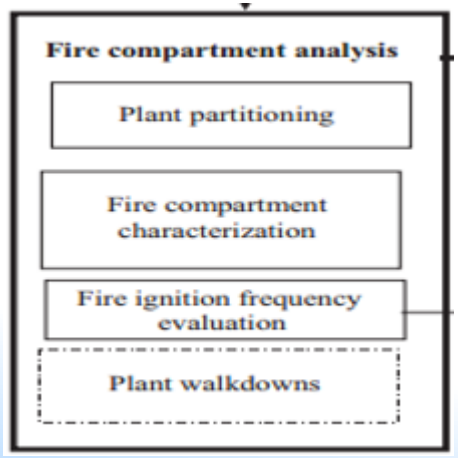
Internal Fire PSA



Internal Fire PSA

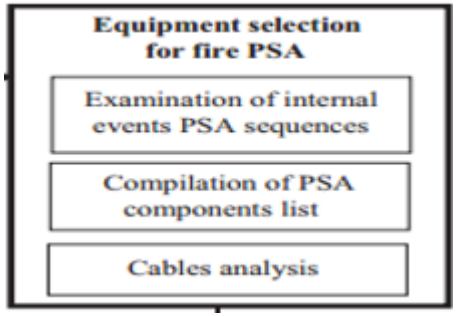
- Data collection
  - Data on fire events
  - Cable routes of the plant
  - Information on the fire compartments, inventory and ignition source
  - Human actions in the event of a fire and human error probabilities
  - fire suppression means
  - Equipment failure information





- For the purposes of the PSA for internal fire, all buildings and structures included in the analysis should be partitioned into distinct fire compartments, which are examined individually
- Walkdowns to Verify and confirm the information, obtain additional information, identify interactions between equipment and areas that may affect fire propagation.

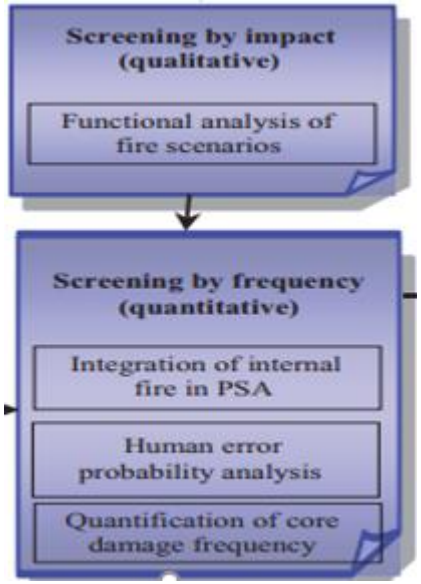
Internal Fire PSA



- The list should include equipment that may:
  - lead to an initiating event
  - affect the ability of safety functions to mitigate an initiating event
  - affect operator actions after the occurrence of an initiating event induced by fire (type C human interactions)
  - lead to spurious actuation of functions that could induce other unsafe effects on the plant

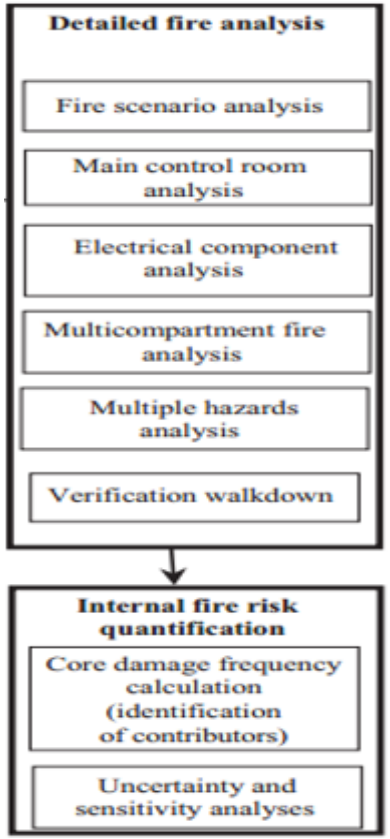
Screening by impact should be used to eliminate non-significant fire scenarios on the basis of qualitative ('impact oriented') criteria. The pessimistic assumptions are made (e.g. equipment in the fire compartment assumed failed)

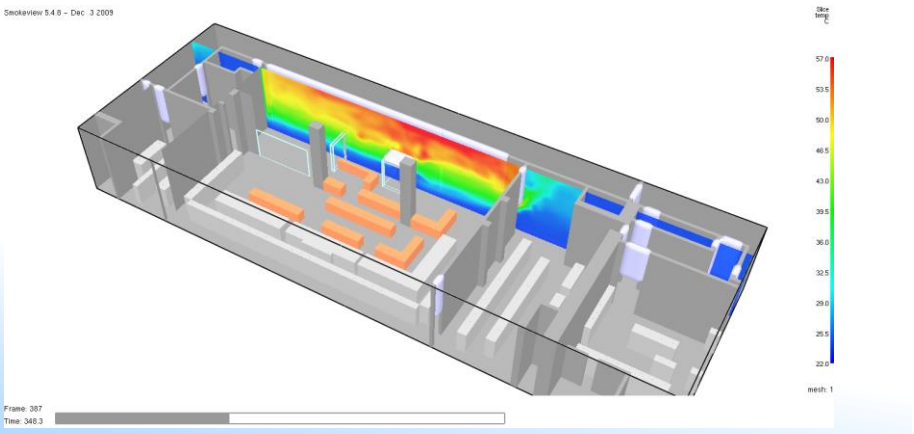
Screening by risk contribution: Integration of internal fire in the Level 1 PSA for internal initiating events, Implementation of assessment. Calculating the contribution of fire to the CDF.



Internal Fire PSA

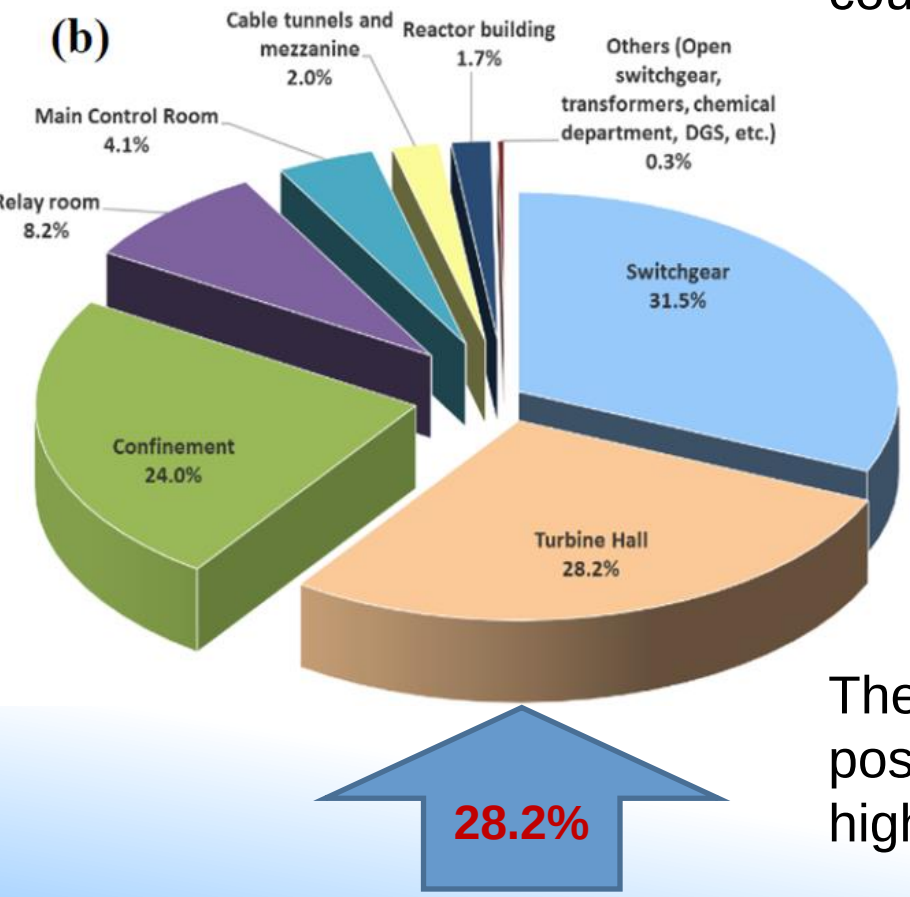
- Is aimed at reducing the level of conservatism in the fire scenarios identified so far in the screening process.
- The effect of fire barriers inside the compartment and other protection means should be taken into account.
- All the effects of fire (flame, plume, ceiling jet, radiant heat from hot gases, high energy arcing and smoke) should be considered
- More realistic models should be applied for assessing human actions for reducing the probability of equipment damage, growth and propagation of fire





Internal Fire PSA

Detailed Fire analysis example



Simplified modeling of fire in Turbine Hall could lead to:

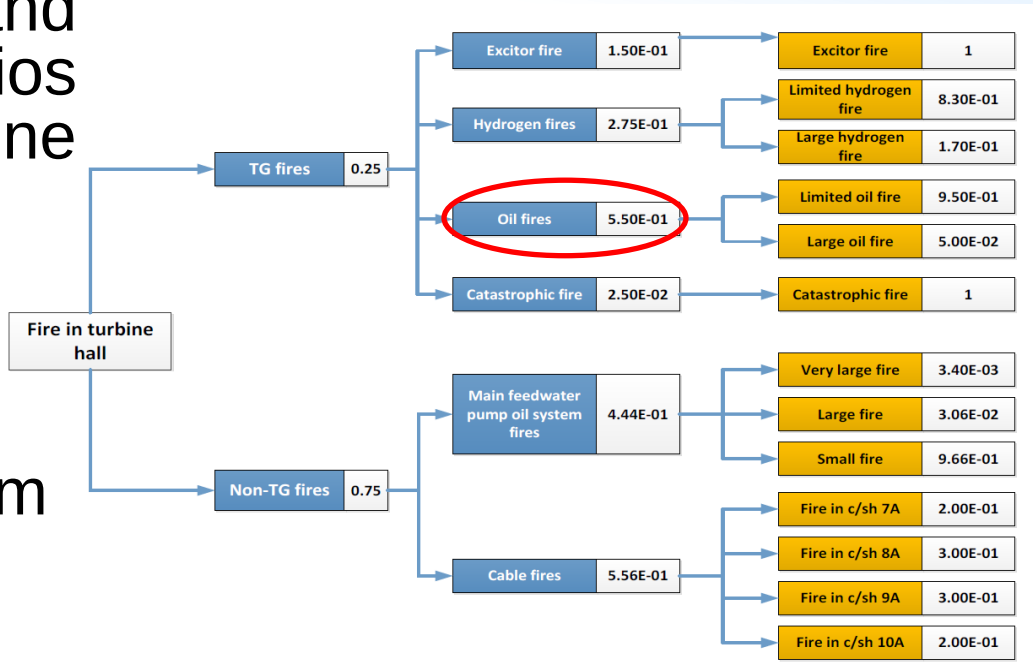
- over-conservative results,
- significant distortion of plant risk profile,
- the inadequate platform for further risk-informed decision making.

The necessity to reveal and address all possible fire induced failure modes was highlighted.

Internal Fire PSA

The ignition sources and corresponding fire scenarios should be identified for Turbine Hall:

- Excitor
- TG oil system
- Main feedwater oil system
- TG hydrogen
- Cable fire
- Catastrophic fire scenario (including all major fire sources)

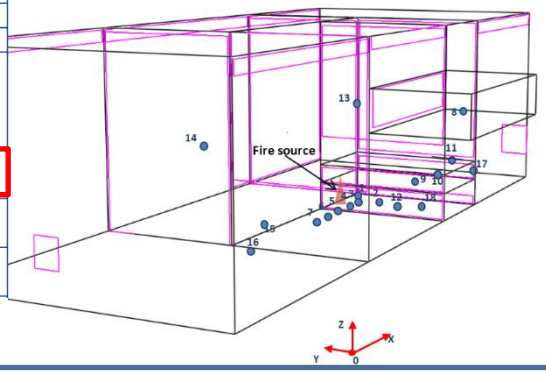


The conditional probabilities were calculated based on NUREG/CR-6850

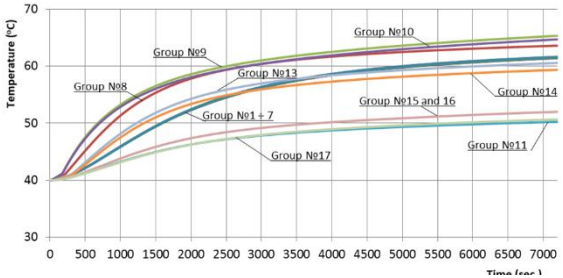
Internal Fire PSA

Detailed fire modeling

Group #	Equipment in the group
Group №1	APEN-1
Group №2	APEN -2
Group №3	PEN-1
Group №4	PEN-2
Group №5	PEN-3
Group №6	PEN-4
Group №7	PEN-5
Group №8	BRU-A TG-3,4; BZOK - I channel; BZOK II channel; RU SG 1÷6; ARU SG 1÷6; 21÷26VP-9; 21÷26VP-10
Group №9	Electrical buses 2804NA, 2601BNN
Group №10	Electrical buses 2518BNN, 2624BNN
Group №11	Electrical buses 2106BN, 2108BNN, 2519BNN,

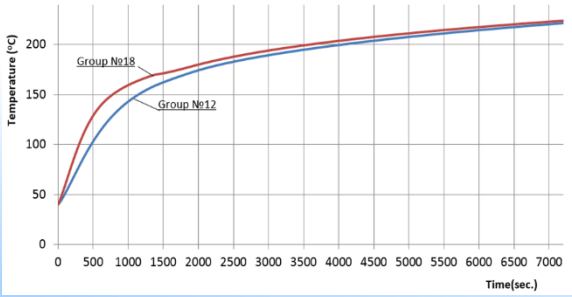


Results



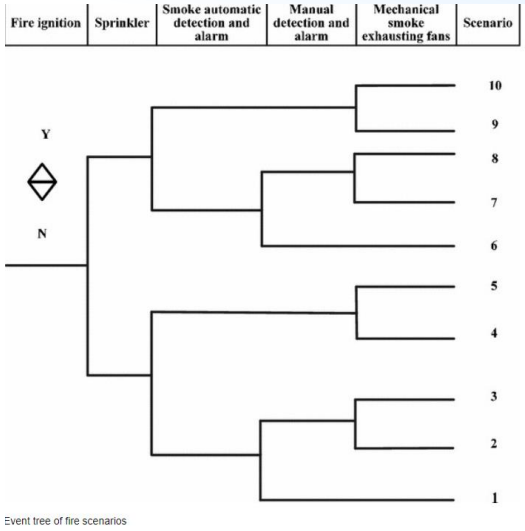
Equipment surface temperature change in time for groups № 1÷11 and №13÷17

Equipment group	Time to failure (sec.)
Group 9	6640
Group 10	7120
Group 12	670

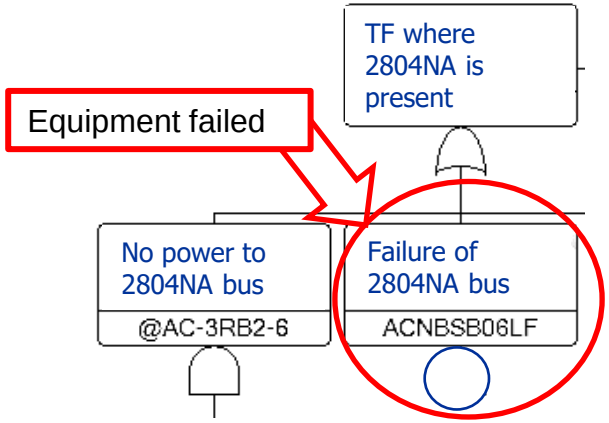


Equipment surface temperature change in time for groups №12 and №18

Integration of detailed analysis results into PSA model

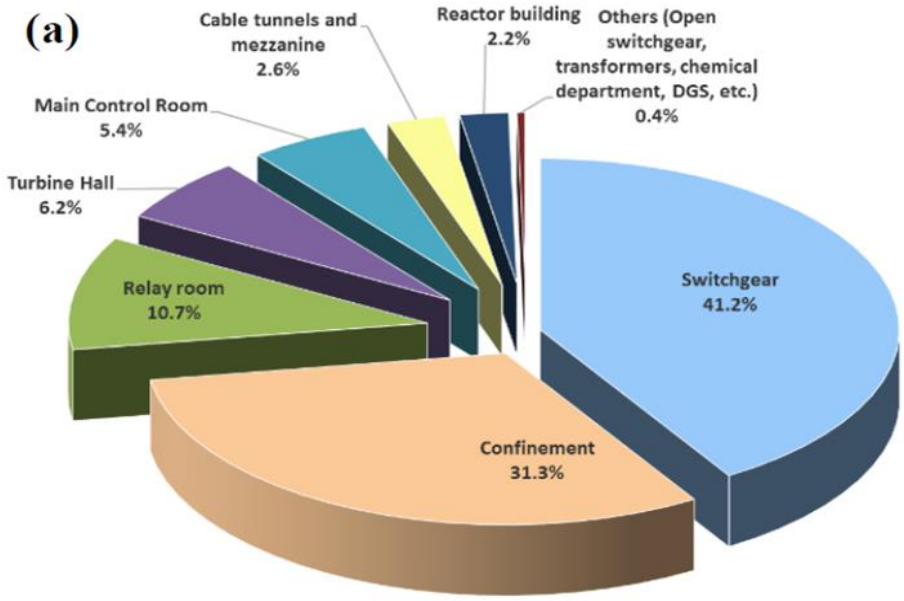


Event tree of fire scenarios

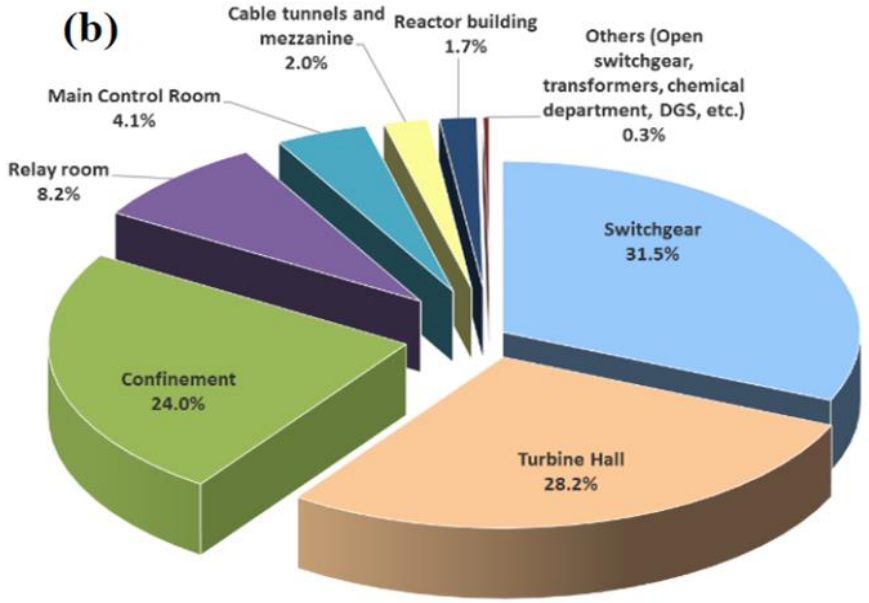


Internal Fire PSA

Detailed Fire analysis example

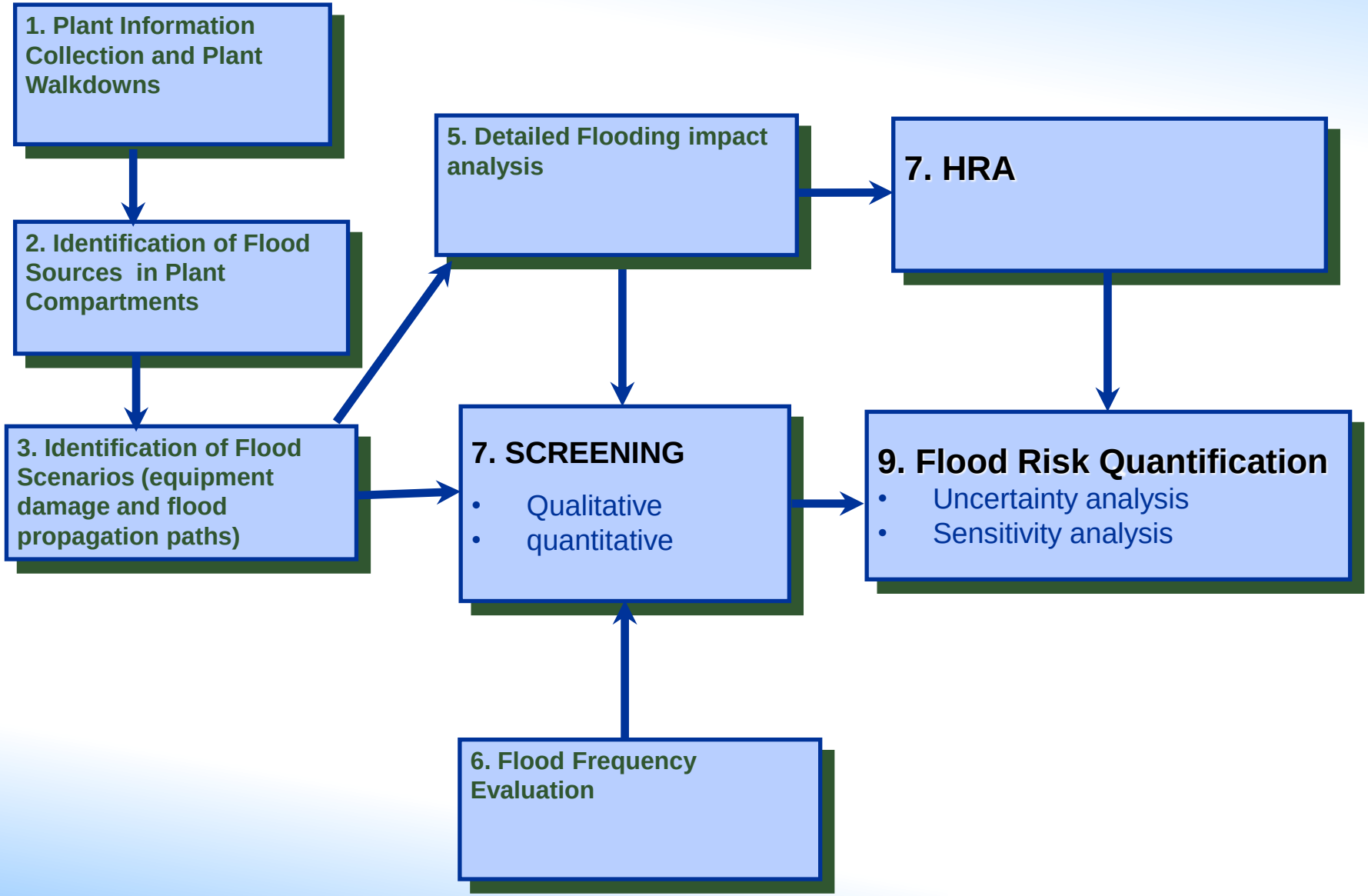


New: Detailed modeling of Turbine building



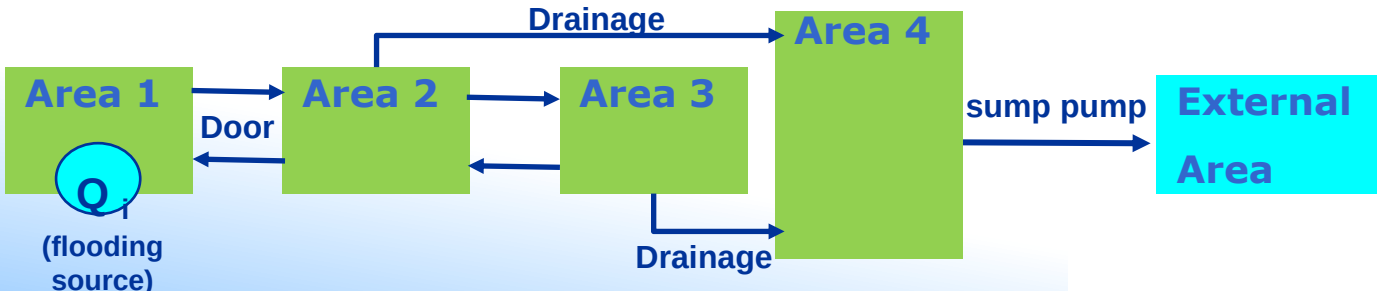
Old: Simplified modeling of Turbine building

Internal Flood PSA



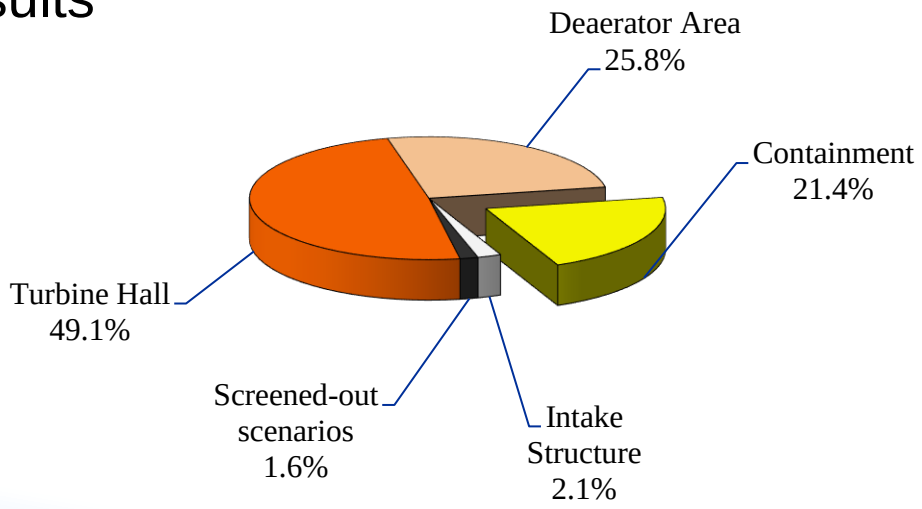
Internal Flood PSA

- Information collected from plant documentation on:
  - Flood sources
  - Flood mitigation
  - Flood barriers
  - Plant connections and penetrations
- Walkdowns of the plant are very important to verify actual conditions and adequate resources should be dedicated for this task
- Identification of flood scenarios
  - For each water source, the propagation of water from the break is analyzed and equipment damaged determined
- Screening analysis:
  - Possibility of initiators due to flood (e.g., flooding of electrical supply)
  - Unavailabilities caused by flood
  - Flood frequencies and quantitative impact



Internal Flood PSA

- Detailed assessment of flooding risk:
  - Timing calculations (flood level vs. time) for recovery
  - Damage to components: based on location with respect to flood source and water level (detailed analysis)
  - Flood detection/isolation: HRA analysis based on available time between detection and damage to targets, and other scenario specific characteristics
- Development of event tree / fault tree models for each scenario (often based on ET/FTs from internal events PSA)
- Quantification & analysis of results



Example of contribution of floods to CDF

Internal hazards (other)

- Other internal hazards such as:
  - Internal missiles;
  - Internal explosions;
  - Heavy load drops.

- The overall methodological stapes are similar to internal fires and floods.

External Hazards

- External hazards originate from the *sources located outside* the site of the nuclear power plant
  - Natural (earthquake, tornado, etc.)
  - Human-induced (airplane crash, accidents at industrial facilities, etc.)

- Natural Hazards
  - Originated from the ground
  - Originated from water
  - Originated from air
- Human Induced Hazards
  - Transportation accidents (including on-site transportation)
  - Accidents at nearby facilities
  - Hazardous material release (including on-site)

- Have a potential for affecting many different *pieces of equipment simultaneously*

External Hazards

A. Structural integrity of buildings or structures

e.g. seismic, aircraft crash, explosion pressure wave

B. Ultimate heat sink

e.g. low sea water level, oil releases, clogging by ice or organic material

C. Air supply (cooling, ventilation,)

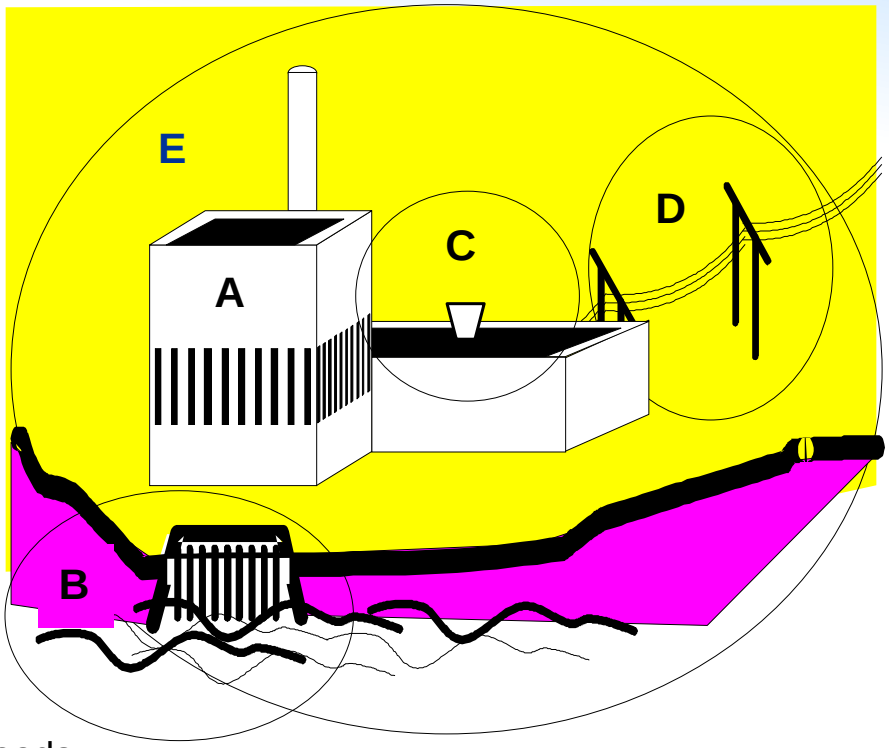
e.g. ventilation blocking or toxic gases

D. External power supply

e.g. salt storm, severe wind, extreme snow loads

E. Operating environment of safety related equipment

e.g. lightning, corrosive gases



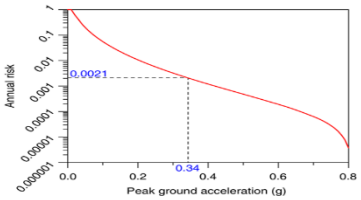
External hazards

Collection of information

Familiarization with the plant, collection of relevant information, walkdowns, etc.

Selection of hazards

Analysis of generic hazard lists, examination of plant buildings, development of plant-specific hazard list

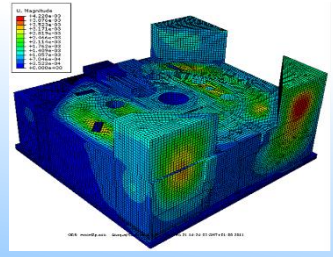


Hazards screening

Screening criteria, quantitative + qualitative screening, hazard parameterization (hazard curves)

Bounding assessment

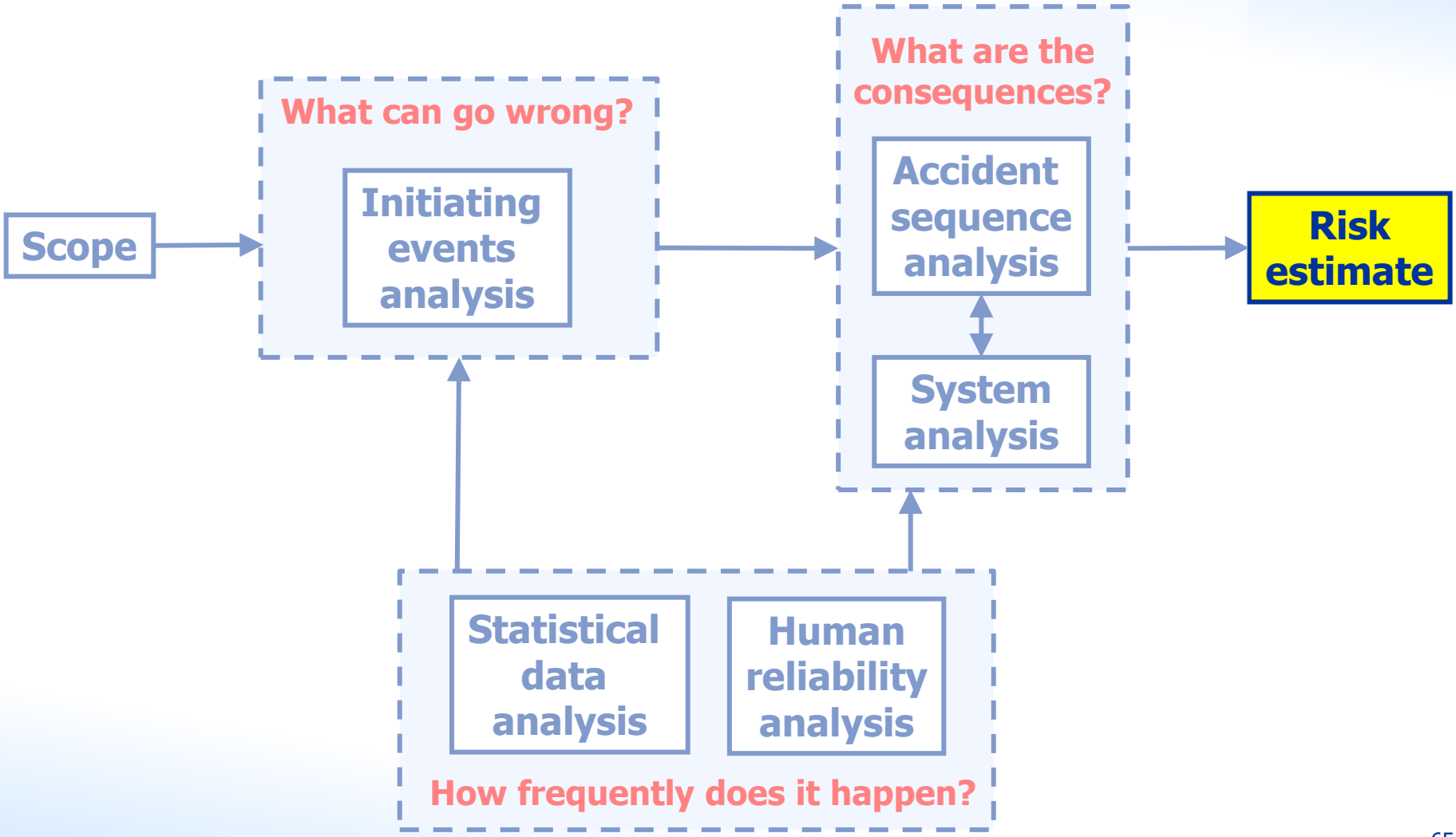
Conservative assessment of selected hazards impact on NPP safety, selection of critical hazards for detailed analysis



Detailed analysis

Detailed analysis of accident scenarios aimed at realistic estimation of the potential damage

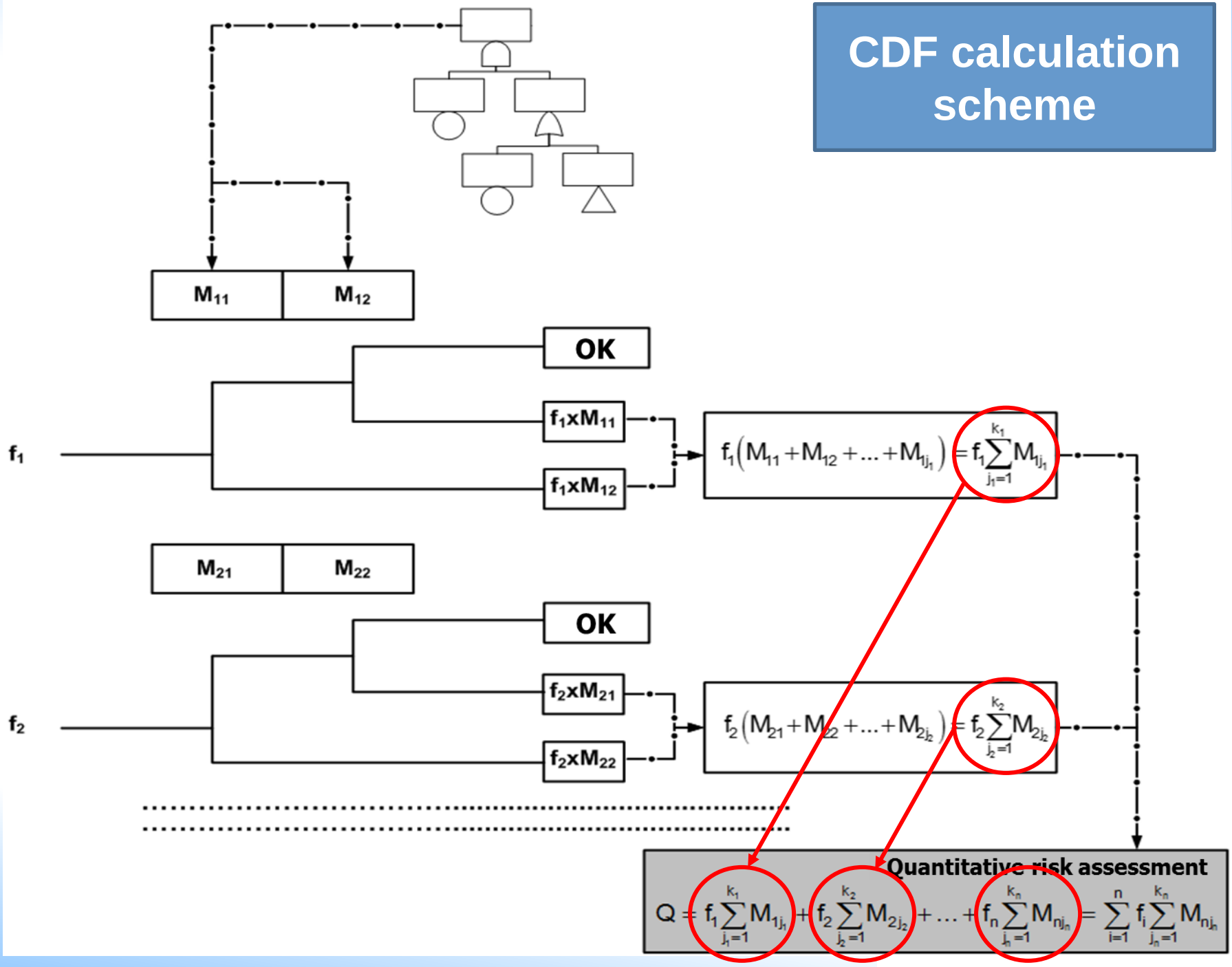
Quantification & Interpretation



Quantification & Interpretation

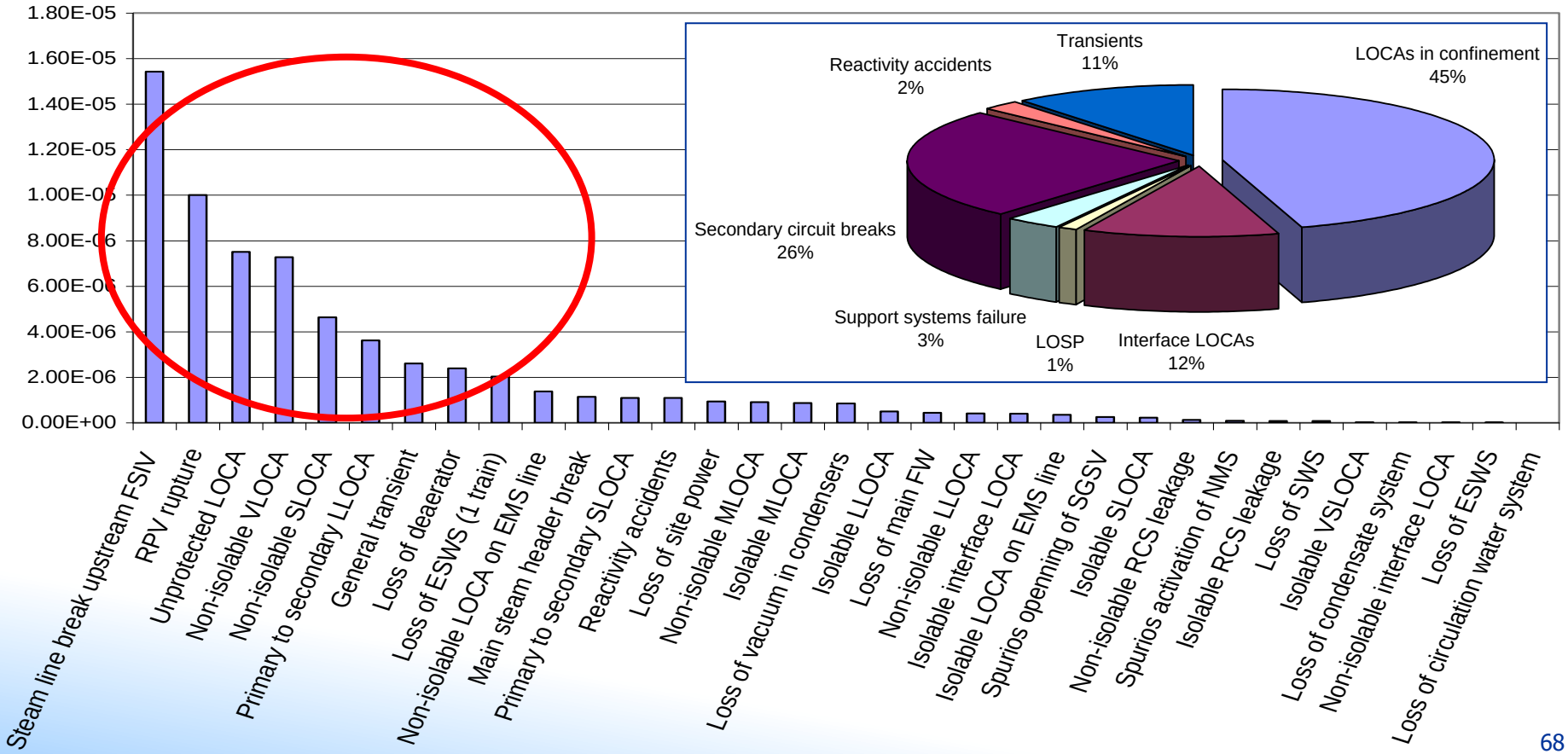
- Quantification and interpretation of PSA model imply implementation of following analysis
  - Analysis of dominant risk contributors (risk profile)
  - Importance analysis
  - Sensitivity analysis
  - Uncertainty analysis

CDF calculation scheme



Quantification & Interpretation

- **Risk profile** should be carefully examined. Further recommendations will be based on main contributors investigation.



Quantification & Interpretation

- **Importance analysis** is performed for following elements of PSA model:
  - basic events
  - attributes (groups of basic events)
  - systems
  - initiating events
  - CCFs

Quantification & Interpretation

- Importance measures

The purpose of an importance evaluation is to identify the important basic events, parameters, systems with regard to the occurrence of the undesired event.

Based on importance measures a ranking can be established to find the most critical events in the risk or reliability model.

Fussell-Vesely importance

$$F\text{-}V = \frac{[\text{sum of all CDF cut-sets containing the basic event}]}{[\text{total CDF}]}$$

F-V < 1, The F-V is a measure of the risk associated with a given basic event, it shows how much component or event contributing to the CDF

Risk reduction worth (RRW)

$$RRW = \frac{[\text{CDF when component is assumed working (P=0)}]}{[\text{total CDF}]}$$

RRW < 1, The RRW is a measure of the risk reduction that would be achieved when the unavailability of a component is reduced to zero, i.e. the event certainly does not occur.

Quantification & Interpretation

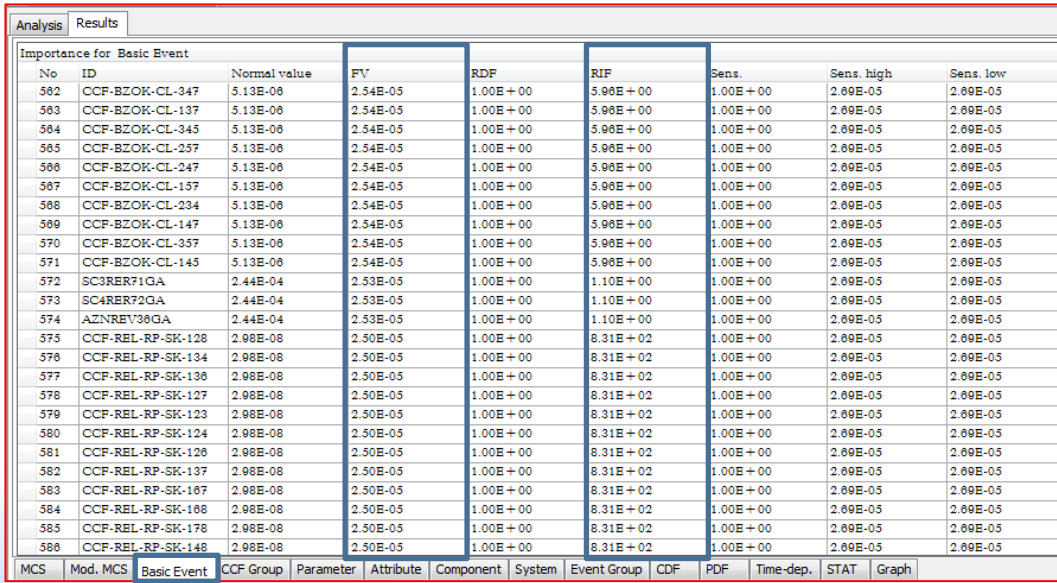
- Importance measures

Risk achievement worth (RAW)

$$RAW = \frac{[\text{CDF when the component is assumed failed } (p=1)]}{[\text{total CDF}]}$$

RAW > 1, The Risk Achievement Worth measure is expressed as a ratio giving the factor by which the top event probability increases due to a component not being available (p=1). It is the change of the outcome in a worst case scenario.

Importance measures are widely used in PSA applications



Analysis | Results

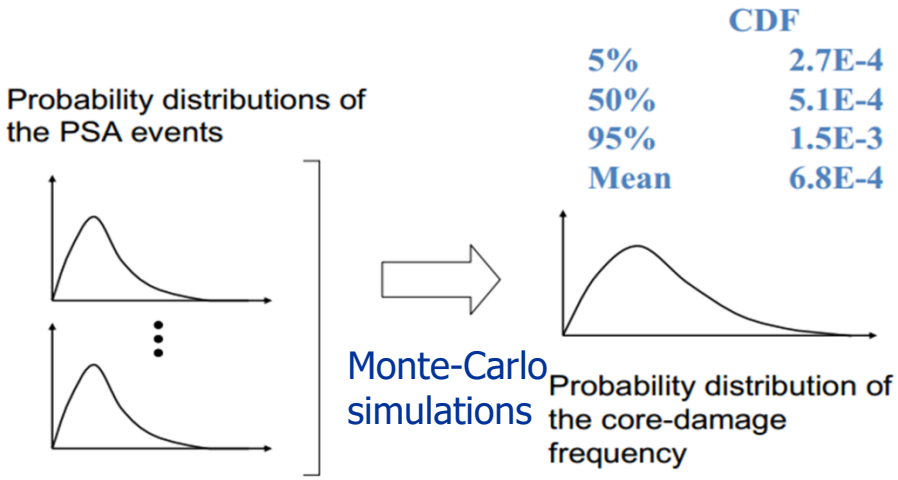
Importance for Basic Event

No	ID	Normal value	FV	RDF	RIF	Sens.	Sens. high	Sens. low
562	CCF-BZOK-CL-347	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
563	CCF-BZOK-CL-137	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
564	CCF-BZOK-CL-345	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
565	CCF-BZOK-CL-257	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
566	CCF-BZOK-CL-247	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
567	CCF-BZOK-CL-157	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
568	CCF-BZOK-CL-234	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
569	CCF-BZOK-CL-147	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
570	CCF-BZOK-CL-357	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
571	CCF-BZOK-CL-145	5.13E-06	2.54E-05	1.00E+00	5.96E+00	1.00E+00	2.69E-05	2.69E-05
572	SC3RER71GA	2.44E-04	2.53E-05	1.00E+00	1.10E+00	1.00E+00	2.69E-05	2.69E-05
573	SC4RER72GA	2.44E-04	2.53E-05	1.00E+00	1.10E+00	1.00E+00	2.69E-05	2.69E-05
574	AZNREV36GA	2.44E-04	2.53E-05	1.00E+00	1.10E+00	1.00E+00	2.69E-05	2.69E-05
575	CCF-REL-RP-SK-128	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
576	CCF-REL-RP-SK-134	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
577	CCF-REL-RP-SK-136	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
578	CCF-REL-RP-SK-127	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
579	CCF-REL-RP-SK-123	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
580	CCF-REL-RP-SK-124	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
581	CCF-REL-RP-SK-126	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
582	CCF-REL-RP-SK-137	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
583	CCF-REL-RP-SK-167	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
584	CCF-REL-RP-SK-168	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
585	CCF-REL-RP-SK-178	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05
586	CCF-REL-RP-SK-148	2.98E-08	2.50E-05	1.00E+00	8.31E+02	1.00E+00	2.69E-05	2.69E-05

MCS | Mod. MCS | Basic Event | CCF Group | Parameter | Attribute | Component | System | Event Group | CDF | PDF | Time-dep. | STAT | Graph

Quantification & Interpretation

- PSA results carry **uncertainty** from two sources
  - aleatory uncertainty or random behaviour - includes data, HEPs, etc. and may be reduced as more statistical data are collected
  - epistemic or “state-of-knowledge” uncertainty – includes assumptions, simplification, etc. may be reduced by new research activities



Quantification & Interpretation

- Before making conclusions about NPP risk or propose NPP modifications to reduce risk the results of PSA should be checked for robustness (partly done in uncertainty analysis)

- **Sensitivity analysis** is aimed to determine the sensitivity of the results of the Level 1 PSA to the assumptions made and the data used.

- How would the PSA results change if …?

- To investigate the influence of the assumptions and limitations on PSA results
  - Change assumption/data/etc. (one by one)
  - Change the event trees, fault trees, equipment unavailability accordingly
  - Regenerate MCSs

Quantification & Interpretation

- The final stage of quantification and interpretation of PSA results is development of insights and recommendations:
  - Detailed description of obtained risk profile
  - Proposed design changes
  - Modification of operating procedures
  - Identification of areas for further investigation

Level 1 PSA project organization

- Level 1 PSA project starts with the definition of the scope and objectives of the project
  - Objectives, potential use of PSA, hazards, operational modes, etc.
- The scope of the PSA should be compatible with both the objectives of the study and the available resources and information (the necessary procedures and methods, personnel, expertise, funding, time)
- After the objectives and the scope of the PSA have been specified, the management scheme for the PSA project should be developed
  - selection of methods and establishment of procedures
  - selection of personnel and the organization of the PSA team
  - training of the PSA team,
  - preparation of a PSA project schedule
  - estimation and securing of the necessary funds,
  - establishment of quality assurance procedures
  - establishment of review procedures (e.g. peer review, inviting IAEA TSR-PSA former IPSART mission, etc.)

Level 1 PSA project organization

- A PSA study is normally commissioned by (a) The plant designer, (b) The operating organization of the plant, (c) The regulatory body.
- The PSA can be performed by these groups or by consultants, research institutes, universities or a combination of these. In any case, the operating organization should always participate as a source of operational knowledge, as well as being a beneficiary from the insights obtained.
- It is desirable to start the process of performing the PSA as early as possible in the lifetime of the plant.
- The documentation for the PSA should be developed in a clear, traceable, systematic and transparent manner so that it can effectively support the review of PSA, applications of PSA and future PSA upgrades.
- The PSA study should consider a particular ‘freeze date’ for modelling theas built and as operated plant conditions.

Level 1 PSA project organization

- Once PSA team is defined the lines of communication should be set up and specific tasks should be assigned.
- The training necessary should be determined and planned
- The expertise necessary to conduct a PSA should provide two essential elements:
  - knowledge of the plant
  - knowledge of PSA techniques

  the participation of the plant designer and the operating organization of the plant should be foreseen, if possible.

- QA program should be established. Appropriate quality - an end product that is correct and usable and one which meets the objectives and fulfils the scope of the PSA.

IAEA
International Atomic Energy Agency
Atoms for Peace and Development

Thank you!