Licensing of New Build Reactors in the UK – Part 2

Keith Ardron
UK Licensing Manager ,
AREVA NP UK

Imperial College – Nuclear Thermalhydraulics Course: February 2014

Contents

Pre-construction Safety Report -Chapter Structure (UK EPR Example)

1	**Introduction and General Description**
2	**Site Envelope and Data**
3	**General Design and Safety Aspects**
4	**Reactor and Core Design**
5	**Reactor Coolant System and Associated Systems**
6	**Containment and Safeguard Systems**
7	**Instrumentation & Control**
8	**Electrical Supply and Layout**
9	**Auxiliary Systems**
10	**Main Steam and Feedwater Lines**
11	**Discharges and Waste – Chemical& Radiological**
12	**Radiological Protection**
13	**Hazards Protection**
14	**Design Basis Analysis**
15	**Probabilistic Safety Analysis**
16	**Risk Reduction and Severe Accident Analyses**
17	**Compliance with ALARP Principle**
18	**Man-Machine Interface and Operational aspects**
19	**Commissioning**
20	**Design aspects in relation to the Decommissioning**
21	**Quality and Project Management**

Deterministic Safety Analysis

Design Safety Principles for New Build Reactors

FIVE LEVELS OF DEFENCE IN DEPTH (IAEA)

- Prevention Use of conservative design, quality assurance, and surveillance activities to prevent abnormal occurrences
- Detection Deviations from normal operation detected and protection devices and control systems provided to cope with them to ensure integrity of the fuel cladding and Reactor Coolant Pressure Boundary
- Mitigation Engineered safety features and protective systems provided to mitigate accidents and prevent their evolution into severe (core melt) accidents
- Severe Accident Control Measures implemented to preserve the integrity of the containment and control severe (core melt) accidents if they occur
- Off-site emergency response Emergency response plans prepared (evacuation and sheltering) to protect public if other defence lines fail

Design Safety Principles for New Build Reactors

DESIGN BASIS INITIATING EVENTS

- Plant must be protected by Safety Systems, Structures and Components to withstand all conceivable initiating events ($f>10^{-6}$/yr)
- Plant initiating events *within the Design Basis* grouped into Categories (Design Basis Conditions – DBC) depending on frequency of occurrence (Example for EPR below). Events analysed by computer modelling to show acceptable outcome
  - DBC 1 : Normal operational transients 1/yr <f
  - DBC 2 : Anticipated Operational Occurrences 10^{-2} <f<1/yr
  - DBC 3 : Incidents 10^{-4} <f< 10^{-2} /yr
  - DBC 4: Accidents 10^{-6} <f< 10^{-4} /yr
- The computer analyses (Fault Studies) use pessimistic data and assumptions to compensate for uncertainties in the modelling of complex events. The degree of pessimism is increased for more frequent IEs
- Hazards (earthquake, flooding, fire, aircraft impact) treated as special class on initiating events due to their ability to affect multiple plant systems simultaneously
- Design Extension Conditions also analysed to cover ‘complex sequences’ that dominate risk in probabilistic analysis: generally these are frequent initiating events combined with common mode failure of Safeguard Systems.

Identification of Plant Initiating Events

- Designers need to demonstrate that list of PIEs used in the Design Basis Analysis is 'complete'
- In the case of PWRs can use feedback experience over 50 years of PWR operation in many countries + judgment of generations of plant designers
- New events may arise during plant operation that were not considered in the design basis…

  - examples….

Identification of IEs from Reactor Operating Experience…

Failure of large pipe in an Essential Cooling Water System: Plant flooding event which threatened important safety systems

Identification of IEs from Reactor Operating Experience…

Fork lift truck collapses services trench containing high voltage cables. Vehicle impact event which threatened grid supplies to site

INTERNAL HAZARDS (EPR EXAMPLE)

- **Hazards are events that could potentially cause widespread plant failures.**
- **For EPR the following Internal hazards considered in the design :**
  - Pipe leaks or ruptures
  - Tanks, Pumps valves ruptures
  - Flooding
  - Fire
  - Internal explosion
  - Load drop
  - Internal missiles
- In EPRs risk of common mode failure due to internal hazards is minimized by locating the four safety trains in separate buildings
- Safety analysis of internal hazards is performed using rules similar to those applied for DBC events (consideration of an additional single failure and of preventive maintenance)

EXTERNAL HAZARDS (EPR EXAMPLE)

- **Following external hazards considered in the design :**
  - Earthquake
  - Airplane crash
  - External explosion
  - External flooding
  - Lightning & electromagnetic interference
  - Groundwater
  - Extreme meteorological conditions (temperature, wind, snow, rain, …)
  - Drought & ice formation
  - Toxic, corrosive and burnable gases
- **For EPRs, protection against external hazards is implemented through load cases assumed in design of buildings and by choice of operating conditions for safeguard systems (e.g. ambient temperature assumed in design of Heating and Ventilation systems).**

Definition and examples of DECs & Severe Accidents

- **DECs: sequences involving IE combined with failure of a major safety system, where core melt is averted by use of back-up systems e.g.**
  - **Station Blackout (Loss of offsite power combined with failure of all 4 Emergency Diesel Generators)**
  - **Main feedwater failure combined with failure of the 4 Emergency Feed trains,**
  - **SB-LOCA combined with failure of all 4 Medium Head Injection trains**
  - **SGTR combined with stuck open SG relief valve**
- **Severe Accidents : core melt accident in which a large release of radioactivity to environment is prevented e.g.**
  - **LOCA with total failure of all Safety Injection Systems**
  - **SBO with failure of all diesel generators (including 2 back-up DGs)**

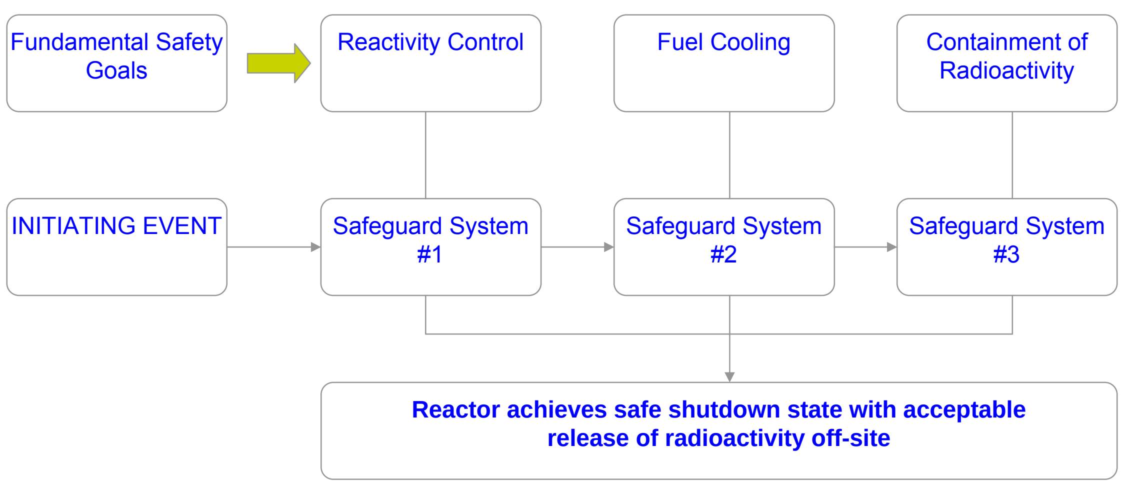
Design Safety Principles for New Build Reactors

SAFETY CLASSIFICATION

- **Structures, systems and components, including instrumentation and control systems must be 'Safety Classified' on the basis of their function and significance to safety.**
- **Standards of design, construction, maintenance, quality and reliability depend on classification.**
- **Method of classification generally based on deterministic approach, complemented by probabilistic methods. Classification level depends on factors such as:**
  - **the safety function performed by the item;**
  - **the consequences of failure to perform its function;**
  - **the probability that the item will be called upon to perform a safety function;**
  - **the time following the initiating event at which it will be called upon to operate.**
- **Classification requirements can impact strongly on capital costs of plant**

Design Safety Principles for New Build Reactors – Safeguard Systems (1/2)

SAFEGUARD SYSTEM DESIGN



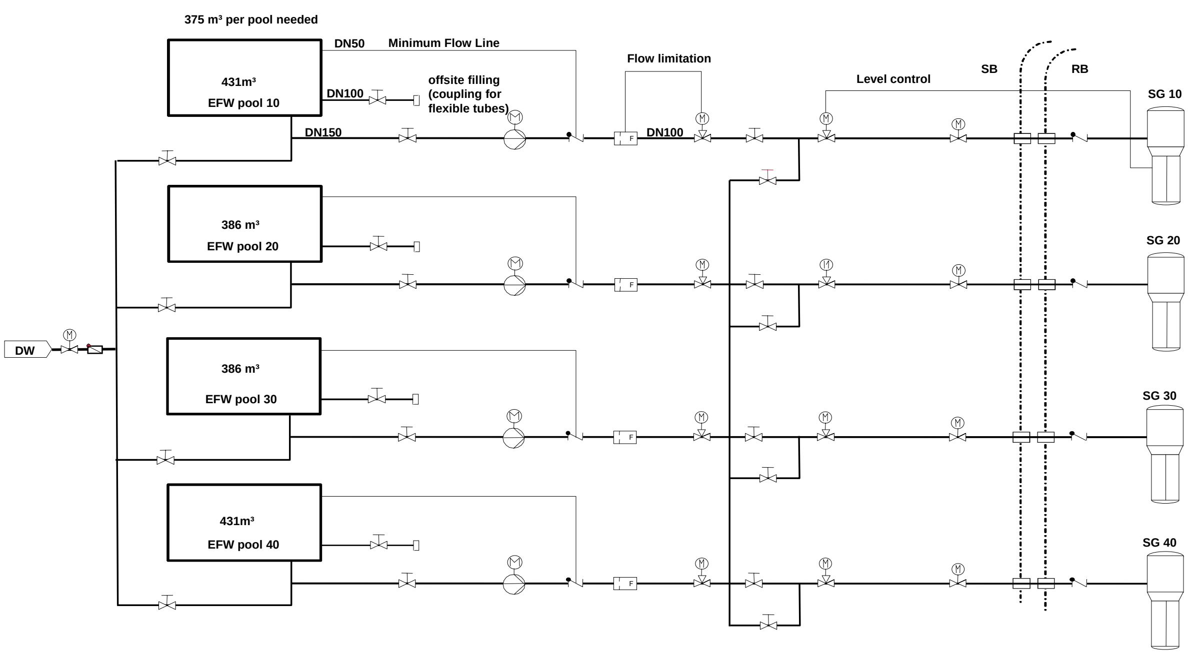
Design Safety Principles for New Build Reactors - Safeguard Systems (2/2)

SAFEGUARD SYSTEM DESIGN: General Principles

- System must be functionally capable of achieving a safe plant shutdown state with an acceptably small release of radioactivity off-site
- System must contain enough redundant elements (trains) so that its function can be performed with any single randomly occurring failure in addition to initiating event (single failure principle)
- System must contain sufficient multiple redundant elements (trains) so that its function can be performed in any normal maintenance state
- Common cause failure of redundant trains of a safeguard system must be considered in the design basis. A back-up system of diverse design must be provided if required to meet probabilistic targets (e.g. core melt frequency limit)

➡ ***4 TRAIN CONCEPT***

Safeguard System – Example: EPR Emergency Feedwater S



SG Steam Generator
EFW Emergency Feedwater
DW Demineralized Water
RB Reactor Building
SB Safeguard Building

Functional diversity: system backup: EPR Example

Safety-grade system	Diverse system functions		
MHSI Medium Head Safety Injection System	Fast Depressurization via Secondary Side + Pressurizer Relief Valve	Accumulator Injection System	Low Head Safety Injection System
LHSI Low Head Safety Injection System	Medium Head Safety Injection System	For small breaks: Secondary Side Heat Removal System	
RHR Residual Heat Removal System	RCS closed: Secondary Side Heat Removal System	RCS open: Medium Head Safety Injection System + Steaming into the Containment	
FPC Fuel Pool Cooling System	Fuel Pool Water Heat-up with subsequent Steaming + Coolant make-up		
Diesels	SBO Diesels		
EFWS Emergency Feedwater System + Steam relief	Primary side Bleed via the Primary Depressurization System (PDS)	Primary side Feed with MHSI	

Design Safety Principles for New Build Reactors

MITIGATION OF SEVERE ACCIDENTS

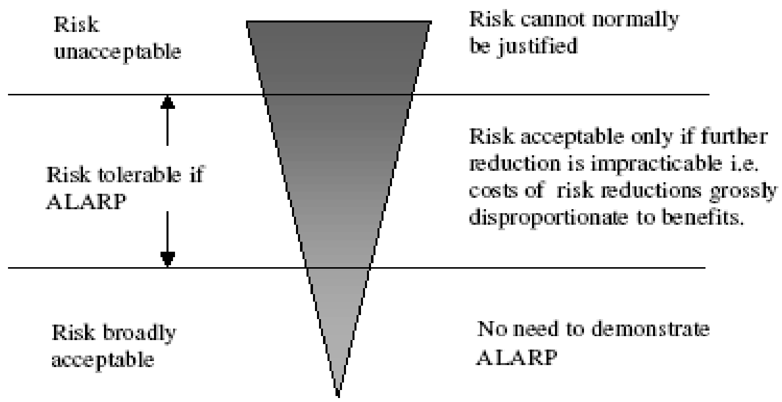
- **Latest Generation of NPPs (Generation 3 plants) have 4th level of defence to prevent off-site radioactivity release if Safeguard Systems fail to prevent core melt**
- **Examples of design features for core melt mitigation (EPR):**
  - **Containment building designed to remain leak-tight at high pressures and temperatures characteristic of core melt conditions**
  - **Core catcher prevents basemat melt-through in the event of release of melted fuel from RPV**
  - **Recombiners prevent build-up of H2 in containment (explosion risk)**
  - **Dedicated instruments provide operators with information on plant conditions in core melt scenarios**

CORE MELT SPREADING COMPARTMENT (CORE CATCHER) AT OLKILUOTO 3 EPR

Risk Targets & ALARP

- In UK a supplementary requirement is to demonstrate that the risk of harm to workers and the public due to radiation from operation of a nuclear reactor is As Low As Reasonably Practicable (ALARP)
- To demonstrate ALARP, must show that the cost and difficulty of reducing risk is grossly disproportionate to the risk reduction achieved
- HSE have defined the risk as Broadly Acceptable if the chance of the most exposed member of public receiving a dose >1000mSv due to an accident at a power plant is below 1 in 10^6 /yr (risk of death $=10^{-6}$/yr).
- HSE have defined the Maximum Tolerable risk as that where the chance most exposed member of public receiving a dose >1000mSv reaches 1 in 10^4 /yr (risk of death $=10^{-4}$ /yr).
- For existing UK nuclear installations, risks up to the Maximum Tolerable level can be justified to HSE if the risk is ALARP
- For new build reactors, HSE require the risk to be Broadly Acceptable;

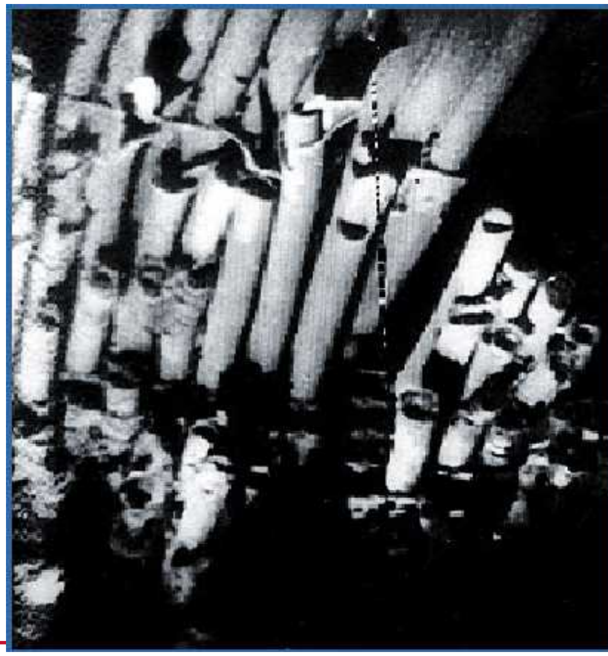
Risk Targets & ALARP (HSE, 1990, Tolerability of Risk from Nuclear Reactors)



Probabilistic Analysis

- **Generation 3 plants are designed to meet probabilistic targets.**
- **For EPR**
  - Core melt frequency due to all events and hazards in all plant states (power operation, shutdown, refuelling) must be below a prescribed maximum ($<10^{-5}$/yr)
  - Risk of large release of radioactivity off-site requiring evacuation/sheltering of members of public must also be practically eliminated ($<10^{-7}$/yr)
  - Risk levels are calculated using Probabilistic Safety Analysis (PSA)
  - PSA techniques originally developed for aerospace industry. Widespread use in nuclear power industry began in 1980s after accident at Three Mile Island plant in US
  - PSA has been used in the design of Generation 3 plants such as EPR to identify where back-up systems are required to mitigate against common mode failure of Safeguard Systems

TMI 2 – Above Core Region: PSA Motivator



PSA method for Reactor Analysis

- **Level 1 PSA: analysis of initiating events and equipment failures that result in core damage (output is core melt frequency/ reactor year)**
- **Level 2 PSA: Failure states from the Level 1 PSA are input to Containment Event Trees whose outcomes are frequency of different Radioactivity Release Categories (RRC- isotope quantities released to environment) (output is frequency of different RRCs/reactor year)**
- **Level 3 PSA: Release categories and frequencies from the Level 2 PSA are used to calculate the frequency of human health and economic consequences for the local population (output is frequency of individual radiation doses of different magnitude or total fatalities/reactor year).**

PSA method – Event Tree

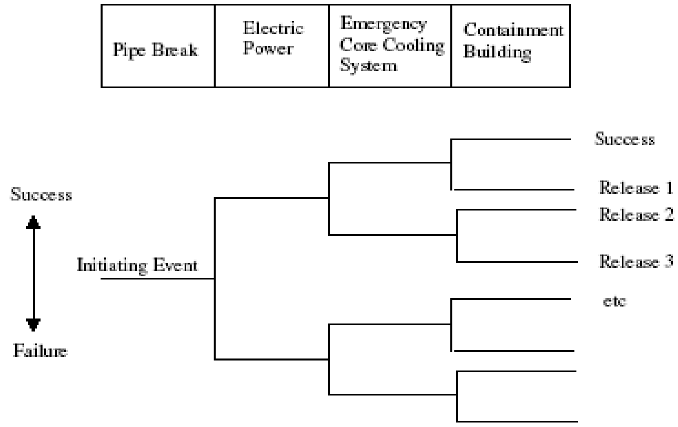
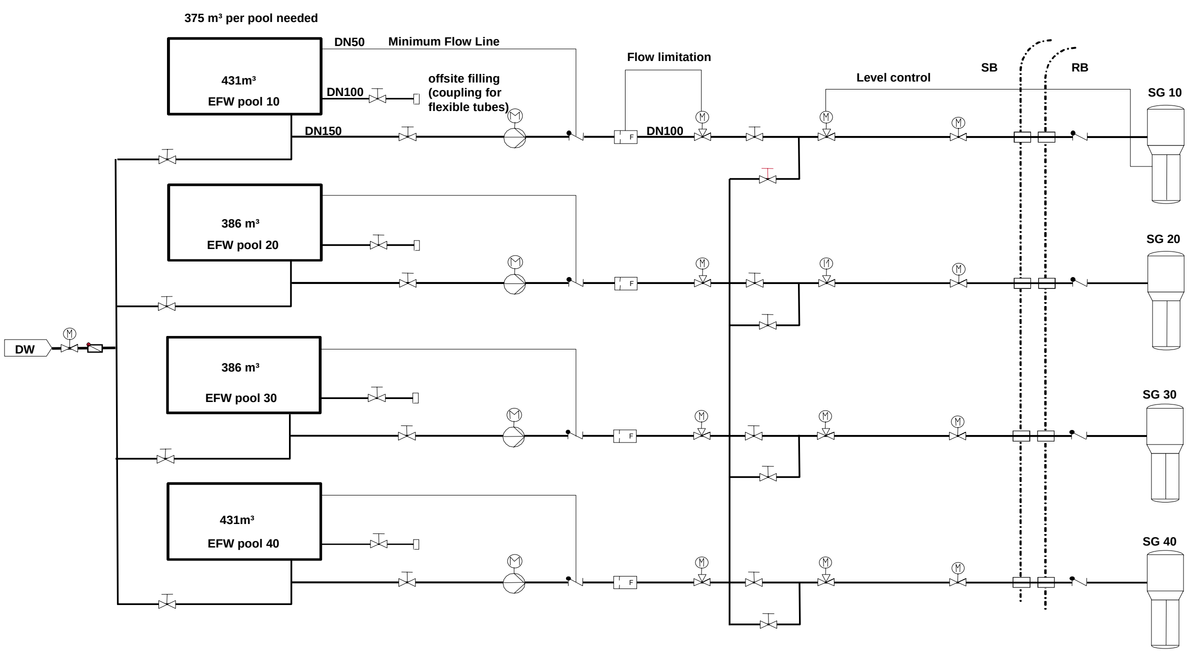


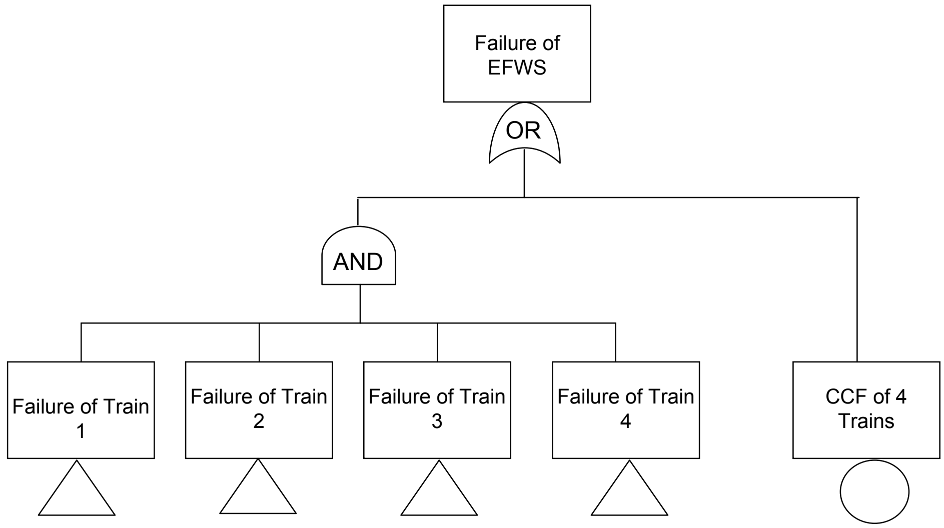
Fig 5 Illustrative Event Tree

PSA Method - Fault Tree – Emergency Feedwater System Example

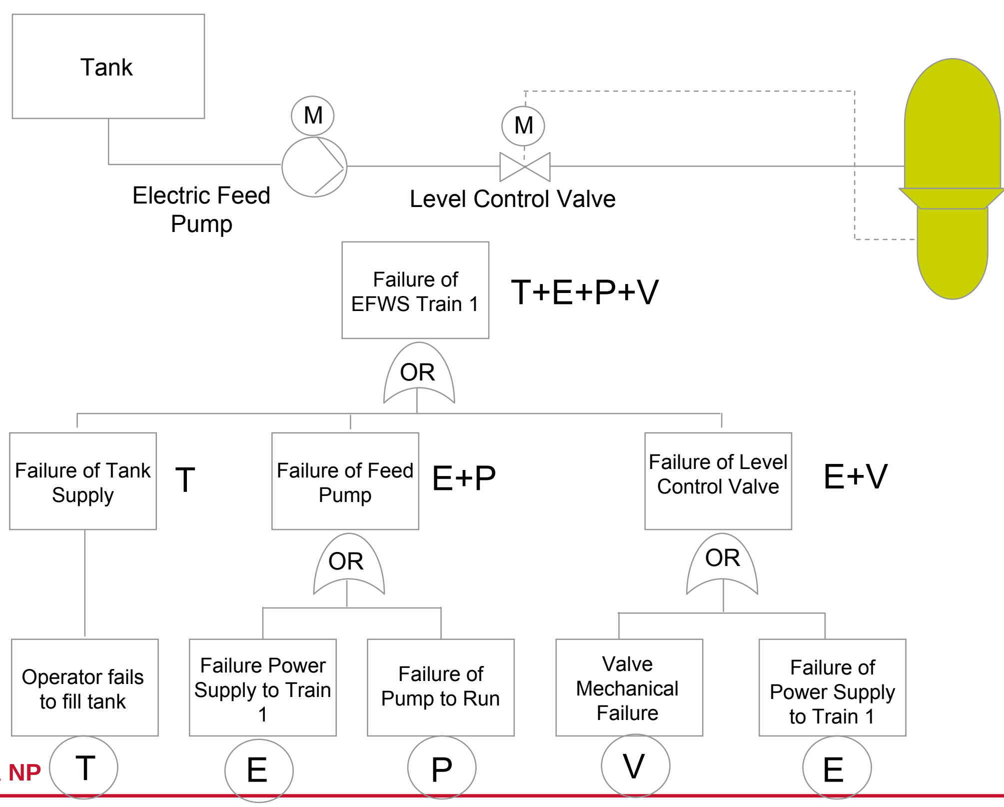


SG Steam Generator
EFW Emergency Feedwater
DW Demineralized Water
RB Reactor Building
SB Safeguard Building

EFWS – Illustrative Fault Tree



EFWS Train #1 – Simplified Fault Tree



MINIMUM CUT SET – BOOLEAN ALGEBRA

$$F = A.D + B.C + C.D.E + \ldots\ldots$$

F = failure of function at top of fault tree (units = probability of failure/demand)

A, B, C = Basic Events (mutually independent)

+ = Logical OR . = Logical AND

Elements containing combinations appearing elsewhere in the summation must be eliminated (Law of absorption defined in Boolean Algebra)

(Thus A+A.B=A etc)

Final elements of summation after elimination are the minimum combinations of basic events that would result in failure of function (F) – called *minimum cutsets*

Minimum cutsets are generated by a computer code using a Boolean reduction algorithm

Once minimum cutsets have been determined, probability of failure usually calculated by first order summation (so called rare event approximation, valid if P(A)<<1 etc):

$$P(F) = P(A)P(D) + P(B)P(C) + P(C)P(D)P(E) + \ldots$$

MEASURES OF IMPORTANCE OF BASIC EVENTS (1/2)

- In the Level 1 PSA for NPPs, the event trees and the fault trees are solved simultaneously to derive the core melt frequency (CMF) as:

$$F_{CD} \text{ (/reactor year)} = \Sigma\, f_i\{ s_1 s_{2\ldots} s_n\}^j$$

Summation taken over all initiating events f_i and minimum cutsets j

Note that f_i have units (/reactor year); s_k have units (failures/demand)

MEASURES OF IMPORTANCE OF BASIC EVENTS (2/2)

- Fussel-Vesely factor (FV) and Risk Increase Factor (RIF) are used to measure the importance of a basic event to F_{CD} the overall CMF
- FV= ratio of cutsets containing the basic event to the total CMF

$$F_{CD} = \underbrace{S_A B}_{\text{Cutsets containing } S_A} + \underbrace{C}_{\text{Cutsets not containing } S_A} \qquad (1)$$

- If FV_A is Fussel-Vesely factor for S_A then by definition

$$FV_A = S_A B / F_{CM} \qquad (2)$$

Hence from (2)

$$(\Delta F_{CM}/F_{CM}) = FV_A (\Delta S_A / S_A)$$

FV_k = Measure of fraction of core damage frequency contributed by a component or initiating event

USE OF IMPORTANCE FACTORS IN SYSTEM DESIGN

In Nuclear Power Plant design we must assign components to Safety Class (1, 2, 3, NC) depending on its importance to safety

Classification decisions can have strong impact on plant cost – but no consensus on how to link Safety Class of equipment to its "Safety importance"

PSA metrics such as FV_k can help us decide the reliability required for a system or component

USE OF PSA METRICS IN SYSTEM DESIGN

A possible way of determining the *maximum acceptable failure probability* (MAFP) of a component could be to require that the component should not contribute more than 0.1% (say) to the target Core Melt Frequency for the plant i.e.

CMF contribution due to failure of component A ≤ 10^{-8}/yr

This implies, from (1)

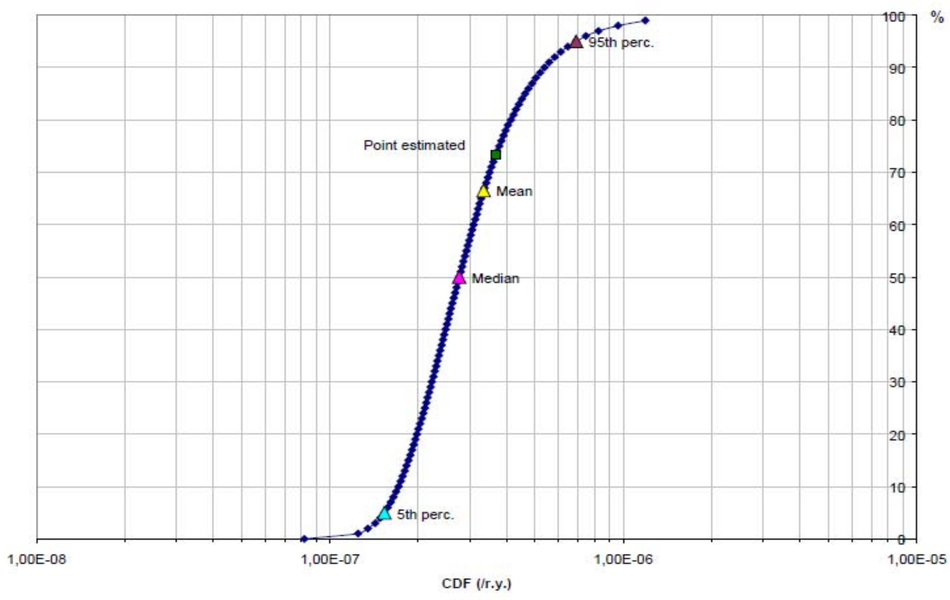
$$S_{A,MAX}\,B = 10^{-8}/yr \qquad (3)$$

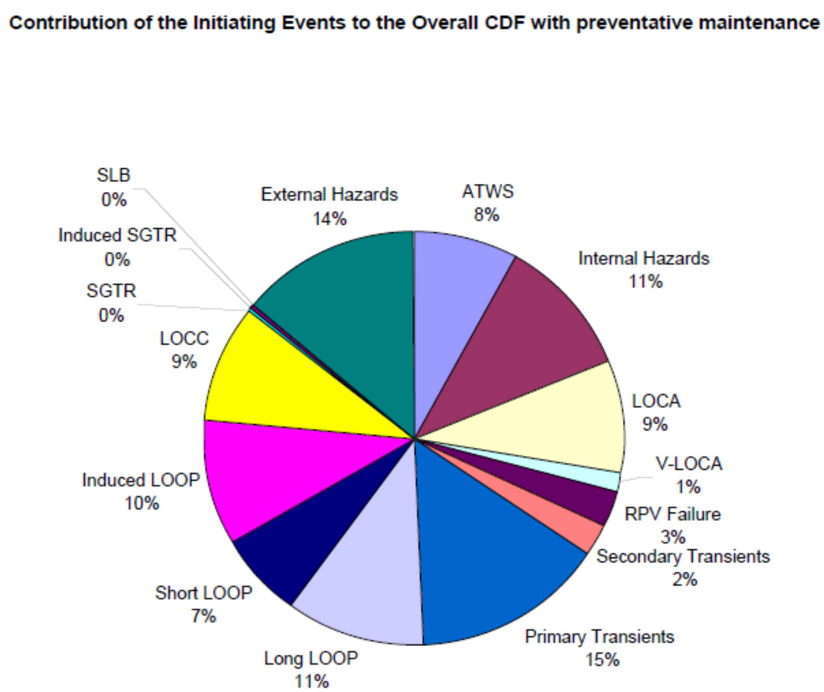
Using (2) to eliminate B, and using the PSA result for CMF: F_{CD}=5.10^{-7}/yr

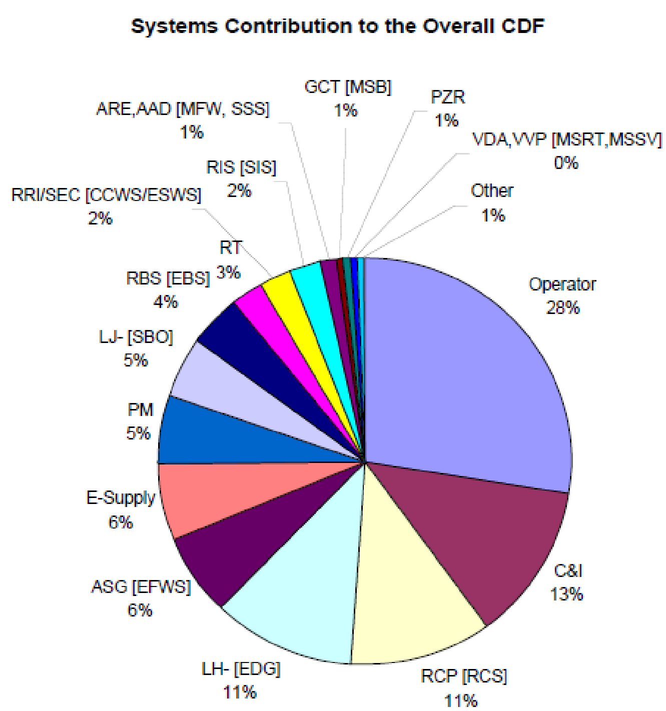
$$S_{A,MAX}=2.10^{-2}S_A/FV_A \qquad (4)$$

System Class Required	Probability of failure on demand (failures/demand)	MAPF Range (failures/demand)
Class 1	10-3 ≥ *fpd* ≥ 10-5	MAPF ≤10^{-3}
Class 2	10-2 ≥ *fpd* > 10-3	10^{-3}< MAPF ≤10^{-2}
Class 3	10-1 ≥ *fpd* > 10-2	10^{-2}< MAPF ≤10^{-1}
NC	*fpd* > 10-1	10^{-1}< MAPF

EPR Level 1 PSA – CDF Showing Uncertainty




Contribution of the Initiating Events to the Overall CDF with preventative maintenance
SLB
0%
External Hazards
14%
ATWS
8%
Induced SGTR
0%
Internal Hazards
11%
SGTR
0%
LOCC
9%
LOCA
9%
V-LOCA
1%
Induced LOOP
10%
RPV Failure
3%
Secondary Transients
2%
Short LOOP
7%
Primary Transients
15%
Long LOOP
11%


Systems Contribution to the Overall CDF
GCT [MSB]
1%
PZR
1%
ARE,AAD [MFW, SSS]
1%
VDA,VVP [MSRT,MSSV]
0%
RIS [SIS]
2%
RRI/SEC [CCWS/ESWS]
2%
Other
1%
RT
3%
RBS [EBS]
4%
Operator
28%
LJ- [SBO]
5%
PM
5%
E-Supply
6%
C&I
13%
ASG [EFWS]
6%
LH- [EDG]
11%
RCP [RCS]
11%