Twinning Project Turkey

Workshop: Systems Engineering

Ankara, Turkey
26th and 27th of September 2018
<table>
<thead>
<tr>
<th>No</th>
<th>Topic</th>
<th>Day / Time</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Wed 26.09.2018</td>
<td></td>
</tr>
</tbody>
</table>
| 1  | Failure Mode and Effects Analysis  
    • Fields of application  
    • Methodology | 09:30 – 12:00 |         |
| 2  | Overarching protection goals  
    • Control of reactivity  
    • Fuel cooling  
    • Confinement of radioactivity  
    • Limitation of radiation exposition | 12:00 – 12:30 |         |
|    | Lunch Break | 12:30 – 13:30 |         |
| 3  | Defence-in-Depth Concept  
    • Level 1: Normal Operation  
    • Level 2: Abnormal operation  
    • Level 3: Design Basis Accidents  
    • Level 4: Beyond Design Basis Accident | 13:30 – 14:00 |         |
| 4  | Applicable Events  
    • Level 1: e.g. power ramps  
    • Level 2: e.g. loss of high pressure preheater  
    • Level 3: e.g. loss of coolant accident (LOCA), earthquake  
    • Level 4: e.g. station black out (SBO), loss of primary heat sink | 14:00 – 15:30 |         |
| 5  | Engineered Safety Systems  
    • Level 1: Operational systems  
    • Level 2: Limitation systems  
    • Level 3: Safety systems (e.g. reactor protection)  
    • Level 4: Severe accident management guidelines (SAMG’s) | 15:30 – 16:30 |         |
<table>
<thead>
<tr>
<th>No</th>
<th>Topic</th>
<th>Day / Time</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Safety Classification of SSC • Applicable Criteria • Safety Classes 1 to 4 or equivalent</td>
<td>Thu 27.09.2018</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Design of Safety Systems • Redundancy concept (single failure, maintenance case) • Diversity (common cause failure)</td>
<td>09:30 – 11:00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lunch Break</td>
<td>11:00 – 12:30</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Operating manual and Changes • Content of Operating Manual in German NPP • Plant modifications • Examples</td>
<td>12:30 – 13:30</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Wrap-up Questions</td>
<td>13:30 – 15:30</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>15:30 – 16:30</td>
<td></td>
</tr>
</tbody>
</table>
Risk Analysis

Failure Mode and Effects Analysis
acc. to DIN EN 60812
FMEA Methodology

Risk Analysis Method

- identify and quantify risks in technical systems / processes

Fields of Application

- broad field: automotive, rail, process industry (e.g. chemical), power generation etc.

Target

- e.g. personnel protection / operability / environment / nuclear safety
FMEA Methodology

FMEA - Systematic Approach
Overview

- Definition
- System Analysis
- Risk Analysis
- Implementation of Measures
- Final Report
FMEA Methodology

Definition
- Focus / Target
- Scope
- Boundary Conditions

System Analysis
Risk Analysis
Implementation of Measures
Final Report
FMEA Methodology

Focus / Target

• focus only on changed functions / equipment (e.g. at plant revamp)
• personnel protection / operability / environment / nuclear safety

Scope

• system or process to be analyzed
• system limits

Boundary Conditions

• plant states to be considered (e.g. normal / abnormal operation, maintenance, commissioning etc.)
• e.g. consideration of SF or CCF
Structural Analysis

**Structural elements** of the system to be analyzed e.g.
- mechanical components (e.g. Moisture Separator Reheater, Feedwater Pumps)
- electrical / I&C components (e.g. Automated Turbine Testing System)

Functional Analysis

**Specified Functions** of the structural elements established

Failure Analysis

For the **Functions** defined above the **Failure-Effects-Chains** to be established:
- What can go wrong in fulfilling these **Functions**
- What are the **causes** and the **effects** thereof
FMEA Methodology

Structural element “MSR”

Functional Analysis

Specified Function(s):
- increase steam quality to $x=1$
- reheat steam at certain $T$ (K)
- deliver steam to LP turbine at certain $Q$ (kg/s)
- ...

Failure Analysis

Malfunction(s) / departure(s) from specified function(s):
- steam quality increased to $x < 1$
- ...

Failure-Effects-Chains
Effects < Failure Mode < Cause
FMEA Methodology

Failure-Effects-Chains
Effects < Failure Mode < Cause

• What are the possible causes for these Malfunctions / Failure Modes
• What are the effects thereof on operability / personnel / nuclear safety / environment etc.

for function ‘increase steam quality to x=1’

power reduction < turbine trip < LP turbine wear/damage < increase steam quality to x < 1,0 < insufficient moisture separation < failure of moisture separator module < defect < not properly maintained

Caution:
• Focus on changes (e.g. functional, electrical, I&C, hardware etc.)
• Causes of failure: as precise as possible
• Single Failure to be considered
FMEA Methodology

- Definition
- System Analysis
- Risk Analysis
- Implementation of Measures
- Final Report

FMEA table
## Categorization: Severity

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very low / negligible</td>
<td>No or negligible damage component / system; function / performance not (or imperceptibly) affected; Negligible / no implications in plant operation: short load reduction (some hours); Restoration not necessary</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>Low impact on component / system; function / performance slightly affected; Plant operable at reduced power 80-95%; Restoration of function / performance on plant-own means (spare parts, maintenance base etc.); low restoration time and cost</td>
<td>2</td>
</tr>
<tr>
<td>Medium</td>
<td>Considerable deterioration in performance of component / system; Impact on plant operation (plant operable at reduced power 64-80%); Performance / damage of component / system restorable on plant-own means (spare parts, maintenance base etc.); considerable restoration time and cost</td>
<td>3</td>
</tr>
<tr>
<td>High</td>
<td>Component / system inoperable (damaged/unavailable); Severe implications in plant operation (load reduction below 64% or scram); Heavy damage of component / system, repairable but not on plant-own means and at high cost (restoration time and cost)</td>
<td>4</td>
</tr>
<tr>
<td>Very high</td>
<td>Component / system destructively affected (inoperable); failure / damage immediately affecting plant’s overall safety or violating statutory regulations; Plant immediately inoperable; Damage irreparable or economically not reasonable</td>
<td>5</td>
</tr>
</tbody>
</table>
### Categorization: Occurrence

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Flaw rate in ppm</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost impossible</td>
<td>Cause of failure mode very unlikely to occur / occurrence likelihood negligible (1 time / 30 years)</td>
<td>1-50</td>
<td>1</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Cause of failure mode unlikely to occur (1 time / 10 years) / an appropriate and proven safety concept exists</td>
<td>50-100</td>
<td>2</td>
</tr>
<tr>
<td>Occasionally</td>
<td>Cause of failure mode not often to occur (1 time / 3 years) / an appropriate safety concept exists, which has been applied to similar projects</td>
<td>100-5.000</td>
<td>3</td>
</tr>
<tr>
<td>Probably</td>
<td>Cause of failure mode probable to occur (1 time / 1 year) / a not proven safety concept with respect to this cause exists</td>
<td>5.000-30.000</td>
<td>4</td>
</tr>
<tr>
<td>Frequently</td>
<td>Cause of failure mode to occur frequently (more often than once a year) / there is no safety concept to meet this cause</td>
<td>30.000-500.000</td>
<td>5</td>
</tr>
</tbody>
</table>

These rates are commonly used in the automotive industry.
## Categorization: Detection

<table>
<thead>
<tr>
<th>Category of detectability</th>
<th>Description</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>Failure mode or its cause very likely to be detected through testing / monitoring; an appropriate and proven detection method exists</td>
<td>1</td>
</tr>
<tr>
<td>High</td>
<td>Failure mode or its cause likely to be detected through appropriate and proven detection method</td>
<td>2</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate detection likelihood of failure mode or its cause; an appropriate detection method exists, which has been applied to similar projects</td>
<td>3</td>
</tr>
<tr>
<td>Low</td>
<td>Poor detection of failure mode or its cause; detection method not sure or valid</td>
<td>4</td>
</tr>
<tr>
<td>Very low</td>
<td>Unlikely detection of failure mode or its cause; testing not performed or not possible to be performed; Faults during manufacturing / installation not detected</td>
<td>5</td>
</tr>
</tbody>
</table>
FMEA Methodology

- if RPN < 27, risk is acceptable, no improving measures necessary

- if RPN > 27, risk needs to be reduced, improving measures necessary

Measures to **avoid** causes of Failure Modes (preventive measures)

Measures to **detect** Failure Modes or their causes
FMEA Methodology

Measures to **avoid** causes of Failure Modes (preventive measures)

- Administrative / organizational measures
  - working instructions
  - personnel qualification
- Technical measures
  - (safety) equipment
  - automation

Measures to **detect** Failure Modes or their causes

- Control / check
- Monitoring
- etc.
  - triggering automatic / manual actions before effects set in
<table>
<thead>
<tr>
<th>Component / Process</th>
<th>Function</th>
<th>Possible effects (on operability)</th>
<th>S</th>
<th>Possible Mode</th>
<th>Possible Causes</th>
<th>Measures to avoid failure mode or its cause</th>
<th>O</th>
<th>Measures to detect failure mode or its cause</th>
<th>D</th>
<th>RP</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR</td>
<td>Increase steam quality to $x=1$</td>
<td>power reduction $&lt;\text{turbine trip}&lt;\text{LP turbine wear/damage}$</td>
<td>4</td>
<td>steam quality increased to $x &lt; 1.0$</td>
<td>insufficient moisture separation $&lt;\text{failure of moisture separator module}&lt;\text{defect}&lt;\text{not maintained properly}$</td>
<td>high quality manufacturing of moisture separator; component testing in workshop; preventative maintenance of MSR's</td>
<td>2</td>
<td>temperature monitoring of MSR steam outlet; flow monitoring of MSR condensate; periodic inspection of MSR's</td>
<td>2</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>MSR</td>
<td>Increase steam quality to $x=1$</td>
<td>power reduction $&lt;\text{turbine trip}&lt;\text{LP turbine wear/damage}$</td>
<td>4</td>
<td>steam quality increased to $x &lt; 1.0$</td>
<td>insufficient reheating $&lt;\text{reheater tube damage or shell side (cycle steam flow distribution abnormal}&lt;\text{defect}$</td>
<td>component design/sizing specified per plant heat balances; high quality manufacturing of moisture separator; preventative maintenance of MSR's</td>
<td>3</td>
<td>planned periodic inspection of MSR's; temperature monitoring of MSR steam outlet</td>
<td>2</td>
<td>24</td>
<td></td>
</tr>
</tbody>
</table>
Protection Goals
Protection goals and their compliance in German nuclear power plants
Application of protection goals

- Are used in the basic design of new nuclear power plants

- Are used for the evaluation of nuclear installations during periodic safety reviews

- To this end, the subordinate safety functions are evaluated (the safety functions correspond to active and passive technical measures for compliance with the protection goals).
Protection Goals

Safety goal

Protection against ionising radiation

Protection goal

Control of radioactivity

Cooling of the fuel elements

Confinement of radioactive substances

Limitation of radiation exposure

Safety functions

Measures
Protection Goals

Limitation of radiation exposure

NO
**Protection Goals**

*Limitation of radiation exposure*

To comply with this protection goal, there are several measures, such as:

- Filtering installations in the exhaust air, waste gas and sewage systems
- Shielding, barriers and the locking concept

- Reduction of activity concentrations in systems, on surfaces and in indoor air
- Environmental monitoring
Confinement of radioactive substances

The protection goal “confinement of radioactive substances” is safeguarded through the barrier concept at normal power operation.
Protection Goals

Confinement of radioactive substances

Furthermore, the radioactive substances are detained due to the graded underpressure concept (lowest pressure in the containment)
Protection Goals

Confinement of radioactive substances

When barriers are destroyed, protection goals are safeguarded through the following safety functions:

- Containment isolation (cutting off all systems penetrating the containment – provided the are not credited to control the applicable event)
- Ventilation isolation
**Protection Goals**

**Control of reactivity**

To meet this protection goal following systems are needed:

- that allow a rated criticality of the core during startup,
- that are required to control the core according to the requested load ramps,
- that in case of accidents enable the safe shutdown of the reactor (SCRAM) and ensure that the core remains subcritical.
Protection Goals

Control of reactivity

• For PWR these are the following systems:

• Control rods with their drives to regulate power or SCRAM
• Borating system for startup (deborating of primary cooling system) to long-term power control and borating to ensure undercriticality when reactor shut down
**Protection Goals**

**Cooling of the fuel elements**

- To meet this protection goal all systems serving the reactor core and the fuel storage pool cooling are needed. In a pressurized water reactor (PWR) these systems are:

  In the reactor:
  - the primary circuit
  - the emergency core cooling systems
  - the secondary circuit including the emergency feedwater systems

  In the fuel storage pool:
  - fuel storage pool cooling system
TOP 3

Defence-in-Depth
Defence-in-Depth Concept
acc. to IAEA Specific Safety Requirements SSR-2/1 (Rev. 1)

- Defence in depth involves the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment.

- If one level of protection or barrier were to fail, the subsequent level or barrier would be available.

- This concept is applied to all safety related activities, whether in full power, low power or various shutdown states.

- This is to ensure that all safety related activities are subject to independent layers of provisions so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures.
Defence-in-Depth

Physical Barriers Concept

Implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations.
Defence-in-Depth

IAEA Levels

- Level 1: Normal Operation
- Level 2: Abnormal Operation
- Level 3: Design Basis Accidents
- Level 4: Beyond Design Basis Accidents
- Level 5: Accident Mitigation
Defence-in-Depth

German Safety Requirements for NPP

- Level 1: Normal Operation
- Level 2: Abnormal Operation
- Level 3: Design Basis Accidents
- Level 4: Beyond Design Basis Accidents
  - 4a: very rare events (but: covered by plant design, like DBA)
  - 4b: events with multiple failure of safety systems
  - 4c: severe accidents with failure of fuel elements
Level 1: Normal Operation

The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety.

This leads to requirements that the plant shall be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices.

To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning.

Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence.

Attention is also paid to the processes and procedures involved in design, manufacture, construction, and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.
The purpose of the second level of defence is to **detect and control deviations** from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions.

This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them.

This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or otherwise to minimize their consequences, and to return the plant to a safe state.
Defence-in-Depth

Level 3: Design Basis Accidents

For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop.

In the design of the plant, such accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety systems and procedures shall be in place being capable of preventing damage to the reactor core or preventing radioactive releases requiring off-site protective actions and returning the plant to a safe state.
Defence-in-Depth

Level 4: Beyond Design Basis Accidents

The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth.

This is achieved by preventing the progression of such accidents and mitigating the consequences of a severe accident.

The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized.

Event sequences that would lead to an early radioactive release or a large radioactive release are required to be ‘practically eliminated’.
Level 5: Accident Mitigation

The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents.

This requires the provision of adequately equipped emergency response facilities and emergency plans and emergency procedures for on-site and off-site emergency response.
Applicable Events
Events at Level 1:

Normal operation
- Full power operation
- Power reduction according to grid operator
- Power changes >50%
- Power operation between 30 and 45%

Power changes
- Continuous power changes
- Power ramps
Events at Level 1:

- These operation modes are „normal operation“
- All protection goals are met
- Plant shall be simply monitored


**Events at Level 2:**

All events where further operation is possible without shutting down the power plant.
Events at Level 2:

Here to belong following events:

- Load rejection to houseload
- Turbine trip
- Failure of external grid
- Spurious opening of turbine by-pass valves
- Spurious closing of one main steam isolation valve
- Reactor coolant pump trip
- Malfunction or failure of feedwater supply
- Malfunction of one control rod
- Non-closing of pressurizer spray valves
- Spurious alarm "activity high" during power operation
- Spurious alarm "steam generator level"
Detection of a fault in level 2 (abnormal operation)

Example: Reactor coolant pump trip

At the signal "speed low" of the RCP the control rods are positioned like that, that the reactor power is reduced quickly to about 45%. At the same time, the generator power is reduced to 45%.

Since the corresponding steam generator of the loop with the failed pump delivers only 3% of the total output, the corresponding feedwater control is switched to low load.

The primary flow direction of the loop with the defect RCP turns.

The system is stabilized at a capacity of approx. 40% through the coolant temperature control and can continue to be operated in 3-loop operation.

Conclusion: Continued operation of the system is possible, albeit only with limited power
Events at Level 3:

Events in the nuclear power plant,

with SCRAM,

which, however, are controlled by the safety systems due to the basic design of the power plant

without endangering the protection goals
Events at Level 3:

Here to belong following events:

- Small LOCA without actuation of emergency cooling criteria
- Medium-size LOCA
- Non-closing of pressurizer spray valve or a small leakage in pressurizer steam area
- Big LOCA
- Steam generator tube leakage with/without exceeding radiation limits
- Primary leakage outside containment (JNA)
- Leakage in feedwater pipes outside containment
- Small leakage in secondary circuit inside containment
- Leakage in main steam pipe outside containment
- Non-closing of main steam safety or blow-off valves after actuation
- Secondary circuit undercooling transient (malfunction feedwater)
- RCP shaft break
- Loss of Offsite Power (LOOP)

- External events (airplan crash, earthquake)
Detection of a fault in level 3 (event)

For example: LOOP
**Applicable Events**

*Lost of Offsite Power (LOOP):*

**Process:**
- No external electricity supply possible
- Island operation fails

**Consequences:**
- 4 main cooling pumps fail – SCRAM/automatical turbine trip
- No main cooling water supply
- No feed water supply

**Check protection goals:**
- No leakages – Limitation of radiation exposure and containment of radioactive material not relevant
- SCRAM - Sufficient undercriticality ensured

!!! Cooling of fuel elements is still relevant !!!
**LOOP:**

Process:

Primary circuit

Natural circulation: Heat produced in the reactor is transported naturally to the steam generator. No pumps needed.

Secondary circuit

Steam generator fed by small feedwater pumps or emergency feedwater system

Heat is transported via main steam safety valves into the air

Details later!!!
With the exception of the "Terrorist Airplane Crash Threat" event, all events are brought under control under consideration of protection goals. Emergency procedures are prepared for each protection goal.
Events at Level 4:

Control of reactivity

- Safeguarding of subcriticality by actuation of volume control system *KBA* and Extra Borating System *JDH*
Applicable Events

Events at Level 4:

Cooling of Fuel Elements

- Secondary bleed and feed
- Emergency feeding of deionate pool
- Primary bleed
- Heat removal through main steam safety valves
- Heat removal through mobile short cooling chain
- Fill-up spent fuel pool after power cut
- Decay heat removal from spent fuel pool through pressure reduction of the containment
Confinement of radioactive substances (integrity of containment)

- Filtered venting of containment *JMA 30*
Events at Level 4:

Limitation of radioactive substances release

- Sampling *UJA* (PRONAS)
Events at Level 4:

For execution of the emergency measures, auxiliary systems and functions are needed.

This is, essentially, the electricity supply.

To ensure these functions work, emergency procedures are also prepared.
Events at Level 4:

These functions are:

- Use of the 3rd grid supply to feed the steam generator
- Emergency power supply D2-grid with mobile emergency diesel generator 1
- Emergency power supply D2-grid with mobile emergency diesel generator 2
**Events at Level 4:**

Further measures are:

- Mobile accident filtering for MCR
- Refilling of diesel fuel to use existing resources onsite
- EDG operation during a long-term LOOP (up to one week)
- Preventive measures at threatening flooding
**Events at Level 4:**

After every SCRAM a post-SCRAM-control by using the protection goals shall be done.

In case of an event at level 3 the use of Operating Manual (Part 3) is sufficient for complying with the protection goals.

Through the protection goals control we are entering into the preparing internal emergency procedure.
Applicable Events

Example (KKI 2) – Page 1

Source: KKI 2 - copyrighted
TOP 5

Safety Systems
Safety Systems
Safety Systems

Level 1: Normal Operation

• Frequency of plant state / event: regularly

• Technical features and measures: Operational components and systems

• Design principles: Conservative design
  Qualitative characteristics
  Monitoring
  Personnel qualification
Safety Systems

Level 2: Abnormal Operation

- Frequency of plant state / event: often

- Technical features and measures: Control devices / systems
  Limitation devices / systems
  Component protection devices

- Design principles: Inherent safety
  Thermohydraulic stability
  Reactor physics stability
Safety Systems

Level 2: Abnormal Operation

Examples of technical features and measures:

- Normal (process) control devices or installations (flow, temperature, pressure, level)
- Turbine control system
- Reactor power control system (power adaptation, limitation)
- Pump protection installations (minimum quantity, by-pass, cavitation protection, vibration protection)
Safety Systems

Level 3: Design Basis Accidents

• Frequency of plant state / event: rarely

• Technical features and measures: Engineered safety systems

• Design principles: Redundancy
  Diversity
  Fail safe
  Physical separation
  Automatisation
  Autarky
Safety Systems

Level 3: Design Basis Accidents

Requirement 61: A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions.

Passive or active safety systems

The reactor protection system monitors certain crucial safety parameters (e.g. T, P, voltage), combines logical values and then actuates the corresponding safety system to control the event in question.

There is a variety of safety systems in place to cope with a variety of events/accidents.
Safety Systems

Examples of Engineered Safety Systems

High pressure safety injection system

Low pressure safety injection system

Primary circuit overpressure protection system
  relief valve of a pressurizer, discharge into a relief tank

Secondary circuit overpressure protection system

Emergency boron injection system
  Ensure subcriticality, leakage compensation, ATWS

Emergency feedwater system
Safety Systems

Level 4: Beyond Design Basis Accidents

4a: Special, very rare events -> e.g. APC, EPW

• Frequency of plant state / event: Very rarely

• Technical features and measures: Selective preventive measures

• Design principles: Specific design requirements
Safety Systems

Level 4: Beyond Design Basis Accidents

4b: (Genuine) beyond design basis events

• Frequency of plant state / event: Very rarely

• Technical features and measures: Plant internal emergency protection measures

• Design principles: Flexibility in using existing installations / equipment

State-of-the-art emergency installations
Level 4: Beyond Design Basis Accidents

4b: (Genuine) beyond design basis events

e.g. multiple failure of redundant systems

Station Black Out (SBO), Loss of Ultimate Heat Sink

To cope with these events some additional equipment is needed on site, e.g. mobile EDG, mobile electrical and/or fire-fighting pumps, hosepipes and additional connections to intermediate cooling system heat exchanger (usually fed by the fire fighting system or with water from a well).

Measures: secondary / primary bleed and feed, mobile short cooling chain
Level 4: Beyond Design Basis Accidents

Source: ROSATOM-CICE&T
VVER 1200
Corium localization system
The corium localization system (or core catcher) is one of the technical means specially envisaged to manage severe beyond design basis accidents at the off-vessel stage. The core catcher performs intake, placement and cooldown of the molten materials of the core, reactor internals and reactor pressure vessel up to complete crystallization.
Containment hydrogen removal system ensures:

Under design basis accidents the system maintains hydrogen concentration at levels excluding a hydrogen detonation.

The hydrogen removal system equipment includes a set of passive autocatalytic hydrogen recombiners.
Safety Systems

Level 4: Beyond Design Basis Accidents

4c: damage situations with implications for the environment

- Frequency of plant state / event: Extremely unlikely / practically impossible
- Technical features and measures: External emergency management / civil protection
- Design principles: International rules e.g. Severe Accident Management Guidelines

Goal: to maintain containment integrity as long as possible
TOP 6

Safety Classification
Safety Classification

IAEA Specific Safety Requirements SSR-2/1 (Rev. 1)

The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, considering:

(a) The safety function(s) to be performed by the item;
(b) The consequences of failure to perform a safety function;
(c) The frequency with which the item will be called upon to perform a safety function;
(d) The time following a postulated initiating event at which the item will be called upon to perform a safety function.
Safety Classification

Classification Approach

- Generic / specific
- Prescriptive / less prescriptive
- Deterministic / deterministic combined with probabilistic approach
- Time-independent / time-dependent safety functions
- However: all are based on the same fundamental principles!
<table>
<thead>
<tr>
<th>Functions credited in the safety assessment</th>
<th>Severity of the consequences if the function is not performed</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Functions to reach a controlled state after anticipated operational occurrences</td>
<td>Safety category 1</td>
</tr>
<tr>
<td>Functions to reach a controlled state after design basis accidents</td>
<td>Safety category 1</td>
</tr>
<tr>
<td>Functions to reach and maintain a safe state</td>
<td>Safety category 2</td>
</tr>
<tr>
<td>Functions for the mitigation of consequences of design extension conditions</td>
<td>Safety category 2 or 3</td>
</tr>
</tbody>
</table>
Safety Classification: IAEA

IAEA SSG-30

**SSC Safety Class?**

According to Safety Category of the functions performed
The HSE follows a deliberately non-prescriptive approach to site licensing.

Vendor/Designer/Site Licence Applicant to identify those SSCs that contribute to safety, to classify them according to their significance (on a consequence basis) and provide evidence as to why the Codes & Standards proposed to be applied to the design of those SSC are appropriate.

HSE stipulates the criteria for the safety classification of SSCs in the Safety Assessment Principles (SAPs) for Nuclear Facilities and the pertinent Technical Assessment Guide (TAG) T/AST/008.
SAP, Paragraph 149: Categorising of Safety Functions

- Category A – any function that plays a **principal role** in ensuring nuclear safety.
- Category B – any function that makes a **significant contribution** to nuclear safety.
- Category C – any other safety function

The method for categorising safety functions should take into account:

- consequence of failing to deliver the safety function;
- extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults;
A safety classification scheme could be determined on the following basis:

- **Class 1** – any structure, system or component that forms a principal means of fulfilling a Category A safety function.

- **Class 2** – any structure, system or component that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function.

- **Class 3** – any other structure, system or component
Safety Classification: HSE (UK)

International Nuclear and Radiological Event Scale (INES)

- 1 Anomaly: Below Scale / Level 0
- 2 Incident
- 3 Serious Incident
- 4 Accident with Local Consequences
- 5 Accident with Wider Consequences
- 6 Serious Accident
- 7 Major Accident

No Safety Significance
**Class 1:** Any SSC which forms a principal means of ensuring nuclear safety. These items are the most important to safety. "Principal means" of ensuring nuclear safety should include the following:
- any item whose failure would lead directly to a beyond design basis event corresponding to an INES 5 or higher rating.

**Class 2:** Any SSC which makes a significant contribution to nuclear safety. The definition of "significant contribution" should include any item which is not otherwise required to be class 1, but which:
- is claimed to reduce the frequency of an initiating fault or hazard within the design basis with potential for an INES 3 or 4 event rating;

**Class 3** Any other SSC, i.e., that which is not in class 1 or 2, and where failure cannot lead to an event greater than an INES 2 rating.

**Class S** A further class of plant, "S" (seismic by association), that is used for classifying plant which, although itself having no safety significance, might seriously affect the operation of class 1 or 2 plant if it were to fail structurally during a seismic event.

(e.g. walls, pipework etc. -> these items must be then designed against applicable seismic loads)
Safety Classification: NRC

Risk-informed classification

New approach: safety-significance!

From a safety perspective, the benefits are associated with a better licensee and NRC focus of attention and resources on matters that are safety-significant.

A risk-informed SSC categorization scheme should result in an increased awareness on that set of equipment and activities that could impact safety, and hence an overall improvement in safety.
### Safety Classification: NRC

#### Risk-Informed Safety Classes acc. to 10 CFR §50.69

<table>
<thead>
<tr>
<th>RISC: Risk-Informed Safety Class</th>
<th>safety-related SSCs</th>
<th>Non safety-related SSCs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Integrity of RCPB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reactor shutdown and maintenance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or prevention/mitigation of accidents leading to offsite exposure</td>
<td></td>
</tr>
</tbody>
</table>

**SSCs performing safety significant\(^1\) functions which degradation or loss could result in a significant adverse effect on defence-in-depth, safety margin, or risk**

<table>
<thead>
<tr>
<th>RISC-1</th>
<th>RISC-2</th>
</tr>
</thead>
</table>

**SSCs performing low safety\(^1\) significant functions**

<table>
<thead>
<tr>
<th>RISC-3</th>
<th>RISC-4</th>
</tr>
</thead>
</table>

---

\(^1\) Result of PSA
Safety Classification: NRC

Risk-informed classification

Combines deterministic with probabilistic approach

Less prescriptive taking into account safety relevance combined with results of PSA

Progressive, more flexible method (cost effective)

Not yet extensive practical experience
Safety Classification: EUR

Level F1A:
Safety Functions needed to reach a Controlled State in Design Basis Category 3 and 4 Conditions (DBC) and in certain DBC 2.

Level F1B:
Safety Functions needed to reach a Safe Shutdown State in DBC 3, 4 and in certain DBC 2. If this state is reached before 24h the safety level F1B functions shall maintain the plant in this state at least until 24h from accident initiation.

Level F2:
Safety Functions needed to maintain a Safe Shutdown State beyond 24h and up to 72h from the initiating event in DBC 2, 3 and 4. Level F2 also includes Safety Functions needed in Complex Sequences up to 72h after onset of event as well as Safety Functions needed to reach and maintain a Severe Accident Safe State.

Non Safety (NS):
For times beyond 72h from the initiating event non-safety (NS) level is allowed for DBC and complex sequences.
Safety Classification: EUR

Initiating event $t=0\text{ s}$

In case of DBC

FIA

In case of DEC

F2

Controlled State

Safe Shutdown State

24h

72h

Time

Non-Safety
<table>
<thead>
<tr>
<th>Highest Safety Function Level performed by SSC</th>
<th>SSC Safety Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1A, F1B</td>
<td>Safety Class 1</td>
</tr>
<tr>
<td>F2</td>
<td>Safety Class 2</td>
</tr>
<tr>
<td>Non Safety (NS)</td>
<td>Non Safety (NS)</td>
</tr>
</tbody>
</table>
Safety Classification: YVL

Safety Class 1 shall include nuclear fuel as well as structures and components whose failure could result in an accident compromising reactor integrity and requiring immediate actuation of safety functions.

- reactor pressure vessel and those components of the primary circuit whose failure results in a primary circuit leak that cannot be compensated for by systems relating to normal plant operation.

Safety Class 2 are structures and components whose integrity is required for reactor decay heat removal or the containment of radioactive substances inside the facility following a Safety Class 1 component failure or pipe rupture.

- main components and piping of the emergency core cooling system
- structures of the core support and reactor shutdown system
- primary circuit piping supports and brackets
- the reactor containment including structures relating to the containment isolation function as well as other structures directly connecting to the containment fuel storage racks.
Safety Class 3 are
- buildings and structures ensuring the operability and physical separation of Safety Class 2 systems
- structures and components relating to barriers to the dispersion of radioactive substances
- structures relating to the handling of radioactive materials not assigned to higher safety classes and whose failure could result in a significant release of radioactive substances on-site or to the environment.

Class EYT (non-nuclear safety)
- System with a facility-specific risk importance, such as fire protection systems, protection against internal or external threats, radiation monitoring, environmental radiation monitoring network but not assigned to Safety Class 3.
- Systems necessary for bringing the facility to a controlled state at DEC (combination of failures, rare external events).
Safety Classification: Germany

**Class 1:** systems and components which failure would result in destruction of existing safety-relevant installations and hereby to exceedance of radiological limits.

Kind and scope of quality assurance measures are determined in that way that a catastrophic failure involving the destruction of safety-relevant installations is ruled out.

This class are also assigned systems and components which postulated failure involves a loss of coolant not able to cut off.

**Class 2:** hereto are assigned systems and components

a) necessary to control events with regard to shutdown, long-term maintenance of subcriticality and decay heat removal
b) Which failure would release big energy amounts and the consequences for the nuclear safety are not limited through construction or other safety measures
**Class 3:** hereto are assigned systems and components which specific radioactivity is above a threshold value set (usually systems in the reactor auxiliary building upstream the coolant cleaning or systems with concentrated coolant)

**Class 4:** hereto are assigned systems and components which specific radioactivity is below a threshold value set (usually systems in the CI or in the reactor auxiliary building downstream the coolant cleaning)

**Class 5:** hereto are assigned systems and components not bearing radioactive substances and have no contribution to nuclear safety.
TOP 7

Safety System Design
Requirement 24: Common cause failures

The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

Requirement 25: Single failure criterion

The single failure criterion shall be applied to each safety group incorporated in the plant design. Spurious action shall be considered to be one mode of failure when applying the single failure criterion.
• German Safety Requirements: safety systems at level 3 shall comply with the redundancy requirements (n+2 design)

• n+2: single failure, maintenance case

• Diversity (common cause failure)
### Safety System Design

#### Design of Safety Systems

<table>
<thead>
<tr>
<th>Design (to cover)</th>
<th>Design principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic design</td>
<td>Quality requirements, Break preclusion concept</td>
</tr>
<tr>
<td>Single Failure (A)</td>
<td>Redundancy</td>
</tr>
<tr>
<td>Common Cause Failure (B)</td>
<td>Diversity</td>
</tr>
<tr>
<td>Redundancy-wide internal and external events (hazards) (C)</td>
<td>Spatial separation, Structural protection</td>
</tr>
<tr>
<td>(A), (B), (C) and loss of emergency power supply</td>
<td>Inherent safety and fail-safe</td>
</tr>
<tr>
<td>Human Failure</td>
<td>Automation 30-Minutes concept</td>
</tr>
</tbody>
</table>
A single failure is a failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it.

Applied in a safety system when is called upon to deliver its safety function after a PIE.

Independent of the PIE.
Design of Safety Systems
Safety System Design

Diversity

Existence of two or more components / systems fulfilling the same safety function but based on **different physical** or **technical principles**

- Common Cause Failures (CCF) are important contributors to accidents.
- Prevention of CCF by “diversity” (diverse measures and equipment), e.g.
  - physically different effects, e.g. reactor shut-down by control rods and borating of the coolant
  - different procedures,
  - different designs
  - equipment of different manufacturers
Safety System Design

Inherent Safety / Fail-Safe

Inherent Safety:
Safety pertaining to the design / being design characteristic

e.g. negative reactivity coefficient

Fail-Safe-Design:
Safety-directed behaviour upon failure

e.g. e-driven control rods
Safety System Design

Physical / Spatial separation
Safety System Design

Loss of Offsite Power (LOOP)

Lost of house load (turbine, condenser etc.) AND lost of connection to the grid

---

TUV SÜD Industrie Service GmbH

18-09-28

Slide 110
**Safety System Design**

### Loss of Offsite Power (LOOP)

- **Lost of house load (turbine, condenser etc.) AND lost of connection to the grid**
- **Bus bar voltage < 80%, f < 47.2 Hz**
- **RCP speed < 94%**

**Either stabilise plant until e.g. grid available or shutdown plant**

- **big consumers tripped:**
  - RCP, Feedwater pumps, Condensate Pumps, circulating water pumps

- **Residual heat removal system**

- **P-RCS < 9 bar, T < 180 °C**

- **Scram / Turbine trip**

- **Start start-up/shutdown pumps**

- **Safe shutdown state**

- **Intermediate cooling system**

- **Nuclear service water system**
Safety System Design

Loss of Coolant Accident (LOCA):
Medium-size break

1. T containment
2. Leakage detection system: alarm
3. Leakage compensation (Borating system, VCS)
   - \( \Delta P \text{ cont/atm} > 30 \text{ mbar} \)
   - or \( L\text{-Pres} < 2.28 \text{ m} \)
   - or \( P\text{-RCS} < 131 \text{ bar while reactor power > 12\%} \)
4. RP
5. Scram / Turbine trip
Safety System Design

Earthquake

EQ detected

Bus bar voltage < 80%, f < 47.2 Hz

RCP speed < 94%

Leakages in RCS?

EDG

Leakage compensation (EBS, VCS if available)

RCS isolation

Start startup/shutdown pumps

P-RCS < 9 bar, T < 180 °C

Residual heat removal system

Safe shutdown state

Intermediate cooling system

Nuclear service water system

LOOP

Scram / Turbine trip

RP

A series of systems not credited / not available because not designed against EQ e.g.:
MS break after IV
FW pipe break after IV
VCS
Operational intermediate cooling system

Intermediate cooling system

Residual heat removal system

P-RCS < 9 bar, T < 180 °C

Start startup/shutdown pumps

RCS isolation

Leakage compensation (EBS, VCS if available)

Bus bar voltage < 80%, f < 47.2 Hz

EQ detected

Scram / Turbine trip

RP

Loop
Safety System Design

External hazards (e.g. APC, explosion pressure wave)

A series of systems not credited / not available because not designed against APC/EPW e.g.: MCR, EDG, ...

- Unavailability of MCR
- Scram / Turbine trip
- 10 h autarky
- Emergency control room

Secondary side

- Blow-off station
- Emergency feedwater pumps
- EDG for emergency feedwater system

Primary side

- P-RCS < 9 bar, T < 180 °C
- Residual heat removal system
- Emergency residual heat removal chain

- Safe shutdown state
- Intermediate cooling system
- Nuclear service water system
- Small, dedicated pumps
TOP 8

Operating Manual
Plant Modifications
Operating Manual / Plant Modifications

Operating Manual in German NPP

Overall Content

Part 0 Overall content and introduction

Part 1 Plant regulations
  e.g. personnel organisation, tasks and responsibilities in the MCR, maintenance regulation, regulations for radiational exposure, first aid and fire protection, alarms

Part 2 Operation of the overall plant
  Regulatory requirements
    Prerequisites and Conditions for plant's operation incl. allowable failure and maintenance periods of time
    Safety relevant limits / threshold values
    Normal operation of overall plant
  Abnormal operation
  Non-power operation
Part 3 Accidents
All events at level 3 are considered: event-oriented or protection goal oriented.
An accident guidance scheme helps to find the right event. In this case, the procedure is event-oriented. This is in Part 3.
If no event can be found then you proceed protection goal oriented. For every protection goal you find the relevant plant parameters and the corresponding procedure.

Part 4 Description and user manuals for the operation of all systems.
This is the biggest part of the operating manual and the responsibility lies with the operator.
In case of changes the operator simply informs the regulator.

Part 5 This part includes all conventional and computer alarms with their consequences for the plant and the necessary measures.
Plant modifications are regulated in the operating manual

Part 2, Chapter 1.5:

“Guidelines for treating plant modifications to the plant and its operating mode”
Operating Manual / Plant Modifications

Essential changes to the plant and its operating mode:

All that changes giving reason to a new assessment in an official permit procedure

e.g. change I&C from analog to digital
Other type of fuel elements
Non-essential changes

Category 1

All non-essential changes to plant systems and components or their operating mode which are directly relevant to safety.

These are systems and components which are necessary to safely shutdown the reactor or maintain it in a shutdown state, to remove decay heat, to avoid uncontrolled criticality and to minimize radioactivity exposition.

Regulator and his TSO to assess the change.
Regulator informs operator whether the change is completely accepted or accepted under consideration of possible alterations or even rejected.
After regulator’s permit is received, the change can be implemented.

e.g. changes in emergency core cooling system or EDG
Non-essential changes

Category 2

All non-essential changes to plant systems and components or their operating mode which are indirectly relevant to safety.

This involves change to any systems and components (operational, conventional, peripheral) which have a direct influence on safety relevant systems or components or on their operating mode.

TSO to assess the change and confirm category. Once positive assessment is issued and sent to the operator, the change can be carried out.

Any conditions mentioned in the assessment are to be met, tough.
Non-essential changes

Category 3

All the remaining non-essential changes to plant systems and components also to operational, conventional, peripheral ones which have a indirect influence on safety relevant systems or components or on their operating mode.

All the other changes do not fall under these regulations and treated according to operators internal procedures

After positive assessment and confirmation of category by the TSO, the change can be carried out.
Simple example:

The operator informs the regulator, that the HP Safety Injection Pump has a malfunction and the plant needs a new pump. The operator will order a new pump.

When is it a plant modification and what category is it?

The new pump has the same parameters – it is not a modification!

The operator installs the new pump and tests the equipment. It is found that the new pump delivers 120 bar instead of 115 bar, but the mass flow is reduced from 150 Kg / s to 145 Kg / s. The operator informs the regulator.

Due to the parameter changes, it becomes a plant modification!
Operating Manual / Plant Modifications

What is to do?

You as regulator must check

• If the new parameters still fulfill the requirements of the plant permit, or a amended permit is needed (Essential changes or Non essential changes)

• Since the differences between old and new equipment are relatively small, it is a Non essential change
  
  “These are systems and components which are necessary … to remove decay heat … .” also in Category 1

Upon commissioning, the documents such as Operating Manual must be adapted in different parts.
End of Presentation

Thank you for your attention!

Teşekkür ederim!
TOP 9

Wrap-up / Questions