IAEA International Conference in Nuclear Installation Safety

(21-24 October 2013)

Successive evolutions of the Defence in depth concept

Bernard POULAT

Senior Safety Officer

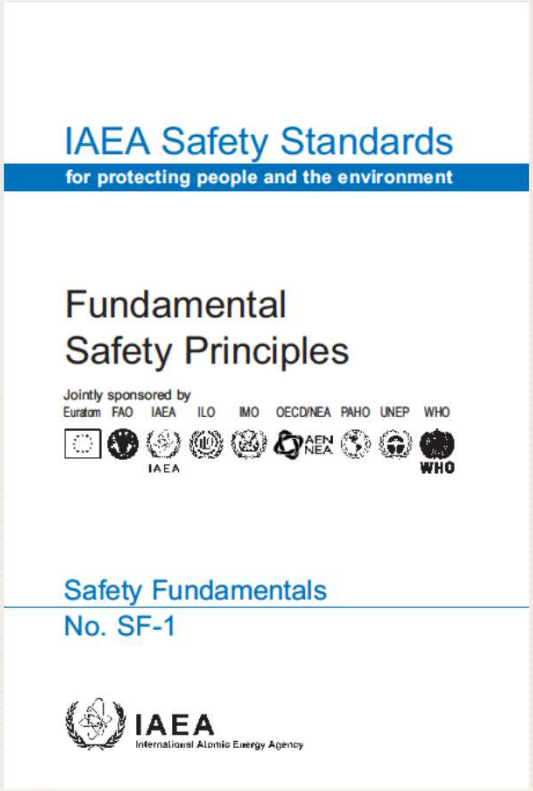
Department of Nuclear Safety and Security

Division of Nuclear Installation Safety

IAEA

International Atomic Energy Agency

IAEA SAFETY FUNDAMENTALS



Principle 8: Prevention of accidents
All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.

A defence in depth strategy has been recognized as a fundamental principle to keep the likelihood of an accident having harmful consequences extremely low.

- 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.
- The independent effectiveness of the different levels of defence is a necessary element of defence in depth.

IAEA

IAEA SAFETY FUNDAMENTALS

For design of NPPS, the successive updates of the original concept elaborated in INSAG 3 (1988) must be considered as needs for clarification and reflect the necessity for a continuous improvement of nuclear safety by integrating feedback, but do not change the fundamental elements of the original concept :

- Protection of the public and environment by consecutive barriers
- Protection of the barriers
- Appropriate quality, conservatism and robustness of each level
- Consideration of accident conditions exceeding those considered for design

IAEA

Defence in depth levels (INSAG 10)

Levels of defence in depth	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

level 1 aims to prevent deviations from normal operation and equipment/system failures. (Level 1 provides the initial basis for protection against external and internal hazards)

level 2 aims to detect and intercept deviations from normal operation in order to prevent anticipated operational occurrences from escalating to accident conditions.

level 3 is the control of postulated design basis accidents within design basis conditions with the objective to prevent core damage,

level 4 is defined as the control of severe conditions in which conditions caused by design basis accidents may be exceeded with the objective to ensure that the likelihood of such accident and the magnitude of radioactive releases are both kept as low as reasonably achievable.

level 5 is defined as the mitigation of the radiological consequences of significant external radioactive releases, and requires the provision of adequately equipped emergency facilities and plans for the on-site and off-site emergency response.

IAEA

Defence in depth: IAEA SSR-2/1

Radiation protection have been enhanced:

- High radiation doses or large radioactive releases shall be practically eliminated, (SSR-2/1 Requirement 5, item 4.3),
- Design basis accidents have no, or only minor, radiological impacts, on or off the site, and do not necessitate any off-site intervention measures (SSR-2/1 Requirement 19, item 5.25),
- For Design extension conditions, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public*, and sufficient time shall be made available to implement these measures (SSR-2/1 Requirement 20, item 5.31).

* In INSAG 10/ NS-R-1 radiological releases were supposed to be kept as low as reasonably achievable

Consequently …

IAEA

Defence in depth: IAEA SSR-2/1

…. More confidence in the success of the mitigation of a severe accident

Levels of defence in depth	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Dedicated safety features for severe accident prevention and mitigation + accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

Level 4 is reinforced by requirements applicable to the means necessary to prevent severe accidents and to mitigate their consequences:

- Dedicated SSCs shall be independent to extent practicable of those used in more frequent accidents, (SSR-2/1 Req. 5.29 a)
- DEC conditions are assessed to define the design bases of the SSCs necessary to mitigate their consequences, (SSR-2/1 Req. 5.28)
- SSCs are capable of performing their intended functions under environmental conditions prevailing during such accident conditions (SSR-2/1 Req. 5.29 a)
- Dedicated SSCs are appropriate and effective enough to meet the radiological limits relevant for DEC

For plants built to earlier standards, mitigation of situations not considered in the reference design might take use of non permanent equipment. Nevertheless, accident management should not be an excuse not to install to the extent practicable permanent complementary equipment.

IAEA

Defence in depth: Post Fukushima-Dai-ichi accident

The Fukushima Dai-ichi accident reminded to all of us the importance of a correct and complete application of the defence in depth strategy, and some elements are of particular importance to ensure that the likelihood of an accident having harmful consequences is extremely low:

- A correct site hazard characterization is of first importance for the design of the plant,
- Appropriate margins are necessary to avoid a cliff edge effect,
- The effectiveness of the defence in depth strategy requires an adequate diversity and independence between levels of defence,
- Accidents more complex and severe than those considered for the reference design cannot be excluded and should be anticipated through accident management strategies and capabilities,
- An emergency preparedness and response plan is available at the site

IAEA

Defence in depth and Margins

SSCs important to safety should not collapse or fail in case of loads moderately exceeding those caused by postulated initiating events and hazards.

Margins are generally commensurate with the safety significance of SSCs and are implemented by assessing the loads with conservatism, and using well proven design/ manufacturing codes*.

New : Taking into account the difficulty to predict the intensity of the future natural hazards, a proposal to verify that the margins provided by design, for a limited number of SSCs**, are sufficient to cope with external hazards of a severity significantly higher, is circulated to MS comments.

- See INSAG 3/ IAEA 50 CD and INSAG 10/ IAEA NS-R-1
- ** SSCs which should not collapse or fail in order to avoid unacceptable consequences (long term off site contamination)

IAEA

Independence between levels of Defence

Independence between levels of defence does not supersede independence between redundancies implemented within one level, and both of them should be considered for the evaluation of the overall effectiveness of the defence in depth concept.

Strengthening one level or the architecture cannot be an excuse to the decrease the reliability of the individual levels.

SF-1: “The independent effectiveness of the different levels of defence is a necessary element of defence in depth.”

SSR-2/1: “ Levels of defence shall be independent as far as is practicable.”

Ideal design where each SSC would be allocated to a single level is unrealistic and could lead to useless complexity,

How far independence between levels should be implemented is not cristal clear and might explain weaknesses in its application.

IAEA

Independence between levels of Defence

- Independence is essential where simultaneous failures would lead to harmful effects to people or to the environment.

Complementary safety features specifically designed to mitigate the consequences of a core melt accident should be independent from the SSCs designed for more frequent accidents.

- For robustness of the design, it makes sense that:

  - The ability of SSCs should not be affected by the initiating event (and its consequences) for which they are designed to respond to,

  - Complementary safety features, designed to back up SSCs implementing safety functions, should be independent from SSCs postulated as failed in the sequence,

IAEA

Consideration of Common Cause Failures

CCF may be initiated by:

- propagation of the effects of an external or internal hazard,
- propagation of a failure,
- unpredictable latent fault in design, manufacturing, etc.

High reliability requires that vulnerabilities for CCF should be eliminated to a reasonable extent.

- segregation and independence is effective to prevent propagation,
- Diversity is more appropriate to eliminate latent faults.

- CCF can be identified by either probabilistic or deterministic approaches
- Plant response should be analysed
- Where consequences are judged unacceptable (e.g. Consequences exceed those accepted for accidents with multiple failures), a change in the layout providing protection, or safety features unlikely to be subjected to the same common cause failure should be implemented.

IAEA

Defence in depth and accident management

IAEA

"Be prepared to the unexpected…"

- Accident management should anticipate accidents and complex sequences beyond those considered in the reference design of the plant (INSAG 3),
- Scenarii should be postulated and the plant response analysed to assess the grace period time before unacceptable consequences, and to identify necessary complementary means,
- Any design should include provisions to facilitate the accident management (complementary equipment, procedures, hook up points for non permanent equipment, etc.),
- Periodic drills should be performed.

Application of Defence in depth to I&C Systems

I&C system architecture should reflect the defence in depth strategy:

- different I&C systems to initiate the operation of the systems designed to accomplish the fundamental safety functions,
- appropriate segregation, independence and diversity between the I&C system**s** in order not to compromise the defence in depth strategy in case of failures affecting one system.

Despite needs and necessity to:

- Exchange information among the divisions,
- Monitor the same plant parameters,
- Convey a lot of information of different safety significance.

IAEA

- level 1: I&C functions should aim to prevent deviations from normal operation by keeping the plant parameters within their specified range for normal operation,
- level 2: I&C functions should aim to detect and control deviations from normal operation in order to prevent AOOs from escalating to accident conditions,
- level 3: I&C functions should aim to detect and control DBAs within the design basis,
- level 4: I&C functions aim to manage the consequences of accidents that result from failures of the third level of defence so as to prevent progression of the accident or to mitigate the consequences of a severe accident,
- level 5: I&C functions aim to support and facilitate decisions with regard to the appropriate off-site emergency measures to be implemented to protect the public in the event of a radiological release.

Application of Defence in depth to I&C Systems

- For modern I&C systems, in particular systems whose functionality depends upon software or HDL code, and irrespective of all preventive measures*, demonstration that I&C system is proven to be error free is very difficult and may always be disputed.
- Therefore, combination of credible PIE with CCF in the I&C should be postulated .
- Verification that the overall I&C design adequately addresses the potential for common cause failure (CCF) is expected.

* Use of life cycle models that describe the activities for the development of I&C systems

CCF vulnerabilities may be addressed by eliminating the vulnerability, or justifying acceptance of the vulnerability:

- Vulnerabilities for combination of credible PIE with CCF in I&C leading to (significant) core damage should be removed,
- Realistic hypotheses may be used to assess the consequences and to demonstrate the efficiency of the diverse provision when implemented.

Diversity is a way to reduce CCF vulnerability resulting from design, manufacturing or maintenance error, and to include conservatism to compensate for the difficulty of demonstrating the specified level of reliability.

E.g: Diverse Actuation System (DAS), which provides a diverse sub-set of backup protection system functions is more and more often implemented where the Reactor Protection System uses digital technology.

Diverse means should be selected not to be subjected to the same CCF and with an adequate reliability to rule out of design a simultaneous failure of the RPS and its back up.

IAEA

Application of Defence in depth to I&C Systems

In conclusion separation, independence and diversity should be adequately considered in the design of the I&C architecture, taking into account that:

- I&C failure (CCF included) should not be a cause for a core melt accident,
- Independence is essential where failure would lead to harmful effects to people or to the environment (e.g. I&C system should be independent from other I&C systems).

IAEA

…Thank you for your attention

E-mail: b.poulat@iaea.org